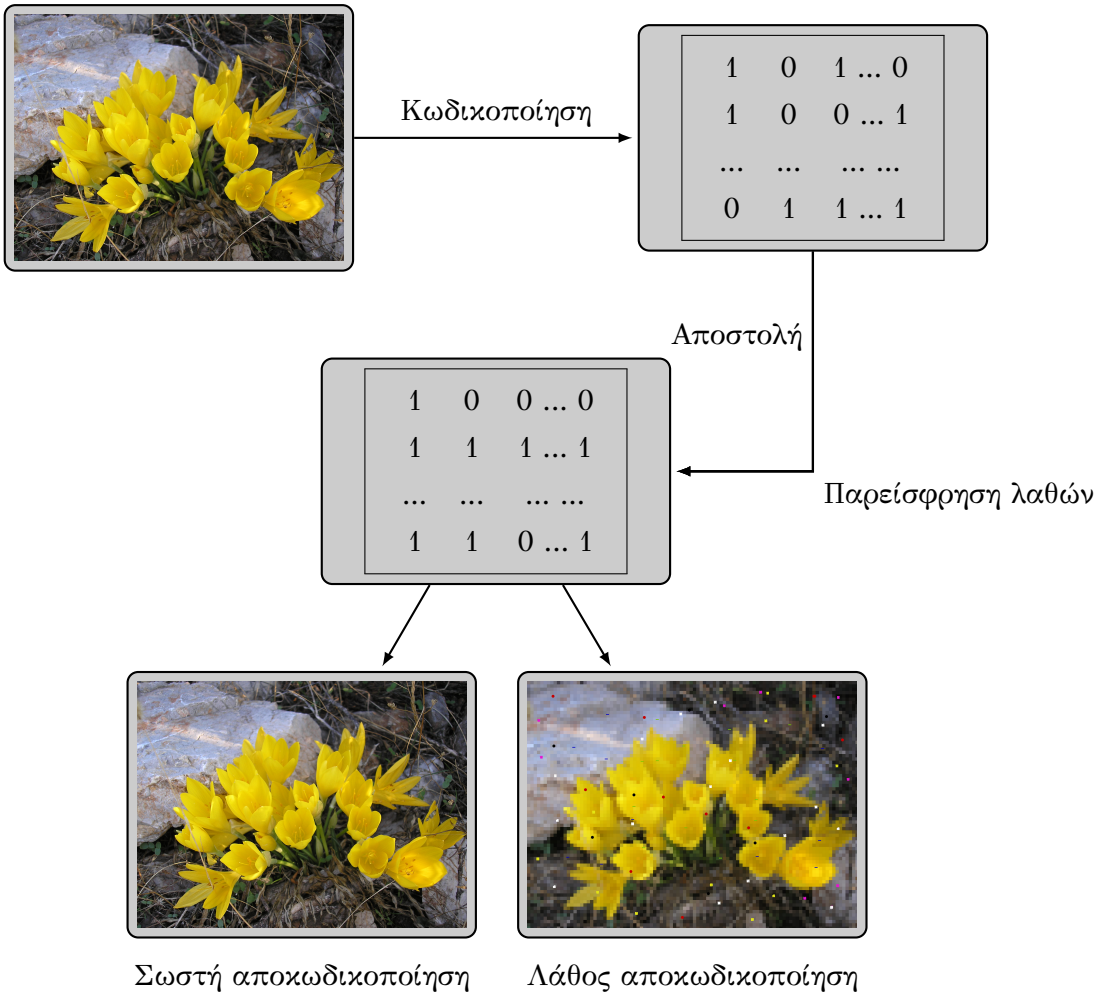
Δημητριος Α. Βαρσος

ΜΙΑ ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΛΓΕΒΡΙΚΗ ΘΕΩΡΙΑ ΚΩΔΙΚΩΝ



ΜΙΑ ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΛΓΕΒΡΙΚΗ ΘΕΩΡΙΑ ΚΩΔΙΚΩΝ

Δημήτριος Α. Βάρσος

Αθήνα 2015

Συγγραφική Ομάδα
Δημήτριος Βάρσος

Κριτικός Αναγνώστης
Μιχάλης Συκιώτης

Συντελεστές Έκδοσης
ΓΛΩΣΣΙΚΗ ΕΠΙΜΕΛΕΙΑ: Αναστασία Τσιαδήμου
ΤΕΧΝΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ: Βασίλειος Πασχάλης

ISBN: 978-960-603-040-6

Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
Εθνικό Μετσόβιο Πολυτεχνείο
Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

http://www.kallipos.gr

Σ' αυτούς που νοιάστηκαν για μένα…

…σ' αυτούς που νοιάζονται για μένα…

Ευχαριστίες

Η επιτυχής συγγραφή ενός διδακτικού βιβλίου, πέραν του συγγραφέως, εξαρτάται και από πολλούς άλλους παράγοντες.

Οι παράγοντες αυτοί, τις περισσότερες φορές, είναι *αφανείς* για τον αναγνώστη. Αυτό δεν σημαίνει ότι είναι και ασήμαντοι.

Καταρχήν το υλικό του βιβλίου έχει δοκιμαστεί στην τάξη. Οι παρατηρήσεις, οι υποδείξεις ακόμη και οι απορίες από "ορεξάτους" φοιτητές με "φρέσκα μυαλά" ήταν πολύτιμες για την διάρθρωση και παρουσίαση της ύλης. Τους ευχαριστώ θερμά.

Δύο όμως πρόσωπα συνέβαλαν ουσιαστικά στην υλοποίηση του όλου εγχειρήματος. Πρόκειται για τους συνεργάτες κ. Μιχαήλ Συκιώτη, επίκουρο καθηγητή στο τμήμα Μαθηματικών του Πανεπιστημίου Αθηνών και κ. Βασίλειο Πασχάλη, υποψήφιο διδάκτορα του Μεταπτυχιακού προγράμματος Λογικής και Αλγορίθμων. Ο πρώτος ως Κριτικός Αναγνώστης και ο δεύτερος ως Υπεύθυνος Τεχνικής Επεξεργασίας, πέραν της *επαγελματικής ευσυνειδισίας* που επέδειξαν, ασχολήθηκαν με μεράκι[1] με το έργο. Με αποτέλεσμα την όσον το δυνατόν αρτιότερη ποιοτική και τεχνική αναβάθμιση του αρχικού κειμένου.

Οι όποιες ευχαριστίες από την θέση αυτή είναι ανεπαρκείς για να εκφράσουν το μέγεθος της προσφοράς τους.

[1] Μεράκι: Μη μετρήσιμη έννοια, ανεκτίμητη αξία.

Πρόλογος

Όπως ο 19ος αιώνας αναφέρεται από τους ιστορικούς ως ο αιώνας της βιομηχανικής επανάστασης, ίσως ο 20ος αιώνας να αναφέρεται ως ο αιώνας της πληροφορίας. Τεχνολογικά επιτεύγματα όπως το τηλέφωνο, το ραδιόφωνο, η τηλεόραση, οι υπολογιστές και το διαδίκτυο, έχουν επηρεάσει βαθύτατα τον τρόπο που βιώνουμε την ζωή μας. Για παράδειγμα, καθένας μπορεί να δει στην οθόνη του υπολογιστή του φωτογραφίες από το διάστημα, να συνομιλήσει με άτομα, τα οποία βρίσκονται στην άλλη "άκρη της γης", να αποθηκεύσει σε μία συσκευή μεγέθους "γομολάστιχας" το περιεχόμενο των βιβλίων μιας ολόκληρης βιβλιοθήκης. Με "δύο λόγια" ένα τεράστιο μέγεθος πληροφοριών μπορεί να αποθηκευθεί, να μεταδοθεί και να επεξεργαστεί με εκπληκτική ταχύτητα, ακρίβεια και οικονομία.

Προφανώς, αυτά τα επιτεύγματα δεν θα μπορούσαν να πραγματοποιηθούν χωρίς θεωρητικό υπόβαθρο. Ως συνήθως, σε τέτοιες περιπτώσεις, στην αρχή (στα μέσα του περασμένου αιώνος) τα πρώτα βήματα έγιναν από μη Μαθηματικούς (από Μηχανικούς), οι οποίοι βασίστηκαν περισσότερο στην εμπειρία και στην διαίσθηση, παρά στα Μαθηματικά καθ' εαυτά. Γρήγορα όμως οι Μαθηματικοί, με μεγάλη ευχαρίστηση, βρήκαν νέο πεδίο εφαρμογών. Νέοι κλάδοι των Μαθηματικών αναπτύχθηκαν και τα πρώτα εμπειρικά αποτελέσματα των Μηχανικών ανήχθησαν σε πλήρεις Θεωρίες "με Ορισμούς,

Θεωρήματα και Αποδείξεις". Παράλληλα δε ορισμένες παλαιότερες Θεωρίες αναβίωσαν μέσω απρόσμενων εφαρμογών. Ποιος θα μπορούσε να προβλέψει, πριν εκατό χρόνια, ότι οι Κώδικες Διόρθωσης Λαθών θα βασίζονταν σε αλγεβρικές καμπύλες επί πεπερασμένων σωμάτων ή ότι τα Κρυπτογραφικά Συστήματα θα εξαρτώνταν από την (βαθεία) γνώση των πρώτων αριθμών και τη Θεωρία Ομάδων;

Η Θεωρία της Πληροφορίας και η Θεωρία Κωδίκων είναι αλληλένδετες από την γεννησή τους, η οποία σηματοδοτείται από το περίφημο άρθρο του Caude Shannon *"A Mathematical Theory of Communications"* το 1948. Τουναντίον η Κρυπτογραφία, αν και συνδέεται με τις Θεωρίες της Πληροφορίας και Κωδίκων, είναι αρχαιοτάτη. Από "καταβολής κόσμου" ο ανθρωπος είχε μυστικά, τα οποία ήθελε να μοιράζεται με άτομα της δικής του επιλογής.

Ο διαχωρισμός γίνεται κυρίως για τεχνικούς και εκπαιδευτικούς λόγους.

Η επί σειράν ετών "δοκιμασία" στην τάξη δημιούργησε την πεποίθηση ότι, σε πρώτο στάδιο, η αυτοτελής παρουσίαση κάθε μίας θεωρίας ξεχωριστά ενδείκνυται από εκπαιδευτικής σκοπιάς. Αυτό κατ' ουδέναν τρόπο δεν σημαίνει ότι πρέπει να "υψώνονται τείχη" μεταξύ των διαφόρων περιοχών των Μαθηματικών.

Για τον λόγο αυτό το "ανά χείρας" βιβλίο, το οποίο απευθύνεται τόσον σε φοιτητές Θετικών Επιστημών, όσον και σε άτομα, τα οποία θα ήθελαν να "αυτοδιδαχθούν", πραγματεύεται μόνο τη Θεωρία Κωδίκων. Σκοπός του είναι να εισάγει τους αναγνώστες στην Θεωρία Κωδίκων και ειδικότερα στην Αλγεβρική Θεωρία Κωδίκων. Παράλληλα όμως σκοπεύει να δείξει, ακόμα και στον ανυποψίαστο αναγνώστη, την αναγκαιότητα, τη δύναμη και την ωραιότητα των Μαθηματικών.

Το προαπαιτούμενο Μαθηματικό υπόβαθρο δεν είναι απαιτητικό και θα μπορούσε κάποιος να ισχυρισθεί ότι στοιχειώδεις γνώσεις Γραμμμικής Άλγεβρας και Πιθανοτήτων, καθώς και μία σχετική ευχέρεια στην χρήση των πολυωνύμων με συντελεστές από ένα σώμα είναι αρκετές για να αρχίσει την μελέτη του βιβλίου αυτού.
Πέραν όμως των συγκεκριμένων γνώσεων απαιτείται μία γενικότερη Μαθηματική ωριμότητα, η οποία δεν διδάσκεται, αλλά την αποκτά κάποιος με την

πάροδο του χρόνου ασχολούμενος με τα Μαθηματικά.

Για τον λόγο αυτό, το επίπεδο, στην αρχή, έχει επιλεγεί ούτως ώστε να είναι προσιτό ακόμη και σε άτομα χωρίς προηγούμενη (υψηλή) Μαθηματική παιδεία, τα οποία όμως είναι διατεθημένα να μελετήσουν τα "απαιτούμενα" Μαθηματικά. Προοδευτικά όμως γίνεται πιο απαιτητικό και σε πολλά σημεία δίνονται ερεθίσματα για περαιτέρω μελέτη.

Το βιβλίο χωρίζεται σε έξι Κεφάλαια και ένα Παράρτημα. Έγινε προσπάθεια ούτως ώστε οι επιμέρους παράγραφοι να είναι όσον το δυνατόν ανεξάρτητοι, για να εξασφαλίζεται η σχετική ευελιξία ως προς την σειρά τόσον κατά τη διάρκεια της διαδασκαλίας στην τάξη (ανάλογα με το επίπεδο και τις *ανάγκες* του ακροατηρίου), όσον και κατά την αυτοδιδασκαλία.

Στο πρώτο κεφάλαιο, εκτός από τις βασικές έννοιες και ορισμούς, γίνεται μια παρουσίαση μαθηματικών τεχνικών για την κατασκευή κωδίκων, καθώς και ανάπτυξη αποτελεσματικών μεθόδων για την χρήση αυτών. Επίσης, εισάγεται η έννοια του τέλειου κώδικα και μελετώνται ορισμένα φράγματα του μεγέθους ενός κώδικα σε συνάρτηση με τις υπόλοιπες παραμέτρους (μήκος και ελάχιστη απόσταση).

Το δεύτερο κεφάλαιο είναι αφιερωμένο στους Γραμμικούς Κώδικες. Εδώ γίνεται προσπάθεια να καταδειχθεί η σημασία της αλγεβρικής δομής των κωδίκων ως διανυσματικών χώρων επί πεπερασμένων σωμάτων. Η γνωστή γεωμετρική έννοια της καθετότητας αποτελεί βασικό εργαλείο τόσον για τον ορισμό και την μελέτη του δυϊκού κώδικα ενός γραμμικού κώδικα, όσον και για τον σχεδιασμό μεθόδων για την αποτελεσματική και γρήγορη διόρθωση/ανίχνευση λαθών μέσω ενός γραμμικού κώδικα.

Στο τρίτο κεφάλαιο, χρησιμοποιώντας απλές ιδιότητες του δακτυλίου πολυωνύμων με συντελεστές από ένα πεπερασμένο σώμα, εισάγονται οι πολυωνυμικοί και κυκλικοί κώδικες. Οι κώδικες αυτοί αποτελούν την σημαντικότερη, ίσως, κατηγορία κωδίκων, τόσον σε θεωρητικό, όσον και σε πρακτικό επίπεδο. Η μελέτη των κωδίκων αυτών απαιτεί τη γνώση της έννοιας του ιδεώδους και του δακτυλίου πηλίκων. Εδώ ο αναγνώστης θα πρέπει να γνωρίζει (ή να φροντίσει τώρα να μελετήσει) και να χειρίζεται με σχετική ευχέρεια αυτές τις αλγεβρικές έννοιες.

Στο τέταρτο κεφάλαιο παρουσιάζονται μερικές πολύ γνωστές κατηγορίες κωδίκων. Οι κώδικες αυτοί παρουσιάζουν πρακτικό και θεωρητικό ενδιαφέρον. Οι κώδικες αυτοί είναι γραμμικοί, πολλοί δε από αυτούς είναι κυκλικοί. Η μελέτη τους αποτελεί εφαρμογή όσων προηγήθηκαν στα προηγούμενα κεφάλαια.

Το πέμπτο κεφάλαιο είναι αφιερωμένο σε μια ευρεία και οικογένεια κωδίκων, τους Reed-Solomon κώδικες. Ενδιαφέρον παρουσιάζουν οι διάφορες (υπο)κατηγορίες, οι οποίες αποτελούν ειδικές περιπτώσεις ή γενικεύσεις των κωδίκων αυτών.

Στην οικογένεια αυτή ανήκουν πολλοί από τους κώδικες που παρουσιάζονται στο προηγούμενο κεφάλαιο. Στο παρόν κεφάλαιο επισημαίνεται το γεγονός αυτό. Η παρουσίασή τους όμως έγινε ανεξάρτητα, διότι, όπως έχουμε προείπει, σκοπός μας είναι μια ευελιξία τόσον στην διδασκαλία όσον και στην αυτόνομη μελέτη, ανάλογα με το επίπεδο και τα ενδιαφέροντα του ακροατηρίου/αναγνώστη.

Στο έκτο κεφάλαιο γίνεται μια προσπάθεια να δειχθεί η σχέση της Αλγεβρικής Θεωρίας Κωδίκων με έναν μεγάλο και ενδιαφέροντα κλάδο των Μαθηματικών, τη Συνδυαστική. Εδώ (για σχετική αυτοτέλεια) απλώς παρατίθενται τα ελάχιστα αναγκαία από τη Συνδυαστική για να τα εφαρμόσουμε στους κώδικες.

Τέλος, στο Παράρτημα παρατίθενται συνοπτικά οι αλγεβρικές έννοιες που απαιτούνται στα προηγούμενα κεφάλαια. Το μέρος αυτό **δεν** είναι (και δεν πρέπει να θεωρηθεί ως) μια εισαγωγή στην Άλγεβρα. Σκοπός του είναι να συμβάλλει στην αυτοδυναμία του βιβλίου και για διευκόλυνση του αναγνώστη, ο οποίος θα ανατρέχει σ' αυτό για να επαναφέρει στην μνήμη του έννοιες, τις οποίες (οφείλει να) έχει διδαχθεί σε ένα μάθημα "Βασικής Άλγεβρας" προπτυχιακού επιπεδου.

Σε κάθε παράγραφο παρατίθενται πολλά παραδείγματα, όπως και αρκετές ασκήσεις. Επειδή πιστεύουμε στην ενεργή συμμετοχή του αναγνώστη κατά τη διάρκεια της μελέτης του, το κείμενο είναι *διανθισμένο* με εκφράσεις του τύπου *...εύκολα βλέπουμε ότι...*, *...δεν είναι δύσκολο να αποδείξουμε ότι...*, *η απόδειξη αφίεται ως άσκηση...*, όπως επίσης και πολλά *γιατί;*. Κατά

τη γνώμη μας τα σημεία αυτά αποτελούν τις πλέον σημαντικές, για την κατανόηση, ασκήσεις και για το λόγο αυτόν συνιστάται να δίνονται τέτοιου είδους ερεθίσματα τόσον κατά τη διδασκαλία στην τάξη όσον και κατά την ιδίαν μελέτη. Το κυριώτερον όμως, όπως (πρέπει να) συμβαίνει με τη μελέτη στα Μαθηματικά, είναι ότι πρέπει να χρησιμοποιείται "μολύβι και χαρτί".

Όπως προείπαμε, στο βιβλίο αυτό δεν εξαντλούμε την μελέτη της Αλγεβρικής Θεωρίας Κωδίκων. Επιπλέον, πιστεύουμε ότι κατά την διάρκεια της μελέτης ενός αντικειμένου ο περιορισμός σε μόνο σύγγραμμα (όσο καλό και να είναι αυτό) *εγκλωβίζει* τον αναγνώστη. Στο τέλος κάθε κεφαλαίου παρατίθεται μια ενδεικτική βιβλιογραφία. Εκτός από τα συγγράμματα, στα οποία παραπέμπεται ο αναγνώστης σε συγκεκριμένα σημεία του κειμένου, περιλαμβάνονται και άλλα, κατά τη γνώμη μας, ενδιαφέροντα συγγράμματα. Με τον τρόπο αυτό ο ενδιαφερόμενος αναγνώστης *απεγκλωβίζεται* και οδηγείται σε περαιτέρω μελέτη.

Τέλος, επειδή το καλύτερο βιβλίο είναι ...αυτό που δεν γράφτηκε..., το βιβλίο αυτό σίγουρα περιέχει λάθη και επιδέχεται βελτιώσεις. Θα θέλαμε να πιστεύουμε ότι: Τα τυπογqαφικ'α λάθη είναι λίγα, τα γραματοικά και ωρθογραφεικά λιγότερα, ελάχιστα συντακτικά λάθη τα εκφραστικά. Κάθε διόρθωση που προέρχεται από καλοπροαίρετη (έστω αυστηρή) κριτική είναι ευπρόσδεκτη και οι ευχαριστίες προκαταβάλλονται....

Περιεχόμενα

Πίνακας συντομεύσεων-Ακρωνύμια

ISBN σελ. 33

MDS σελ. 151

BCH σελ. 306

MOLS σελ. 377

POLS σελ. 377

μκδ σελ. 409

εκπ σελ. 418

ΚΕΦΑΛΑΙΟ 1

Βασικές Έννοιες

Στο Κεφάλαιο αυτό εισάγουμε την έννοια του κώδικα και αναφέρουμε ορισμένες βασικές ιδιότητες, οι οποίες είναι απαραίτητες για τα επόμενα.

Για μια, επίσης, καλή εισαγωγή στις αρχικές έννοιες μπορείτε να ανατρέξετε στο πρώτο μέρος του βιβλίου του Pretzel, O. "Error-Correcting Codes and Finite Fields" Pretzel, O. [1992].

1.1 Τι είναι κώδικας

Όλοι έχουμε ακούσει για κώδικες, για κωδικοποιημένα μηνύματα, για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων και άλλα σχετικά. Λίγοι όμως έχουν συνειδητοποιήσει ότι δεν υπάρχει άνθρωπος που να μην χρησιμοποιεί ανά πάσα στιγμή κώδικες.

Η γλώσσα που χρησιμοποιούμε για να επικοινωνούμε δεν είναι τίποτε άλλο παρά ένας κώδικας. Πράγματι, κάθε τι που θέλουμε να εκφράσουμε προφορικώς ή γραπτώς το *κωδικοποιούμε* σε μία ακολουθία *λέξεων* χρησιμοποιώντας *γράμματα* από ένα *αλφάβητο*. Το σύνολο αυτών των λέξεων αποτελεί ένα *μήνυμα* το οποίο μεταδίδουμε προφορικώς, γραπτώς ή με κά-

ποιον άλλο τρόπο.

Σε μια γλώσσα που έχει ένα αλφάβητο μπορούμε να σχηματίσουμε πάρα πολλές 'λέξεις' (θεωρητικά άπειρες). Από αυτές όμως λίγες έχουν *νόημα*, δηλαδή αποτελούν στοιχεία του γλωσσικού κώδικα επικοινωνίας. Για τον σχηματισμό των λέξεων που έχουν νόημα και γενικώτερα για τη συγκρότηση του γλωσσικού οικοδομήματος χρησιμοποιούνται κανόνες, όπως ορθογραφικοί, γραμματικοί, συντακτικοί κ.λ.π.

Κατά τη μετάδοση ένος μηνύματος, με κάποιον τρόπο, ενδέχεται αυτό (μερικώς) να αλλοιωθεί. Για παράδειγμα, αν η μετάδοση γίνεται προφορικά και ο ομιλητής (ο αποστολέας του μηνύματος) δεν έχει καλή άρθρωση, ή ο παραλήπτης δεν έχει καλή ακοή, ή, το πιθανότερο, υπάρχουν θόρυβοι, οι οποίοι παρεμβάλονται και παρεμποδίζουν τη σωστή λήψη του μηνύματος.

Αυτός που ακούει (ο παραλήπτης του μηνύματος) είναι αναγκασμένος να συνάγει τι μήνυμα εστάλη από το μήνυμα που έλαβε (να *αποκωδικοποιήσει* το μήνυμα). Για βοήθεια έχει τον κώδικα γλωσσικής επικοινωνίας. Πολλές φορές είναι αναγκασμένος να εικάσει για το μήνυμα στηριζόμενος 'στα συμφραζόμενα' ή ακόμα, αναλαμβάνοντας τον κίνδυνο για λανθασμένη απόδοση, να αποδώσει μέρος του μηνύματος τυχαία.

Ένα από τα χαρακτηριστικά ενός κώδικα γλωσσικής επικοινωνίας είναι ο πλούτος του λεξιλογίου του, που μας επιτρέπει να μπορούμε να μεταδώσουμε πολλά και σύνθετα νοήματα. Δηλαδή έχουμε τη δυνατότητα να μεταδώδουμε μεγάλο μέγεθος *πληροφορίας*. Άμεσα με το μέγεθος της πληροφορίας σχετίζεται και η ποιότητα της μεταδιδόμενης πληροφορίας, καθώς επίσης και η οικονομία κατά τη μετάδοση. Οι δυνατότητες αυτές βεβαία καθορίζονται από τη *δομή* του γλωσσικού κώδικα. Οι απαιτήσεις αυτές, από την πλευρά τους, καθορίζουν ως έναν βαθμό το πώς θα αναπτυχθεί ένας γλωσσικός κώδικας για να είναι *αποτελεσματικός*. Δεν πρέπει όμως να αγνοείται ο τρόπος επικοινωνίας, δηλαδή το μέσον που έχουμε στη διάθεσή μας για τη μετάδοση ενός μηνύματος. Το μέσον επικοινωνίας ορισμένες φορές επιβάλλει τον τρόπο με τον οποίο είναι δομημένος ένας κώδικας γλωσσικής επικοινωνίας.

Δεν πρέπει να ξεχνάμε ότι μια γλώσσα πρέπει να είναι καλή τόσο στην μετάδοση του προφορικού όσο και του γραπτού λόγου.

Οι 'ανάγκες' πολλές φορές επιβάλλουν να επινοήσουμε άλλους τρόπους (κώδικες) επικοινωνίας. Όταν λέμε οι ανάγκες, ο καθένας μπορεί να φανταστεί ό,τι θέλει. Από το ότι δεν θέλουμε ένα μήνυμα να γίνει γνωστό σε τρίτους, έως τα μέσα μετάδοσης που έχουμε στη διάθεσή μας. Για παράδειγμα, οι Ινδιάνοι χρησιμοποιούσαν σήματα καπνού. Σήμερα διαθέτουμε σύγχρονα ηλεκτομαγνητικά μέσα εγγραφής, αποθήκευσης και μετάδοσης μηνυμάτων. Ενδιάμεσα, όπου είχαμε στη διάθεσή μας τη στοιχειώδη χρήση του ηλεκτρικού ρεύματος, αρκούμαστε να αναφέρουμε την επινόηση και χρήση του κώδικα Morse.

Τα προηγούμενα αποτελούν μια αχλύ ιδέα για το τι σημαίνει κώδικας επικοινωνίας. Στην αμέσως επόμενη παράγραφο θα προσπαθήσουμε να γίνουμε πιο συγκεκριμένοι.

1.2 Ορισμοί και στοιχειώδεις ιδιότητες

Έστω $\mathbb{A} = \{ a_1, a_2, \ldots, a_r \}$ ένα τυχαίο μη κενό πεπερασμένο σύνολο. Το σύνολο $\mathbb{A}$ θα το ονομάζουμε **αλφάβητο**, τα δε στοιχεία του **γράμματα** ή **χαρακτήρες**.

Μια πεπερασμένη ακολουθία χαρακτήρων από το αλφάβητο $\mathbb{A}$ θα ονομάζεται **στοιχειοσειρά** ή **λέξη**. Μια λέξη συνήθως θα τη συμβολίζουμε με ένα έντονο γράμμα του λατινικού αλφάβητου.

Παράδειγμα 1.2.1. Έστω $\mathbb{A} = \{ 2, a, d, \diamond \}$, τότε τα $\mathbf{a} = a2d2aa$, $\mathbf{b} = d \diamond 2$, $\mathbf{c} = a$ είναι μερικές λέξεις που σχηματίζονται με χαρακτήρες από το αλφάβητο $\mathbb{A}$.

Το σύνολο όλων των λέξεων που μπορούμε να σχηματίσουμε με τους χαρακτήρες από ένα αλφάβητο $\mathbb{A}$ είναι άπειρο (γιατί;) και συμβολίζεται με $\mathbb{A}^*$.

Το πλήθος των χαρακτήρων σε μια λέξη $\mathbf{u} \in \mathbb{A}^*$ ονομάζεται **μήκος** και συμβολίζεται με $\ell(\mathbf{u})$. Στο προηγούμενο παράδειγμα, οι λέξεις κατά σειρά έχουν μήκη $\ell(\mathbf{a}) = 6$, $\ell(\mathbf{b}) = 3$ και $\ell(\mathbf{u}) = 1$, αντίστοιχα.

Κάνουμε την παραδοχή ότι στο σύνολο $\mathbb{A}^*$ ανήκει και η *κενή* λέξη, δηλαδή η λέξη που δεν περιέχει κανέναν χαρακτήρα, η οποία συνήθως συμβολίζεται με $\boldsymbol{\vartheta}$. Το μήκος της κενής λέξης προφανώς ισούται με μηδέν ($\ell(\boldsymbol{\vartheta}) = 0$).

Έστω $\mathbf{u}, \mathbf{v} \in \mathbb{A}^*$ δύο λέξεις. Τότε, με την **παράθεση** των δύο λέξεων τη μια δίπλα στην άλλη σχηματίζεται μια άλλη λέξη $\mathbf{z} = \mathbf{uv} \in \mathbb{A}^*$. Προφανώς $\ell(\mathbf{z}) = \ell(\mathbf{u}) + \ell(\mathbf{v})$.

Έστω n ένας φυσικός αριθμός. Με $\mathbb{A}^n$ θα συμβολίζουμε το σύνολο όλων των λέξεων με χαρακτήρες από το αλφάβητο $\mathbb{A}$, οι οποίες έχουν μήκος n. Προφανώς, επειδή το $\mathbb{A}$ είναι πεπερασμένο, το σύνολο $\mathbb{A}^n$ είναι πεπερασμένο. Μάλιστα ισχύει $\mid \mathbb{A}^n \mid = \mid \mathbb{A} \mid^n$ (γιατί;)

Πολλές φορές, όταν αναφερόμαστε (μόνο) στα στοιχεία του $\mathbb{A}^n$, αντί για λέξεις τα ονομάζουμε **διανύσματα**.

Ορισμός 1.2.2. *Έστω* $\mathbf{x} = a_1 a_2 \cdots a_n, \mathbf{y} = b_1 b_2 \cdots b_n \in \mathbb{A}^n$. *Ορίζουμε την απεικόνιση* $d : \mathbb{A}^n \times \mathbb{A}^n \longrightarrow \mathbb{Z}$ *ως εξής*

$$d(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{n} r_i, \quad \text{όπου } r_i = \begin{cases} 0 & \text{αν } a_i = b_i \\ 1 & \text{αν } a_i \neq b_i \end{cases} .$$

Ο (μη αρνητικός) ακέραιος αριθμός $d(\mathbf{x}, \mathbf{y})$ *ονομάζεται* ***(Hamming) απόσταση*** *των δύο λέξεων* $\mathbf{x}$ *και* $\mathbf{y}$.

Δηλαδή η απόσταση $d(\mathbf{x}, \mathbf{y})$ παριστά το πλήθος των θέσεων στις οποίες οι δύο λέξεις $\mathbf{x}$ και $\mathbf{y}$ διαφέρουν.

Για παράδειγμα για τις λέξεις $\mathbf{a} = 2df3g4$ και $\mathbf{b} = 35fh24$ η μεταξύ τους απόσταση είναι ίση με 4. [Προφανώς η απόσταση δύο λέξεων δεν υπερβαίνει το (κοινό) μήκος τους.]

Θεώρημα 1.2.3. *Η απεικόνιση* d *είναι μια μετρική στο σύνολο* $\mathbb{A}^n$, *δηλαδή για* $\mathbf{x}, \mathbf{y}$ *και* $\mathbf{z} \in \mathbb{A}^n$ *ισχύει:*

1. $d(\mathbf{x}, \mathbf{y}) \geq 0$, *με* $d(\mathbf{x}, \mathbf{y}) = 0$ *αν και μόνο αν* $\mathbf{x} = \mathbf{y}$.
2. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.
3. $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Απόδειξη. Η απόδειξη είναι αμέση συνέπεια του ορισμού και αφίεται ως άσκηση. ό.έ.δ.[1]

[1] όπερ έδει δείξαι

Παρατήρηση 1.2.4. Όλοι έχουμε υπόψη τη γνωστή Ευκλείδεια απόσταση στον χώρο $\mathbb{R}^n$, όπου $\mathbb{R}$ είναι το σύνολο των πραγματικών αριθμών.

Εδώ η έννοια της απόστασης, που ορίσαμε προηγουμένως, είναι θεμελιώδης για τα επόμενα, όπου, επιλέγοντας κατάλληλο αλφάβητο $\mathbb{A}$, μπορούμε να κάνουμε αντίστοιχη *Γεωμετρία*.

Ορισμός 1.2.5. *Έστω $\mathbb{A}$ ένα αλφάβητο. Κάθε μη κενό υποσύνολο $\mathcal{C}$ του $\mathbb{A}^*$ ονομάζεται* ***κώδικας*** *επί του αλφάβητου $\mathbb{A}$ και τα στοιχεία του* ***(κωδικο)λέξεις.***

Πολλές φορές, όταν δεν υπάρχει το ενδεχόμενο σύγχυσης, τα στοιχεία ενός κώδικα τα αναφέρουμε και αυτά ως λέξεις, αντί για (κωδικο)λέξεις.

Ο ορισμός που μόλις δώδαμε είναι απλούστατος στη διατύπωσή του, αλλά πολύ γενικός. Στα επόμενα, θα δούμε τι περιορισμοί τίθενται στην επιλογή ενός *κατάλληλου* κώδικα.

Ας αρχίσουμε με την επιλογή του αλφάβητου. Θεωρητικά κάθε πεπερασμένο μη κενό σύνολο μπορεί να θεωρηθεί ως αλφάβητο. Για μια όμως συστηματική μελέτη και ενασχόληση με τους κώδικες 'επιβάλλεται' η επιλογή του αλφάβητου να μην είναι τυχαία. Συνήθως, επιλέγουμε ως αλφάβητο ένα πεπερασμένο σώμα $\mathbb{F}$. Η επιλογή αυτή μας δίνει το πλεονέκτημα να χρησιμοποιήσουμε τις γνώσεις μας απο τα Μαθηματικά για την κατασκευή 'καλών' κωδίκων. (Το τι σημαίνει καλός κώδικας θα μας δοθεί η ευκαιρία να το διευκρινίσουμε στα επόμενα).

Ένας κώδικας επί του αλφάβητου $\mathbb{Z}_2$ ονομάζεται **δυαδικός** κώδικας και γενικά επί του $\mathbb{Z}_p$ ονομάζεται **p-αδικός** κώδικας .

1.2.1 Κωδικοποίηση - Αποκωδικοποιήση

Άμεσα συνδεδεμένη με έναν κώδικα είναι η διαδικασία της κωδικοποίησης και αποκωδικοποίησης.

Έστω $S = \{a_1, a_2, ..., a_s\}$ ένα πεπερασμένο σύνολο το οποίο ονομάζουμε **πηγή** και $\mathcal{C}$ ένας κώδικας. Μια συνάρτηση **κωδικοποίησης** είναι μια συνάρτηση $f : S \longrightarrow \mathcal{C}$ η οποία είναι 1-1 και επί.

Η διαδικασία **κωδικοποίησης** συνίσταται, εφόσον είναι γνωστά τα σύνολα S και $\mathcal{C}$, στην επιλογή και εφαρμογή της συνάρτησης f.

Παραδείγματα 1.2.6. 1. Έστω ως πηγή $S = \{\alpha, \beta, \gamma, \dots, \psi, \omega\}$, το σύνολο των γραμμάτων του Ελληνικού αλφάβητου και ως κώδικας $\mathcal{C} = \{00, 01, \dots, 23\}$, το σύνολο των διψηφίων αριθμών από το 00 έως και το 23. Μια συνάρτηση κωδικοποίησης είναι η $f(\alpha) = 00$, $f(\beta) = 01$, $f(\gamma) = 02$, $\dots$, $f(\psi) = 22$, $f(\omega) = 23$.

Για παράδειγμα το 'πηγαίο μήνυμα' *αγαπη* θα κωδικοποιηθεί ως:

$$0002001607.$$

2. Ο κώδικας ASCII $\mathcal{C}$ είναι ένας δυαδικός κώδικας που περιλαμβάνει όλους τους αριθμούς από το 0 έως και το 127, αλλά εκφρασμένους ως επταψήφιους αριθμούς στο δυαδικό σύστημα. Δηλαδή $\mathcal{C} = \mathbb{Z}_2^7$. Η πηγή αποτελείται από όλα τα γράμματα του Λατινικού αλφάβητου (κεφαλαία και πεζά), από τα σημεία στίξης, καθώς επίσης και από διάφορους χαρακτήρες ελέγχου (σύνολον 128 χαρακτήρες). Υπάρχει μια συνάρτηση η οποία κωδικοποιεί καθέναν από τους 128 χαρακτήρες σε έναν επταψήφιο δυαδικό αριθμό. Στον πίνακα 1.1 παρουσιάζεται (μερικώς) η κωδικοποίηση του Λατινικού αλφάβητου στον δυαδικό κώδικα ASCII.

Η **αποκωδικοποίηση** συνίσταται στην αντίστροφη διαδικασία. Επειδή η συνάρτηση κωδικοποίησης, έστω f, είναι 1-1 και επί υπάρχει η αντίστροφή της f^{-1}. Οπότε όταν έχουμε μια (κωδικο)λέξη, δεν έχουμε παρά να εφαρμόσουμε την f^{-1} και να βρούμε το στοιχείο της πηγής στο οποίο αντιστοιχεί η δοθείσα (κωδικο)λέξη.

Για παράδειγμα το κωδικοποιημένο, στον κώδικα ASCII, μήνυμα:

$$1001100100111110101101000110$$

αποκωδικοποιείται, με τη βοήθεια του πίνακα, ως LOVE.

Παρατήρηση 1.2.7. Η απαίτηση να είναι η συνάρτηση κωδικοποίησης 1-1 και επί είναι πολύ σημαντική, καθότι μόνο τότε η αποκωδικοποίηση μπορεί να

A $\rightarrow$ 1000001	$J \rightarrow$ 1001010	$S \rightarrow$ 1010011
$B \rightarrow$ 1000010	$K \rightarrow$ 1001011	$T \rightarrow$ 1010100
$C \rightarrow$ 1000011	$L \rightarrow$ 1001100	$U \rightarrow$ 1010101
$D \rightarrow$ 1000100	$M \rightarrow$ 1001101	$V \rightarrow$ 1010110
$E \rightarrow$ 1000101	$N \rightarrow$ 1001110	$W \rightarrow$ 1010111
$F \rightarrow$ 1000110	$O \rightarrow$ 1001111	$X \rightarrow$ 1011000
$G \rightarrow$ 1000111	$P \rightarrow$ 1010000	$Y \rightarrow$ 1011001
$H \rightarrow$ 1001000	$Q \rightarrow$ 1010001	$Z \rightarrow$ 1011010
$I \rightarrow$ 1001001	$R \rightarrow$ 1010010	$Space \rightarrow$ 0100000

Πίνακας 1.1: η κωδικοποίηση του Λατινικού αλφάβητου στον δυαδικό κώδικα ASCII.

είναι αποτελεσματική. Ας δούμε το εξής απλό παράδειγμα. Υποθέτουμε ότι ως πηγή έχουμε το σύνολο $S = \{\, a \in \mathbb{Z} \mid -10 \leq a \leq 10 \,\}$ και ως κώδικα το σύνολο $\mathcal{C} = \{\, a \in \mathbb{Z} \mid 0 \leq a \leq 100 \,\}$. 'Κωδικοποιούμε' κάθε στοιχείο της πηγής S με το τετραγωνό του, δηλαδή έχουμε την συνάρτηση $f : S \longrightarrow \mathcal{C}$ με $f(x) = x^2$. Τότε, αν πάρουμε τον αριθμό 4 ως (κωδικο)λέξη, επειδή η f δεν είναι 1-1, κατά την 'αποκωδικοποίηση' έχουμε πρόβλημα, καθότι δεν γνωρίζουμε αν το 'πηγαίο μήνυμα' ήταν το 2 ή το -2. Επίσης, επειδή η f δεν είναι επί, υπάρχουν (κωδικο)λέξεις οι οποίες δεν είναι εικόνα (μέσω της f) κανενός στοιχείου της πηγής, οπότε αυτές οι λέξεις 'περιττεύουν'.

Δεν αρκεί όμως μόνο η απαίτηση η συνάρτηση κωδικοποίησης να είναι 1-1 και επί. Ας επανέλθουμε στα προηγούμενα παραδείγματα.

Στο πρώτο παράδειγμα, υποθέτουμε ότι ο κώδικας μας δεν είναι ο $\mathcal{C} = \{\, 00, 01, \ldots, 23 \,\}$, αλλά ο $\bar{\mathcal{C}} = \{\, 0, 1, \ldots, 23 \,\}$. Αν συνάρτηση κωδικοποίησης είναι η $\bar{f}(\alpha) = 0$, $\bar{f}(\beta) = 1$, $\bar{f}(\gamma) = 2, \ldots, \bar{f}(\psi) = 22$, $\bar{f}(\omega) = 23$, τότε η ακολουθία χαρακτήρων 0002001607 θα μπορούσε να προέρχεται από περισσότερα του ενός 'πηγαία μηνύματα'. Πράγματι, ενδέχεται να έχουμε *αααγαβηαθ*, αλλά και *αααφαραθ ή αααφαβηαθ*. Το πρόβλημα που προκύπτει στην περίπτωση αυτή οφείλεται στο γεγονός ότι οι (κωδικο)λέξεις στον κώδικα $\bar{\mathcal{C}}$

δεν έχουν όλες το ίδιο μήκος.

Στο δεύτερο παράδειγμα οι κωδικολέξεις έχουν όλες μήκος 7. Εδώ όμως το γράμμα Ε, που χρησιμοποιείται συχνότατα, 'απαιτεί' τον ίδιο χρόνο και χώρο, για να κωδικοποιηθεί, με το γράμμα Q, που συναντάται σπανιώτατα.

Ορισμός 1.2.8. *Ένας κώδικας $\mathcal{C}$ ονομάζεται κώδικας **σταθερού μήκους** αν όλες οι (κωδικο)λέξεις έχουν το ίδιο μήκος, δηλαδή υπάρχει ένας θετικός ακέραιος αριθμός n, έτσι ώστε $\mathcal{C} \subseteq \mathbb{A}^n$. Ο αριθμός n ονομάζεται **μήκος** του κώδικα . Διαφορετικά ο κώδικας ονομάζεται **μεταβλητού μήκους**.*

Ανάλογα με το αν ένας κώδικας είναι σταθερού ή μεταβλητού μήκους, όπως έχουμε επισημάνει, παρουσιάζει πλεονεκτήματα και μειονεκτήματα.

Παρατήρηση 1.2.9. Το κύριο μειονέκτημα ενός κώδικα μεταβλητού μήκους, όπου δεν μπορούμε να γνωρίζουμε κατά την κωδικοποίηση πού τελειώνει μια (κωδικο)λέξη και πού αρχίζει η επόμενη, αντιμετωπίζεται, συνήθως, χρησιμοποιώντας έναν *διαχωριστή* λέξεων ως εξής. Στην πηγή επισυνάπτουμε ένα επιπλέον στοιχείο (π.χ. το $\cdot$), στον κώδικα ένα επιπλέον στοιχείο (τον διαχωριστή λέξεων /) και ορίζουμε $f(\cdot) = /$, όπου f είναι η συνάρτηση κωδικοποίησης. Κατά την κωδικοποίηση, για την δημιουργία ενός κωδικοποιημένου μηνύματος, πάντα μεταξύ δύο (κωδικο)λέξεων (διαφορετικών της /) παρεμβάλουμε την /.

Επομένως, αν στο προηγούμενο παράδειγμα αντί της ακολουθίας χαρακτήρων 0002001607 είχαμε την ακολουθία $0/0/0/20/0/16/0/7$, κατά την αποκωδικοποίηση θα γνωρίζαμε μετά βεβαιότητος (αγνοώντας το στοιχείο $\cdot$) ότι αυτή προέρχεται από το πηγαίο μήνυμα *αααφαραθ*.

Προφανώς, η επιλογή μιας τέτοιας τακτικής επιφέρει και την αντίστοιχη 'επιβάρυνση' στην όλη διαδικασία, καθότι αυξάνει το μέγεθος του κωδικοποιημένου μηνύματος.

Στα επόμενα, εμείς θα ασχοληθούμε με κώδικες σταθερού μήκους επί ενός πεπερασμένου σώματος $\mathbb{F}$. Επομένως, ένας κώδικας θα χαρακτηρίζεται, προς το παρόν από τις εξής παραμέτρους: Το αλφάβητο (το σώμα $\mathbb{F}$), το μήκος n και το μέγεθος του $M = \mid \mathcal{C} \mid$. Μάλιστα για συντομία θα αναφέρεται ως ένας (n, M) κώδικας.

Ένα άμεσο πλεονέκτημα της χρήσης ενός κώδικα σταθερού μήκους επί ενός πεπερασμένου σώματος $\mathbb{F}$ είναι ότι το σύνολο $\mathbb{F}^n$ όλων των λέξεων μήκους n είναι διανυσματικός χώρος. Επομένως, μπορούμε να χρησιμοποιήσουμε τις ιδιότητες ενός διανυσματικού χώρου στη μελέτη των κωδίκων. Προς το παρόν αναφέρουμε έναν ορισμό και μια πρόταση πολύ σημαντική για τα επόμενα.

Ορισμός 1.2.10. *Έστω* $\mathbf{a} \in \mathbb{A}^n$ *(*$\mathbb{A} = \mathbb{F}$*). Η απόσταση της* $\mathbf{a}$ *από τη μηδενική λέξη* $\mathbf{0} = (0, 0, \ldots, 0)$ *ονομάζεται* ***βάρος*** *της* $\mathbf{a}$ *και συμβολίζεται με* $w(\mathbf{a})$*. Δηλαδή* $w(\mathbf{a}) = d(\mathbf{a}, \mathbf{0})$*.*

Διαφορετικά, το βάρος μιας λέξης παριστά τον αριθμό των μη μηδενικών χαρακτήρων της.

Έστω $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}^n$. Ορίζουμε ως **τομή** των $\mathbf{a}$ και $\mathbf{b}$ το εξής στοιχείο του $\mathbb{F}^n$:

$$\mathbf{a} \cap \mathbf{b} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Δηλαδή η λέξη $\mathbf{a}$ έχει μη μηδενινό στοιχείο σε μια θέση, αν και μόνο αν και η $\mathbf{a}$ και η $\mathbf{b}$ έχουν μη μηδενινό στοιχείο στην αντίστοιχη θέση.

Στην περίπτωση όπου το αλφάβητο είναι το δυαδικό ($\mathbb{F} = \mathbb{Z}_2$), ορίζουμε ως **υπόβαθρο** της λέξης $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_2^n$ το σύνολο των θέσεων όπου η λέξη $\mathbf{a}$ έχει 1. Επίσης, θα λέμε ότι η λέξη $\mathbf{a}$ **καλύπτει** την λέξη $\mathbf{b}$ αν ισχύει $\mathbf{a} \cap \mathbf{b} = \mathbf{b}$. Δηλαδή το υπόβαθρο της $\mathbf{b}$ είναι υποσύνολο του υπόβαθρου της $\mathbf{a}$. Με άλλα λόγια, στις θέσεις όπου η $\mathbf{b}$ έχει 1, η $\mathbf{a}$ έχει οπωσδήποτε και αυτή 1.

Πρόταση 1.2.11. *1. Για* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}^n$ *ισχύει:*

(α΄) $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b})$*.*

(β΄) $d(\mathbf{a} + \mathbf{c}, \mathbf{b} + \mathbf{c}) = d(\mathbf{a}, \mathbf{b})$*.*

2. Στην περίπτωση όπου $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$*, τότε* $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} + \mathbf{b}) = w(\mathbf{a}) + w(\mathbf{b}) - 2w(\mathbf{a} \cap \mathbf{b})$*.*

Μάλιστα δε η λέξη $\mathbf{a}$ *καλύπτει την λέξη* $\mathbf{b}$*, αν και μόνο αν* $w(\mathbf{a} + \mathbf{b}) = w(\mathbf{a}) - w(\mathbf{b})$*, αν και μόνο αν* $w(\mathbf{a} \cap \mathbf{b}) \geq w(\mathbf{b})$*.*

Όπου οι πράξεις της πρόσθεσης και αφαίρεσης είναι οι γνωστές πράξεις κατά συντεταγμένες στον διανυσματικό χώρο $\mathbb{F}^n$.

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια των ορισμών και αφίεται ως άσκηση. ό.έ.δ.

Κατά την κωδικοποίηση ενός (πηγαίου) μηνύματος, όπως έχουμε πει, εφαρμόζεται η συνάρτηση κωδικοποίησης. Κατόπιν, το κωδικοποιημένο μήνυμα αποστέλλεται κάπου, χρησιμοποιώντας γραμμές τηλεφώνου, ηλεκτρομαγνητικά κύμματα κ.λ.π.. Επίσης μπορεί να αποθηκευθεί σε μαγνητοταινίες, σε δίσκους ακτίνας, στη μνήμη ενός υπολογιστή κ.λ.π. Για την αποκωδικοποιήση ακολουθείται η αντίστροφη διαδικασία, δηλαδή εφαρμόζεται η αντίστροφη συνάρτηση της συνάρτησης κωδικοποίησης.

Σε ιδανικές περιπτώσεις δεν θα είχαμε **κανένα** πρόβλημα. Αρκούσε ο **αποστολέας** να γνωρίζει τον 'τύπο' της συνάρτησης κωδικοποίησης και ο **παραλήπτης**[2] να γνωρίζει τον 'τύπο' της αντίστροφης συνάρτησης. Στην πραγματικότητα όμως η κατάσταση είναι τελείως διαφορετική. Κατά τη 'διαχείριση' του κωδικοποιημένου μηνύματος (αποστολή, αποθήκευση κ.λ.π.) επέρχονται αλλοιώσεις στις (κωδικο)λέξεις,[3] οπότε η εφαρμογή της αντίστροφης συνάρτησης κωδικοποίησης όχι μόνο δεν προσφέρει, αλλά μπορεί να οδηγήσει σε 'στρεβλώσεις'.

Ένας από τους κύριους σκοπούς της Θεωρίας Κωδικών είναι η αντιμετώπιση τέτοιων καταστάσεων. Στην επόμενη παράγραφο θα προσπαθήσουμε να αντιμετωπίσουμε αυτό το πρόβλημα πιο συστηματικά. Προς το παρόν αρκούμαστε να δώσουμε δύο παραδείγματα (πραγματικών) προβλημάτων.

1. Κατά τις πρώτες αποστολές διαστημοπλοίων στο διάστημα για να μεταδοθούν οι (ασπρόμαυρες) φωτογραφίες των πλανητών στη Γη είχε επινοηθεί η εξής απλή, αλλά πολύ ευφυής στη σύλληψή της, μέθοδος. Κάθε φωτογραφία χωριζόταν σε μικρότερα τετράγωνα (π.χ. σε ένα πλέγμα με m γραμμές

[2] Οι λέξεις αποστολέας και παραλήπτης θα χρησιμοποιούνται με την ευρεία έννοια του όρου είτε πρόκειται για πρόσωπα είτε πρόκειται για μηχανές.

[3] Εδώ δεν θα ασχοληθούμε με τα αίτια που προκαλούν τις αλλοιώσεις είτε αυτές είναι σκόπιμες είτε οφείλονται σε τεχνικές ατέλειες κ.λ.π.

και n στήλες), οι διάφορες αποχρώσεις του γκρίζου χρώματος κατατάχθηκαν σε 64 διαβαθμίσεις (από το 0 για το άσπρο έως το 63 για το μαύρο). Κάθε αριθμός μετετράπη στην αντίστοιχη δυαδική έκφραση ($0 = 000000, 1 = 000001, \ldots, 63 = 111111$),[4] οπότε για τη μετάδοση της φωτογραφίας εγίνετο (με προκαθορισμένη σειρά) μια σάρωση των επιμέρους τετραγώνων και ανάλογα με τον βαθμό αμαυρώσεως απεστέλλετο η αντίστοιχη εξάδα των 0 και 1. Οι αποδέκτες στη Γη δεν είχαν παρά, ανάλογα με την εξάδα που ελαμβάνετο, να βρούν την αντίστοιχη απόχρωση του γκρίζου και να αναπαράγουν τη φωτογραφία σύμφωνα με την προκαθορισμένη σειρά σάρωσης.

Όλα αυτά θα συνέβαιναν στην ιδανική περίπτωση όπου δεν θα επέρχονταν αλλοιώσεις κατά τη μετάδοση των εξάδων. Αρκούσε όμως η αλλαγή ενός χαρακτήρα από 0 σε 1 (και αντίστροφα), οπότε η εξάδα αντιστοιχούσε σε διαφορετική απόχρωση με αποτέλεσμα να μην έχουμε πιστή αναπαραγωγή της φωτογραφίας.

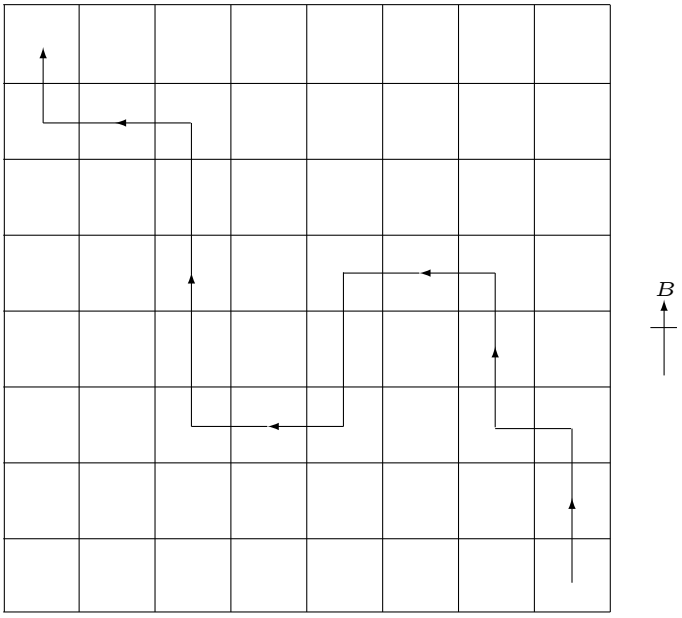
Το πρόβλημα αυτό αντιμετωπίστηκε ως εξής: Οι 64 εξάδες κωδικοποιήθηκαν σε (κωδικο)λέξεις μήκους 32, οι οποίες αποτελούνταν από 0 και 1, κατά τέτοιο τρόπο ώστε όταν απεστέλετο μια 32-άδα, θα μπορούσε να επέλθει αλλοίωση (μέχρι και) σε επτά το πλήθος χαρακτήρες, αλλά να αποδίδεται σωστά η πραγματική απόχρωση. (Στα επόμενα, δες στη σελίδα 257, θα μας δοθεί η ευκαιρία να δούμε πώς έγινε αυτή η κωδικοποίηση). Βέβαια δεν πρέπει να ξεχνάμε το 'κόστος' αυτής της κωδικοποίησης, το οποίο μεταφράζεται σε χρόνο μετάδοσης και σε απαίτηση μνήμης.

2. Υποθέτουμε ότι ένα πλοίο θέλει να διαπλεύσει ανάμεσα σε επικίνδυνες ακτές και ζητά τη βοήθεια των τοπικών λιμενικών αρχών. Ο κυβερνήτης και ο λιμενάρχης έχουν ακριβώς ίδιους χάρτες της περιοχής, αλλά η ασφαλής πορεία είναι χαραγμένη μόνο στον χάρτη του λιμενάρχη, ο οποίος αναλαμβάνει να δώσει οδηγίες. Επειδή δεν είναι δυνατόν να δίνονται φωνητικές οδηγίες της μορφής '*...πήγαινε προς Βορράν, μετά προς Δυσμάς...*', ο τρόπος επικοινωνίας γίνεται μέσω ενός μέσου, όπου μπορούν να μεταδοθούν μόνο τα

[4] Η ίδια ιδέα εφαρμόζεται και σήμερα στις ψηφιακές φωτογραφίες, μόνο που τώρα (για να πετύχουμε υψηλή πιστότητα και ευκρίνεια) δεν χρησιμοποιούμε 64 αποχρώσεις του γκρίζου, αλλά τουλάχιστον $2^{16} = 65536$ αποχρώσεις όλων των χρωμάτων.

σύμβολα 0 και 1. Τότε έχουμε μια πηγή: $S = \{$ **Α**νατολή, **Δ**ύση, **Β**ορράς, **Ν**ότος $\}$, έναν κώδικα $\mathcal{C} = \{\, 00, 01, 10, 11 \,\}$ και μια συνάρτηση κωδικοποίησης $f : S \longrightarrow \mathcal{C}$ με $f(\mathbf{A}) = 00$, $f(\mathbf{\Delta}) = 01$, $f(\mathbf{B}) = 10$, $f(\mathbf{N}) = 11$. Ο κώδικας αυτός είναι με το μικρότερο δυνατόν μήκος, καθότι για την μετάδοση ενός στοιχείου από την πηγή S αρκούν δύο χαρακτήρες. Κατά συνέπεια, είναι 'γρήγορος και οικονομικός'.

Ο λιμενάρχης για να περιγράψει τη χαραγμένη πορεία (βλέπε σχήμα 1.1) πρέπει να μεταδώσει κωδικοποιημένο το εξής (πηγαίο) μήνυμα ΒΒΔΒΒΔ-ΔΝΝΔΔΒΒΒΒΔΔΒ. Δηλαδή μεταδίδει το μήνυμα 10 10 01 10 ... . Ο κυβερνήτης δεν έχει παρά να αποκωδικοποιήσει το μήνυμα που λαμβάνει εφαρμόζοντας την αντίστροφη συνάρτηση f^{-1} και να πορευθεί αναλόγως.



Σχήμα 1.1: Ασφαλής πορεία του πλοίου.

Σε ιδανικές συνθήκες μετάδοσης/λήψης δεν υπάρχει πρόβλημα. Όμως στην πράξη, η αλλαγή ενός χαρακτήρα από 0 σε 1 (και αντίστροφα) μπορεί να οδηγήσει σε λάθος πορεία και να εκθέσει σε κίνδυνο το πλοίο. Επειδή η ασφάλεια προέχει, πρέπει να επινοηθεί ένας άλλος 'ασφαλέστερος' κώδικας, ακόμα και αν είναι πιο 'απαιτητικός' σε χρόνο και μνήμη.

Υποθέτουμε ότι αντί του κώδικα $\mathcal{C}$ έχουμε τον κώδικα:

$$\mathcal{D} = \{\, 000,\, 011,\, 101,\, 110 \,\}$$

και συνάρτηση κωδικοποίησης $g : S \longrightarrow \mathcal{D}$ με $g(\mathbf{A}) = 000$, $g(\mathbf{\Delta}) = 011$, $g(\mathbf{B}) = 101$, $g(\mathbf{N}) = 110$. Παρατηρούμε ότι ο κώδικας $\mathcal{D}$ προέρχεται από τον προηγούμενο κώδικα επισυνάπτοντας ένα επιπλέον ψηφίο με τέτοιον τρόπο, ώστε ο αριθμός των 1 που εμφανίζονται σε κάθε (κωδικο)λέξη να είναι πάντα άρτιος. Αν κατά τη μετάδοση μιας τριάδας χαρακτήρων (μιας (κωδικο)λέξης) επέλθει 'αλλοίωση' ενός χαρακτήρα, τότε η τριάδα που λαμβάνει ο κυβερνήτης του πλοίου δεν αντιστοιχεί σε καμία (κωδικο)λέξη (γιατί;) και αντιλαμβάνεται ότι πρόκειται περί λάθους. Δηλαδή έχει 'ανιχνευθεί' λάθος, οπότε (αν υπάρχει δυνατότητα) ζητά την επανάληψη της αποστολής της συγκεκριμένης (κωδικο)λέξης.

Πολλές φορές όμως δεν είναι δυνατή η επικοινωνία του κυβερνήτη (παραλήπτη) με τον λιμενάρχη (αποστολέα) για να ζητηθούν διευκρινίσεις.[5] Τότε είναι αναγκαίο να 'επιστρατευθεί' ένας κώδικας ο οποίος να είναι περισσότερο 'αποτελεσματικός'. Θα δούμε πώς αντιμετωπίζεται αυτό το πρόβλημα στα επόμενα (βλέπε Παράδειγμα 1.3.8$_2$).

1.2.2 Το πρόβλημα της αποκωδικοποίησης

Έστω ότι επικοινωνούμε μέσω ενός κώδικα $\mathcal{C} \subseteq \mathbb{F}^n$ (στο εξής, όπως έχουμε προείπει, εκτός και αν το δηλώνουμε ρητά, το αλφάβητο ενός κώδικα θα είναι ένα πεπερασμένο σώμα $\mathbb{F}$). Όταν αποστέλλεται μία (κωδικο)λέξη, έστω $\mathbf{a}$, ενδέχεται, όπως έχουμε επισημάνει, να λάβουμε μια άλλη λέξη $\mathbf{b}$. Η *διαφορά* $\mathbf{e} = \mathbf{b} - \mathbf{a} \in \mathbb{F}^n$[6] λέγεται **διάνυσμα λάθους** ή απλώς **λάθος** που παρέσφρησε

[5] Η περίπτωση μη δυνατότητας επικοινωνίας παραλήπτη με αποστολέα είναι η πιο συνήθης. Για παράδειγμα, είναι δύσκολο να ζητηθεί η επανάληψη της αποστολής μιας φωτογραφίας από το διάστημα. Όπως είναι αδύνατον, όταν θέλουμε να αναπαράγουμε το αποθηκευμένο υλικό μιας μαγνητοταινίας, να ζητήσουμε την επαναποθήκευσή του, όταν παρουσιάζονται προβλήματα σωστής αναπαργωγής.

[6] Ως αλφάβητο $\mathbb{A}$ έχει επιλεγεί το σώμα $\mathbb{F}$, οπότε η διαφορά ορίζεται ως αφαίρεση κατά συνταταγμένες.

(υπεισήλθε) κατά τη μετάδοση. (Ορισμένες φορές τα λάθη αναφέρονται ως **παράσιτα** ή ως **θόρυβοι**.)

Για παράδειγμα, σε έναν 5-δικό κώδικα μήκους 4, αν εστάλη η λέξη $\mathbf{a} = 2034$ και ελήφθη η λέξη $\mathbf{b} = 3021$, τότε το λάθος είναι $\mathbf{e} = 1042$. Όπως βλέπουμε, στις θέσεις του λάθους, όπου εμφανίζονται μη μηδενικές συντεταγμένες, στις αντίστοιχες θέσεις της αρχικής λέξης έχει επέλθει *αλλοίωση* του αντίστοιχου χαρακτήρα. Τις περισσότερες φορές δεν μας ενδιαφέρει τί είδους αλλοίωση έχει προκληθεί σε έναν χαρακτήρα, αλλά απλώς αν έχει ή δεν έχει επέλθει αλλοίωση ενός χαρακτήρα. Οπότε σαν λάθος εννοούμε ένα διάνυσμα $\boldsymbol{\epsilon} \in \mathbb{A}^n$, το οποίο έχει 1 στις θέσεις όπου έχει επέλθει αλλοίωση του χαρακτήρα και 0 στις υπόλοιπες θέσεις. Στο προηγούμενο παράδειγμα έχουμε $\boldsymbol{\epsilon} = 1011$.

Όπως παρατηρούμε $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{e}) = w(\boldsymbol{\epsilon})$. Επίσης, αν ο κώδικας $\mathcal{C}$ είναι δυαδικός, τότε $\mathbf{e} = \boldsymbol{\epsilon}$.

Το μεγάλο πρόβλημα στην αποκωδικοποίηση είναι η εύρεση μιας διαδικασίας, η οποία να αποφαίνεται, όταν λαμβάνεται μια λέξη, κατά πόσο αυτή η λέξη εμπεριέχει λάθη. Πολύ δε περισσότερο να αποφασίζει ποία (κωδικο)λέξη εστάλη. Μια τέτοια διαδικασία προφανώς εξαρτάται, κατά κύριο λόγο, από το μέσον που χρησιμοποιείται για τη μετάδοση των μυνημάτων.

Για παράδειγμα: Υποθέτουμε ότι έχουμε τον δυαδικό κώδικα:

$$\mathcal{C} = \{\, 00000,\, 11111 \,\}$$

και ότι λάβαμε τη λέξη 11100, τότε εφαρμόζοντας τη 'λογική' ότι αυτή η λέξη είναι 'πλησιέστερα' προς την (κωδικο)λέξη 11111, δεχόμαστε ότι η λέξη που εστάλη είναι η λέξη 11111. Αν όμως κάνουμε την παραδοχή ότι το μέσον μετάδοσης που διαθέτουμε αλλοιώνει πάντα τον πρώτο χαρακτήρα κάθε λέξης που στέλνεται, τότε η λέξη 11100 που λάβαμε είναι 'πλησιέστερα' προς την (κωδικο)λέξη 00000. Επίσης, ενδέχεται σε διαφορετικές χρονικές στιγμές να έχουμε διαφορετικό τρόπο μετάδοσης του ιδίου χαρακτήρα. Επομένως, η φύση του μέσου μετάδοσης καθορίζει κατά κύριο λόγο τον 'κανόνα αποφασισιμότητας' με τον οποίο κάνουμε την αποκωδικοποίηση. Ας γίνουμε πιο συγκεκριμένοι.

Ορισμός 1.2.12. *Ένας* ***δίαυλος επικοινωνίας*** *αποτελείται από ένα αλφάβητο*[7] $\mathbb{A} = \{a_1, a_2, \ldots, a_r\}$, *το ίδιο με το αλφάβητο του κώδικα, και ένα σύνολο πιθανοτήτων:*

$$p_{ij} = p(\textit{ελήφθη ο χαρακτήρας } a_i \mid \textit{ εστάλη ο χαρακτήρας } a_j),$$

το οποίο ικανοποιεί τη σχέση:

$$\sum_{i=1}^{r} p_{ij} = 1$$

για όλα τα j.

Οι πιθανότητες p_{ij} ονομάζονται **πιθανότητες μετάδοσης**.

Εδώ γίνεται η παραδοχή ότι οι πιθανότητες αυτές σε έναν δίαυλο επικοινωνίας δεν αλλάζουν από χρονική σε χρονική στιγμή.

Η προηγούμενη σχέση δηλώνει: Δεδομένου ότι εστάλη ένας χαρακτήρας, πάντα λαμβάνεται ένας χαρακτήρας. Επίσης, παραδεχόμαστε ότι ποτέ δεν λαμβάνεται ένας χαρακτήρας, αν δεν έχει σταλεί (κάποιος) χαρακτήρας. Δηλαδή ένας δίαυλος δεν αυξομειώνει το μήκος μιας ακολουθίας χαρακτήρων που αποστέλεται μέσω αυτού.

Ορισμός 1.2.13. *Ένας δίαυλος θα λέγεται* ***αμνήμων*** *αν η μετάδοση ενός χαρακτήρα είναι ανεξάρτητη από τη μετάδοση προηγουμένων χαρακτήρων.*

Η ιδιότητα αυτή με τη βοήθεια των πιθανοτήτων μετάδοσης μπορεί να περιγραφεί ως εξής: Έστω η (κωδικο)λέξη $\mathbf{c} = c_1\, c_2 \cdots c_n$ και η λέξη $\mathbf{x} = x_1\, x_2 \cdots x_n$. Τότε, η πιθανότητα $p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \mathbf{c})$ είναι ίση με το γινόμενο των πιθανοτήτων μετάδοσης $p(\textit{ελήφθη ο χαρακτήρας } x_i \mid \textit{εστάλη ο χαρακτήρας } c_i)$. Δηλαδή:

$$p(\textit{ελήφθη η } \mathbf{x} \mid \textit{ εστάλη η } \mathbf{c}) = \prod_{i=1}^{n} p(\textit{ελήφθη ο } x_i \mid \textit{εστάλη ο } c_i) \quad (1.1)$$

[7] Γενικά θα μπορούσαμε να υποθέσουμε ότι υπάρχουν δύο αλφάβητα, ένα *εισερχομένων* χαρακτήρων και ένα *εξερχομένων* χαρακτήρων. Η αντιμετώπιση είναι παρόμοια και δεν αποτελεί μεγάλο περιορισμό η υπόθεση ότι υπάρχει κοινό αλφάβητο, τόσο για την είσοδο όσο και για την έξοδο.

Όπως καταλαβαίνουμε ένας 'καλός' δίαυλος είναι ένας δίαυλος, όπου οι πιθανότητες μετάδοσης p_{ij} είναι 'πολύ μικρές' για $i \neq j$ και 'πολύ μεγάλες' για $i = j$. Επομένως, ο $r \times r$ πίνακας $\mathrm{P} = (p_{ij})$, που αποτελείται από τις πιθανότητες μετάδοσης, χαρακτηρίζει τον δίαυλο ως προς την *ποιότητά* του.

Στην ιδανική περίπτωση, όπου $p_{ij} = 0$ για $i \neq j$ (οπότε $p_{ii} = 1$) για όλα τα $i, j = 1, 2, \ldots, r$, έχουμε έναν **αθόρυβο** δίαυλο και δεν θα υπήρχε πρόβλημα αποκωδικοποίησης. (Εδώ ο πίνακας που χαρακτηρίζει τον κώδικα είναι ο ταυτοτικός.)

Τις περισσότερες φορές (χωρίς αυτό να συμβαίνει στην πραγματικότητα) υποτίθεται ότι όλες οι πιθανότητες μετάδοσης p_{ij} για όλα τα $i \neq j$ είναι ίσες μεταξύ τους (άρα και όλες οι πιθανότητες p_{ii} για όλα τα i είναι ίσες μεταξύ τους). Οπότε, αν για έναν δίαυλο έχουμε $p_{ij} = p$, τότε $p_{ii} = 1 - (r-1)p$ (γιατί;). Ένας τέτοιος δίαυλος θα λέγεται **συμμετρικός**. (Καθότι ο πίνακας που χαρακτηρίζει τον δίαυλο είναι συμμετρικός.)

Στην περίπτωση ενός δυαδικού κώδικα μήκους n, που οι (κωδικο)λέξεις μεταδίδονται μέσω ενός συμμετρικού δίαυλου επικοινωνίας, η πιθανότητα να αλλοιωθούν k το πλήθος χαρακτήρες είναι *ίση* με $p^k(1-p)^{n-k}$.

Παρατήρηση 1.2.14. Στον ορισμό ενός δίαυλου επικοινωνίας είχαμε δεχθεί ότι μεταξύ των πιθανοτήτων μετάδοσης ισχύει η σχέση:

$$\sum_{i=1}^{r} p_{ij} = 1$$

για όλα τα j, η οποία δηλώνει, δεδομένου ότι εστάλη ένας χαρακτήρας, πάντα λαμβάνεται ένας χαρακτήρας.

Στην πράξη όμως δεν αποκλείεται το ενδεχόμενο, να έχει σταλεί ένας χαρακτήρας, αλλά κατά τη μετάδοση ο χαρακτήρας να *χαθεί* (προσοχή! εννοούμε απώλεια χαρακτήρα και όχι αλλοίωση). Στην περίπτωση αυτή θα είχαμε μείωση του μήκους της μεταδιδόμενης λέξης, κάτι που θα δημιουργούσε πρόσθετα προβλήματα.

Το ενδεχόμενο αυτό αντιμετωπίζεται (συνήθως) ως εξής: Ως αλφάβητο επικοινωνίας, άρα και αλφάβητο του κώδικα, χρησιμοποιείται το *διευρυμμένο* αλφάβητο $\bar{\mathbb{A}} = \mathbb{A} \cup \{\,?\,\}$, όπου ο χαρακτήρας $?$ δεν αποστέλλεται ποτέ, αλλά εμφανίζεται στη θέση ένος απωλεσθέντος χαρακτήρα. Οπότε για τις πιθανότητες

μετάδοσης έχουμε $p(\textit{ελήφθη ο χαρακτήρας } a_i \mid \textit{εστάλη ο χαρακτήρας } ?) = 0$, $p(\textit{ελήφθη ο χαρακτήρας } ? \mid \textit{εστάλη ο χαρακτήρας } a_j) \geq 0$. Επομένως, για να ισχύει η παραπάνω σχέση, αναγκαστικά έχουμε:

$$p(\textit{ελήφθη ο χαρακτήρας } ? \mid \textit{εστάλη ο χαρακτήρας } ?) = 1 \quad (\text{γιατί;}).$$

1.2.3 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Έστω $\mathbf{a} \in \mathbb{Z}_r^n$. Δείξτε ότι υπάρχουν $\binom{n}{k}(r-1)^k$ το πλήθος λέξεις του $\mathbb{Z}_r^n$, οι οποίες απέχουν απόσταση ίση με k από την $\mathbf{a}$.

3. $i)$ Υποθέτουμε ότι θέλουμε έναν δυαδικό κώδικα σταθερού μήκους που να έχει 126 (κωδικο)λέξεις. Ποίο είναι το μικρότερο δυνατό μήκος για έναν τέτοιο κώδικα;

   $ii)$ Υποθέτουμε ότι θέλουμε έναν δυαδικό κώδικα σταθερού μήκους που να έχει n το πλήθος (κωδικο)λέξεις. Ποίο είναι το μικρότερο δυνατό μήκος για έναν τέτοιο κώδικα;

4. Ποιές συναρτήσεις κωδικοποίησης μπορούμε να ορίσουμε από την πηγή $S = \{\, a, b, c \,\}$ στον κώδικα $\mathcal{C} = \{\, 00, 01, 11 \,\}$;

5. Να υπολογίσετε τον αριθμό των συναρτήσεων κωδικοποίησης από μια πηγή μεγέθους n σε έναν κώδικα μεγέθους n.

6. Να υπολογίσετε τον αριθμό των κωδίκων μήκους n που μπορούμε να ορίσουμε επί ενός αλφάβητου μεγέθους m.

7. Υποθέτουμε ότι έχουμε έναν δυαδικό συμμετρικό δίαυλο επικοινωνίας με πιθανότητα μετάδοσης:

$$\begin{aligned} p &= p(\textit{ελήφθη ο χαρακτήρας } 0 \mid \textit{εστάλη ο χαρακτήρας } 1) \\ &= p(\text{ελήφθη ο χαρακτήρας } 1 \mid \textit{εστάλη ο χαρακτήρας } 0) > \frac{1}{2}. \end{aligned}$$

   Τί πρέπει να κάνουμε;

1.3 Κανόνες Αποκωδικοποίησης

Όπως έχουμε επισημάνει στην προηγουμένη παράγραφο, το μεγάλο πρόβλημα στην αποκωδικοποίηση είναι η εύρεση μιας διαδικασίας, η οποία να αποφαίνεται, όταν λαμβάνεται μια λέξη, κατά πόσο αυτή η λέξη εμπεριέχει λάθη. Πολύ δε περισσότερο να αποφασίζει ποιά λέξη εστάλη.

Στην παράγραφο αυτή θα δούμε πώς αντιμετωπίζεται το πρόβλημα της αποκωδικοποίησης, εφαρμόζοντας κάποιους *κανόνες αποφασισιμότητας*.

Ορισμός 1.3.1. *Έστω $\mathcal{C}$ ένας κώδικας μήκους n με χαρακτήρες από το αλφάβητο $\mathbb{A}$. Ένας κανόνας* ***αποφασισιμότητας*** *είναι μια συνάρτηση $\varphi : \mathbb{A}^n \longrightarrow \mathcal{C} \cup \{?\}$, η οποία αποδέχεται, δεδομένου ότι λάβαμε τη λέξη $\mathbf{x} \in \mathbb{A}^n$, ότι εστάλη η λέξη $\varphi(\mathbf{x})$, αν $\varphi(\mathbf{x}) \in \mathcal{C}$ ή αποφαίνεται ότι πρόκειται για λάθος αν $\varphi(\mathbf{x}) = ?$*[8].

Εδώ πρέπει να επισημάνουμε ότι η συνάρτηση φ, που αναφέρεται στον προηγούμενο ορισμό, είναι το αμέσως προηγούμενο στάδιο πριν την εφαρμογή της αντίστροφης συνάρτησης f^{-1}, όπου f είναι η συνάτρηση κωδικοποίησης που είχαμε ορίσει στην παράγραφο 1.2 στη σελίδα 5.

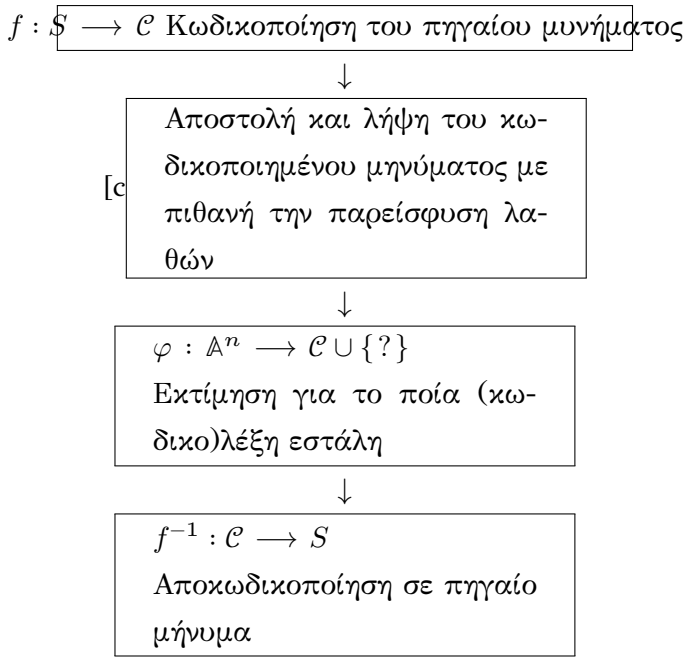
Σχηματικά θα μπορούσαμε το όλο εγχείρημα 'Κωδικοποίηση-Αποστολή-Λήψη-Αποκωδικοποίηση' να το παραστήσουμε όπως φαίνεται στο σχήμα: 1.2.

Παρατηρήσεις 1.3.2.

1. Όπως βλέπουμε η επιλογή και εφαρμογή της συνάρτησης φ αποτελούν πολύ σημαντικά βήματα στην όλη διαδικασία. Για τον λόγο αυτό έχει επικρατήσει, αντί για κανόνα αποφασισιμότητας, να ονομάζουμε τη συνάρτηση φ **συνάρτηση αποκωδικοποίησης** και ως αποκωδικοποίηση να αναφέρεται η διαδικασία εφαρμογής της φ.

2. Λογικό θα ήταν η συνάρτηση f^{-1} να ονομάζεται συνάρτηση αποκωδικοποίησης, ως αντίστροφη της συνάρτησης κωδικοποίησης f και ως αποκωδικοποίηση η εφαρμογή της f^{-1}, όπως άλλωστε αναφέρεται στην παράγραφο 1.2. Μετά όμως από την προηγούμενη παρατήρηση δεν υπάρχει

[8] Το σύμβολο ? δεν σημαίνει ότι η ληφθείσα λέξη $\mathbf{x}$ εμπεριέχει λάθη, αλλά ότι τα λάθη που εμπεριέχει δεν μας επιτρέπουν να αποφανθούμε για το ποιά λέξη εστάλη.



Σχήμα 1.2: Κωδικοποίηση-Αποστολή-Λήψη-Αποκωδικοποίηση.

κίνδυνος σύγχυσης και θα χρησιμοποιούμε τον όρο αποκωδικοποίηση σε ό,τι έχει σχέση με τη συνάρτηση φ.

3. Στην περίπτωση, όπου $\varphi(\mathbf{x}) \in \mathcal{C}$ η διαδικασία συνεχίζεται. Αν $\varphi(\mathbf{x}) = ?$, οπότε αποφαινόμεθα ότι πρόκειται για λάθος, η διαδικασία σταματά και ο δέκτης είτε αγνοεί τη ληφθείσα λέξη είτε (αν είναι δυνατόν) ζητά την επανάληψη της αποστολής της *αμφισβητούμενης/ύποπτης* λέξης.

Έστω ότι έχει σταλεί μια λέξη $\mathbf{c} \in \mathcal{C}$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$. Η αποκωδικοποίηση είναι *σωστή* αν, $\varphi(\mathbf{x}) = \mathbf{c}$. Ενδέχεται όμως να έχει σταλεί η λέξη $\mathbf{a} \in \mathcal{C}$, να έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$ και $\varphi(\mathbf{x}) = \mathbf{b} \in \mathcal{C}$ με $\mathbf{b} \neq \mathbf{a}$. Στην περίπτωση αυτή η αποκωδικοποίηση **δεν** είναι σωστή.

Υπάρχουν πολλοί τρόποι προσδιορισμού της συνάρτησης αποκωδικοποίησης. Εδώ εμείς θα παρουσιάσουμε τους δύο πλέον γνωστούς τρόπους. (Στην πραγματικότητα, όπως θα δούμε, πρόκειται για τις δύο όψεις του *ιδίου νομίσματος*).

1.3.1 Η Αρχή της αποκωδικοποίησης μέγιστης πιθανότητας

Έστω ότι ο κώδικας $\mathcal{C}$ αποτελείται από τις (κωδικο)λέξεις $\mathbf{c}_i$, $i = 1, \ldots, M$. Κατά την αποκωδικοποίηση μηνυμάτων σημασία έχουν οι **πιθανότητες αποστολής** $p(\mathbf{c}_i) = p($ *η πιθανότητα να έχει σταλεί η λέξη* $\mathbf{c}_i)$.

Οι πιθανότητες αποστολής **δεν** εξαρτώνται από τον δίαυλο επικοινωνίας. Επομένως, δεν πρέπει να συγχέονται με τις πιθανότητες μετάδοσης, οι οποίες καθορίζουν τον δίαυλο επικοινωνίας. Συνήθως εξαρτώνται από το είδος των μηνυμάτων που αποστέλλονται και από την πηγή, η οποία κωδικοποιείται με τον κώδικα. Είναι μεγάλο πρόβλημα για τον παραλήπτη να καθορίσει αυτές τις πιθανότητες.

Για παράδειγμα, αν ως κώδικα χρησιμοποιήσουμε το Ελληνικό αλφάβητο ((κωδικο)λέξεις είναι τα γράμματα), τότε η πιθανότητα αποστολής (χρησιμοποίησης) του γράμματος ϵ είναι πολύ μεγαλύτερη από την πιθανότητα αποστολής του γράμματος ψ.[9]

Μια ακραία περίπτωση, η οποία απλοποιεί την κατάσταση, αλλά τις περισσότερες φορές δεν ανταποκρίνεται στην πραγματικότητα, είναι η εξής: Κάνουμε την παραδοχή ότι για όλες τις λέξεις του κώδικα οι πιθανότητες αποστολής είναι ίσες, δηλαδή $p(\mathbf{c}_i) = 1/M$ για όλες τις λέξεις $\mathbf{c}_i$, $i = 1, 2, \ldots, M$ του κώδικα.

Μια *καλή* συνάρτηση αποκωδικοποίησης είναι μια συνάρτηση φ, η οποία μεγιστοποιεί την πιθανότητα σωστής αποκωδικοποιήσης. Δηλαδή (δεδομένου ότι ελήφθη η λέξη $\mathbf{x}$) η πιθανότητα να εστάλη η λέξη $\varphi(\mathbf{x})$ να είναι όσον το δυνατόν μεγαλύτερη.

Έστω φ μια συνάρτηση αποκωδικοποίησης. Υποθέτουμε ότι εστάλη η λέξη $\mathbf{c} \in \mathcal{C}$, δεδομένου ότι ελήφθη η λέξη $\mathbf{x}$, για μια σωστή αποκωδικοποίηση πρέπει να εχουμε $\varphi(\mathbf{x}) = \mathbf{c}$. Επομένως, η (δεσμευμένη) πιθανότητα:

$$\begin{aligned} p(\mathbf{c} \mid \mathbf{c}) &= p(\textit{ έχουμε σωστή αποκωδικοποίηση} \mid \textit{δεδομένου ότι εστάλη η } \mathbf{c}) \\ &= p(\varphi(\mathbf{x}) = \mathbf{c} \mid \textit{δεδομένου ότι εστάλη η } \mathbf{c}) \end{aligned}$$

[9] Οι πιθανότητες αποστολής αποτελούν ένα μέτρο, εκ των προτέρων, της *βεβαιότητας* για το ποία λέξη έχει αποσταλεί.

είναι ίση με το άθροισμα όλων των πιθανοτήτων:

$$p(\ \textit{ελήφθη η λέξη}\ \mathbf{x}\ \mid\ \textit{εστάλη η λέξη}\ \mathbf{c}\ ),$$

όπου το $\mathbf{x}$ διατρέχει όλες τις λέξεις στο $\mathbb{A}^n$ που ικανοποιούν τη σχέση $\varphi(\mathbf{x}) = c$. Δηλαδή:

$$p(\mathbf{c}\ \mid\ \mathbf{c}) = \sum_{x\in\varphi^{-1}(\mathbf{c})} p(\ \textit{ελήφθη η λέξη}\ \mathbf{x}\ \mid\ \ \textit{εστάλη η λέξη}\ \mathbf{c}\ ).$$

Από το Θεώρημα ολικής πιθανότητας προφανώς έχουμε:

$$p(\textit{σωστής αποκωδικοποίησης}) = \sum_{\mathbf{c}\in\mathcal{C}} p(\mathbf{c}\ \mid\ \mathbf{c})\cdot p(\mathbf{c}).$$

Οπότε από τα προηγούμενα έχουμε:

$$\begin{aligned} &p(\textit{σωστής αποκωδικοποίησης}) = \\ &\quad = \sum_{\mathbf{c}\in\mathcal{C}} \sum_{x\in\varphi^{-1}(\mathbf{c})} p(\textit{ελήφθη η λέξη}\ \mathbf{x}\ \mid\ \textit{εστάλη η λέξη}\ \mathbf{c}\ )\cdot p(\mathbf{c}). \end{aligned}$$

Επομένως, αν θέλουμε να μεγιστοποιήσουμε την πιθανότητα σωστής αποκωδικοποίησης, θα πρέπει να βρούμε μια συνάρτηση αποκωδικοποίησης φ τέτοια, ώστε:

$$\begin{aligned} p(\textit{ελήφθη η λέξη}\ \mathbf{x}\ \mid\ \ \textit{εστάλη η λέξη}\ \varphi(\mathbf{x})\ ) &= \\ = \max\{\, p(\ \textit{ελήφθη η λέξη}\ \mathbf{x}\ \mid\ \ \textit{εστάλη η λέξη}\ \mathbf{c}\ )\ \mid\ c\in\mathcal{C}\,\} & \end{aligned}$$

για όλες τις λέξεις $\mathbf{x}$ που είναι δυνατόν να ληφθούν (δηλαδή για όλα τα $\mathbf{x}\in\mathbb{A}^n$). Μια τέτοια συνάρτηση αποκωδικοποίησης θα λέγεται συνάρτηση **αποκωδικοποίησης μέγιστης πιθανότητας** και η αποκωδικοποίηση με τη βοήθεια μιας τέτοιας συνάρτησης θα λέγεται αποκωδικοποίηση ως προς την **Αρχή της μέγιστης πιθανότητας**.

Στην σχέση της πιθανότητας σωστής αποκωδικοποίησης εμφανίζονται οι πιθανότητες μετάδοσης, καθότι, όπως γνωρίζουμε, σε έναν (αμνήμονα) δίαυλο ισχύει η σχέση:

$$p(\textit{ελήφθη η λέξη}\ \mathbf{x}\ \mid\ \textit{εστάλη η λέξη}\ \mathbf{c}\ ) = \prod_{i=1}^{n} p(\textit{ελήφθη ο}\ x_i\ \mid\ \textit{εστάλη ο}\ c_i).$$

Οπότε μπορούμε να αντικαταστήσουμε στην παραπάνω σχέση της πιθανότητας σωστής αποκωδικοποίησης.

Η σχέση που τελικά προκύπτει για τον υπολογισμό της πιθανότητας σωστής αποκωδικοποίησης είναι πολύ δύσχρηστη και δεν μπορεί να εφαρμοσθεί με ευχέρεια, δεδομένου ότι, επιπλέον, έχουμε και το πρόβλημα υπολογισμού των πιθανοτήτων αποστολής.

Θα μπορούσαμε να υπολογίσουμε την πιθανότητα σωστής αποκωδικοποίησης στηριζόμενοι όχι στις πιθανότητες μετάδοσης ενός διαύλου, αλλά δυϊκά στις πιθανότητες λήψης ενός διαύλου.

Ορισμός 1.3.3. *Σε έναν δίαυλο επικοινωνίας με αλφάβητο:*

$$\mathbb{A} = \{a_1, a_2, \dots, a_r\}$$

οι (δεσμευμένες) πιθανότητες:

$$q_{ij} = p(\textit{εστάλη ο χαρακτήρας } a_i \mid \textit{ελήφθη ο χαρακτήρας } a_j)$$

ονομάζονται ***πιθανότητες λήψης.***

Δεν πρέπει να γίνεται σύγχυση μεταξύ των πιθανοτήτων μετάδοσης και των πιθανοτήτων λήψης. Στις μεν υποτίθεται ότι εστάλη μια λέξη, έστω $\mathbf{c} \in \mathcal{C}$ και ελήφθη μια λέξη $\mathbf{x} \in \mathbb{A}^n$. Στις δε υποτίθεται ότι ελήφθη μια λέξη $\mathbf{x} \in \mathbb{A}^n$ ενώ εστάλη η λέξη $\mathbf{c} \in \mathcal{C}$.

Προφανώς, σε έναν αμνήμονα δίαυλο για τις πιθανότητες λήψης ισχύει ανάλογη σχέση με τη σχέση που ισχύει για τις πιθανότητες μετάδοσης.

Έστω η (κωδικο)λέξη $\mathbf{c} = c_1\, c_2 \cdots c_n$ και η λέξη $\mathbf{x} = x_1\, x_2 \cdots x_n$. Τότε η πιθανότητα:

$$p(\ \textit{εστάλη η λέξη } \mathbf{c} \mid \ \textit{ελήφθη η λέξη } \mathbf{x}\ )$$

είναι ίση με το γινόμενο των πιθανοτήτων λήψης:

$$p(\textit{εστάλη ο χαρακτήρας } c_i \mid \textit{ελήφθη ο χαρακτήρας } x_i).$$

Δηλαδή:

$$p(\textit{εστάλη η λέξη } \mathbf{c} \mid \ \textit{ελήφθη η λέξη } \mathbf{x}\ ) = \\ = \prod_{i=1}^{n} p(\textit{εστάλη ο χαρακτήρας } c_i \mid \textit{ελήφθη ο χαρακτήρας } x_i).$$

Επανερχόμενοι τώρα στον υπολογισμό της πιθανότητας σωστής αποκωδικοποίησης και στηριζόμενοι στις πιθανότητες λήψης ενός διαύλου έχουμε:

$$p(\textit{σωστής αποκωδικοποίησης}) = \sum_{\mathbf{x}\in\mathbb{A}^n} p(\textit{σωστής αποκωδικοποίησης} \mid \textit{ελήφθη η λέξη}\ \mathbf{x}) \cdot p(\textit{ελήφθη η λέξη}\ \mathbf{x}).$$

Όταν έχουμε μια συνάρτηση αποκωδικοποίησης φ, μια ληφθείσα λέξη $\mathbf{x}$ αποκωδικοποιείται σωστά, αν η λέξη που εστάλη είναι πράγματι η $\varphi(\mathbf{x})$. Οπότε:

$$p(\textit{σωστής αποκωδικοποίησης} \mid \textit{ελήφθη η λέξη}\ \mathbf{x}) = p(\textit{εστάλη η λέξη}\ \varphi(\mathbf{x}) \mid \textit{ελήφθη η λέξη}\ \mathbf{x}).$$

Αντικαθιστώντας στην προηγούμενη σχέση έχουμε:

$$p(\textit{σωστής αποκωδικοποίησης}) = \sum_{\mathbf{x}\in\mathbb{A}^n} p(\ \textit{εστάλη η λέξη}\ \varphi(\mathbf{x}) \mid\ \textit{ελήφθη η λέξη}\ \mathbf{x}) \cdot p(\ \textit{ελήφθη η λέξη}\ \mathbf{x}).$$

Επομένως, αν θέλουμε να μεγιστοποιήσουμε την πιθανότητα σωστής αποκωδικοποίησης, θα πρέπει να βρούμε μια συνάρτηση αποκωδικοποίησης φ, τέτοια ώστε:

$$p(\textit{εστάλη η λέξη}\ \varphi(\mathbf{x}) \mid \textit{ελήφθη η λέξη}\ \mathbf{x}) = \max\{p(\textit{εστάλη η λέξη}\ \mathbf{c} \mid \textit{ελήφθη η λέξη}\ \mathbf{x}) \mid c \in \mathcal{C}\}$$

για όλες τις λέξεις $\mathbf{x}$ που είναι δυνατόν να ληφθούν (δηλαδή για όλα τα $\mathbf{x} \in \mathbb{A}^n$). Μια τέτοια συνάρτηση αποκωδικοποίησης θα λέγεται συνάρτηση **ιδανικού παρατηρητή**. Με άλλα λόγια, μια συνάρτηση ιδανικού παρατηρητή είναι μια συνάρτηση αποκωδικοποίησης φ, τέτοια ώστε, δεδομένου ότι ελήφθη η λέξη $\mathbf{x}$, το πιθανότερο είναι να έχει σταλεί η (κωδικο)λέξη $\varphi(\mathbf{x})$.

Παρατήρηση 1.3.4. Εδώ δεν πρέπει να παραβλέψουμε το εξής ενδεχόμενο. Μπορεί να υπάρχουν δύο (κωδικο)λέξεις (ή και περισσότερες) $\mathbf{c}_i$ και $\mathbf{c}_j$, έτσι

ώστε:

$$p(\textit{εστάλη η λέξη } \mathbf{c}_i \mid \textit{ελήφθη η λέξη } \mathbf{x}) = \\ = p(\textit{εστάλη η λέξη } \mathbf{c}_j \mid \textit{ελήφθη η λέξη } \mathbf{x}) \\ = \max\{\, p(\textit{εστάλη η λέξη } \mathbf{c} \mid \textit{ελήφθη η λέξη } \mathbf{x}) \mid c \in \mathcal{C}\,\}.$$

Στην περίπτωση αυτή υπάρχει πρόβλημα ως προς τον ορισμό της συνάρτησης φ. Θα θέσουμε $\varphi(\mathbf{x}) = \mathbf{c}_i$ ή $\varphi(\mathbf{x}) = \mathbf{c}_j$; Στην πράξη το θέμα αντιμετωπίζεται κατά περίπτωση. Τις περισσότερες φορές θέτουμε $\varphi(\mathbf{x}) = ?$, όπου εδώ το σύμβολο $?$ δεν δηλώνει ότι η λέξη $\mathbf{x}$ που λάβαμε είναι λανθασμένη, αλλά *αδυναμία* αποκωδικοποίησης. Υπάρχουν περιπτώσεις, όπου, αναλαμβάνοντας τον κίνδυνο λανθασμένης αποκωδικοποίησης, θέτουμε τυχαία η τιμή της συνάρτησης φ στη θέση $\mathbf{x}$ να είναι μια από τις (κωδικο)λέξεις που πληρούν τη σχέση:

$$p(\textit{εστάλη η λέξη } \mathbf{c}_i \mid \textit{ελήφθη η λέξη } \mathbf{x}) = \\ = \max\{\, p(\textit{εστάλη η λέξη } \mathbf{c} \mid \textit{ελήφθη η λέξη } \mathbf{x}) \mid c \in \mathcal{C}\,\}.$$

Όταν αναφερόμαστε σε συναρτήσεις αποκωδικοποίησης μεγίστης πιθανότητας ή ιδανικού παρατηρητή, στην πραγματικότητα αναφερόμαστε στην ίδια συνάρτηση.

Πράγματι, από το Θεώρημα του Bayes έχουμε:

$$p(\textit{εστάλη η λέξη } \mathbf{c} \mid \textit{ελήφθη η λέξη } \mathbf{x}) = \\ = \frac{p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \mathbf{c}) \cdot p(\mathbf{c})}{\sum_{i=1}^{M} p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \mathbf{c}_i) \cdot p(\mathbf{c}_i)}.$$

Στην προηγούμενη σχέση εμφανίζονται οι πιθανότητες αποστολής οι οποίες δεν εξαρτώνται από τον δίαυλο επικοινωνίας, αλλά από τη φύση του μηνύματος. Εδώ κάνουμε την παραδοχή ότι για όλες τις λέξεις του κώδικα οι πιθανότητες αποστολής είναι ίσες ($p(\mathbf{c}_i) = 1/M$, για όλες τις λέξεις $\mathbf{c}_i$, $i = 1, 2, \ldots, M$ του κώδικα). Οπότε η προηγούμενη σχέση γίνεται:

$$p(\textit{εστάλη η λέξη } \mathbf{c} \mid \textit{ελήφθη η λέξη } \mathbf{x}) = \\ = \frac{p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \mathbf{c})}{\sum_{i=1}^{M} p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \mathbf{c}_i)}.$$

Επομένως, όπως είπαμε, για τη συνάρτηση ιδανικού παρατηρητή πρέπει να μεγιστοποιηθεί το πρώτο μέλος της παραπάνω σχέσεως. Τούτο όμως είναι ισοδύναμο με το να μεγιστοποιηθεί ο αριθμητής του δευτέρου μέλους (ο παρανομαστής είναι σταθερός, καθότι το άθροισμα των πιθανοτήτων μετάδοσης εξαρτάται από τον δίαυλο επικοινωνίας και δεν μεταβάλεται). Ο αριθμητής όμως δεν είναι τίποτε άλλο απο την πιθανότητα μετάδοσης, οπότε η συνάρτηση ιδανικού παρατηρητή είναι η συνάρτηση μεγίστης πιθανότητας.

Συνεπώς, έχουμε αποδείξει το εξής σημαντικό θεώρημα.

Θεώρημα 1.3.5. *Με την υπόθεση ότι οι πιθανότητες αποστολής είναι ίσες για όλες τις λέξεις του κώδικα, η συνάρτηση ιδανικού παρατηρητή, όπως και η συνάρτηση μεγίστης πιθανότητας, εξασφαλίζει αποκωδικοποίηση μεγίστης πιθανότητας.*

Παράδειγμα 1.3.6. Έστω ότι έχουμε τον δυαδικό κώδικα $\mathcal{C} = \{\,000,\, 111\,\}$ και έναν συμμετρικό δίαυλο με πιθανότητα μετάδοσης λάθους χαρακτήρα ίση με 0.01, δηλαδή:

$p(\textit{ελήφθη ο χαρακτήρας } 1 \mid \textit{εστάλη ο χαρακτήρας } 0) =$

$= p(\textit{ελήφθη ο χαρακτήρας } 0 \mid \textit{εστάλη ο χαρακτήρας } 1) = 0.01,$

οπότε η πιθανότητα μετάδοσης σωστού χαρακτήρα είναι ίση με 0.99, δηλαδή:

$p(\textit{ελήφθη ο χαρακτήρας } 0 \mid \textit{εστάλη ο χαρακτήρας } 0) =$

$= p(\textit{ελήφθη ο χαρακτήρας } 1 \mid \textit{εστάλη ο χαρακτήρας } 1) = 0.99.$

Υποθέτουμε ότι ο δέκτης λαμβάνει τη λέξη $\mathbf{x} = 100$ και θέλουμε να υπολογίσουμε την τιμή της συνάρτησης αποκωδικοποίησης μέγιστης πιθανότητας για τη λέξη $\mathbf{x} = 100$. Σύμφωνα με τα προηγούμενα, η $\varphi(\mathbf{x})$ πρέπει να πληροί τη σχέση:

$$p(\ \textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \varphi(\mathbf{x})\ ) = \max\{\, p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \ \textit{εστάλη η λέξη } 000\,),\ p(\ \textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } 111\,)\,\}.$$

Αλλά από τη σχέση (1.1) έχουμε:

$$p(\ \textit{ελήφθη η λέξη } 100 \mid \ \textit{εστάλη η λέξη } 000\,) = (0.01)(0.99)^2 = 0.009801$$

και

$$p(\ \textit{ελήφθη η λέξη}\ 100 \mid\ \textit{εστάλη η λέξη}\ 000\ ) = (0.99)(0.01)^2 = 0.00099.$$

Επειδή η πρώτη πιθανότητα είναι μεγαλύτερη από τη δεύτερη, σύμφωνα με την Αρχή της αποκωδικοποίησης ως προς την μέγιστη πιθανότητα, πρέπει να έχουμε $\varphi(\mathbf{x}) = 000$, δηλαδή η λέξη $\mathbf{x} = 100$ αποκωδικοποιείται ως η λέξη 000.

1.3.2 Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη

Ας ξεκινήσουμε την παράγραφο με το τελευταίο παράδειγμα. Έστω ότι έχουμε τον κώδικα $\mathcal{C} = \{\, 000, 111 \,\}$ και ο δέκτης λαμβάνει τη λέξη 100, η οποία δεν ανήκει στον κώδικα. Λογικό είναι να υποτεθεί, ότι το πιθανότερο είναι να εστάλη η λέξη 000, η οποία είναι πλησιέστερη στην λέξη που ελήφθη. Οπότε αποκωδικοποιείται ως 000.

Υπενθυμίζουμε ότι, αν έχει σταλεί μια λέξη $\mathbf{c} \in \mathcal{C}$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$, η αποκωδικοποίηση είναι *σωστή* αν $\varphi(\mathbf{x}) = c$.

Γενικά, μια συνάρτηση αποκωδικοποίησης **ως προς την πλησιέστερη λέξη** την ορίζουμε ως εξής. Έστω ότι έχει σταλεί μια λέξη $\mathbf{c} \in \mathcal{C}$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{A}^n$. Αν η $\mathbf{x}$ ανήκει στον κώδικα, τότε ορίζουμε $\varphi(\mathbf{x}) = \mathbf{x}$, δηλαδή κατά την αποκωδικοποίηση δεχόμαστε ότι εστάλη η λέξη $\mathbf{x}$. Αν η $\mathbf{x}$ δεν ανήκει στον κώδικα, υπολογίζουμε την απόσταση της $\mathbf{x}$ από όλες τις λέξεις του κώδικα. Υπάρχει μια λέξη $\mathbf{d}$ του κώδικα με την μικρότερη απόσταση από την $\mathbf{x}$. Αν η λέξη $\mathbf{d}$ είναι η μοναδική με την ιδιότητα αυτή, τότε ορίζουμε $\varphi(\mathbf{x}) = \mathbf{d}$ και κατά την αποκωδικοποίηση δεχόμαστε την $\mathbf{d}$. Αν υπάρχουν περισσότερες λέξεις οι οποίες απέχουν την ίδια ελάχιστη απόσταση από τη λέξη $\mathbf{x}$, τότε προς αποφυγή *σύγχυσης* δηλώνουμε *αδυναμία* αποκωδικοποίησης ορίζοντας $\varphi(x) = ?$.

Η αποκωδικοποίηση με τη βοήθεια μιας τέτοιας συνάρτησης θα λέγεται αποκωδικοποίηση ως προς την **Αρχή της πλησιέστερης λέξης**.

Παρατηρήσεις 1.3.7. 1. Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη είναι ένας *φυσιολογικός* τρόπος αποκωδικοποίησης, του-

λάχιστον στην αρχή. Στην πράξη όμως, παρουσιάζει δυσκολίες σε κώδικες με μεγάλο μήκος, καθώς είναι αρκετά χρονοβόρο κάθε φορά να ελέγχουμε την απόσταση μιας λέξης που λαμβάνουμε από όλες τις λέξεις του κώδικα για να την αντικαταστήσουμε με την πλησιέστερη προς αυτή λέξη του κώδικα.

Ένα καίριο μέλημα στον σχεδιασμό ενός κώδικα είναι η δυνατότητα ο έλεγχος αυτός να γίνεται γρήγορα και αποτελεσματικά. (Βλέπε Παράγραφο 2.4.4).

2. Η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη δεν αποκλείει το ενδεχόμενο να έχει σταλεί μια λέξη $\mathbf{c}$, κατά την μετάδοση να έχει παρεισφρήσει λάθος και να λάβουμε μια λέξη $\mathbf{x}$, η οποία να ανήκει στον κώδικα, οπότε η λέξη $\mathbf{c}$ αποκωδικοποιείται (κακώς βέβαια) σαν λέξη $\mathbf{x}$.

3. Έχουμε δει ότι κατά την αποκωδικοποίηση είτε με την Αρχή της μέγιστης πιθανότητας είτε με την Αρχή ως προς την πλησιέστερη λέξη ενδέχεται να έχουμε αδυναμία αποκωδικοποίησης. Στην περίπτωση αυτή έχει επικρατήσει η όλη διαδικασία να ονομάζεται **μη πλήρης αποκωδικοποίηση**. Ορισμένες φορές όμως, όπως έχουμε προείπει, αναλαμβάνοντας τον κίνδυνο λανθασμένης αποκωδικοποίησης, θέτουμε τυχαία η τιμή της συνάρτησης αποκωδικοποίησης φ στη θέση $\mathbf{x}$ της ληφθείσας λέξης να είναι μια από τις (κωδικο)λέξεις που πληρούν τη σχέση μεγίστης πιθανότητας ή να είναι από τις πλησιέστερες στη λέξη $\mathbf{x}$. Στην περίπτωση αυτή, η όλη διαδικασία ονομάζεται **πλήρης αποκωδικοποίηση**. Το τι είναι προτιμητέο εξαρτάται από την περίπτωση και δεν θα ασχοληθούμε εδώ.

Παραδείγματα 1.3.8. 1. Έστω ότι έχουμε τον κώδικα:

$$\mathcal{C} = \{\, 0000,\, 0011,\, 1000,\, 1100 \,\}.$$

Υποθέτουμε ότι αποστέλεται η (κωδικο)λέξη $\mathbf{a} = 0011$ και ότι λαμβάνεται η λέξη $\mathbf{x} = 0111$. Παρατηρούμε ότι η μικρότερη απόσταση της $\mathbf{x}$ από τα στοιχεία του κώδικα είναι (μόνο) από την (κωδικο)λέξη $\mathbf{a}$ (αυτή

που εστάλη), οπότε ορθώς αποκωδικοποιούμε την $\mathbf{x}$ σαν $\mathbf{a}$. Αν όμως λάβουμε την λέξη $\mathbf{y} = 0101$, τότε βλέπουμε ότι αυτή η λέξη ισαπέχει από τις (κωδικο)λέξεις 0000 και 0011, οπότε δεν μπορούμε να την αποδικωποιήσουμε. Τέλος, δεν αποκλείεται να λάβουμε τη λέξη $\mathbf{z} = 0000$, δηλαδή να έχει επέλθει αλλοίωση σε δύο χαρακτήρες και να την δεχθούμε, λανθασμένα, ως τη λέξη που εστάλη, αφού και αυτή ανήκει στον κώδικα.

2. Ας επανέλθουμε στο Παράδειγμα της σελίδας 11, όπου ζητείται η ασφαλής καθοδήγηση ενός πλοίου μέσω κωδικοποιμένου μηνύματος.

   Αντί του κώδικα $\mathcal{D} = \{\,000,\, 011,\, 101,\, 110\,\}$ χρησιμοποιούμε τον κώδικα $\mathcal{E} = \{\,00000,\, 01101,\, 10110,\, 11011\,\}$ και συνάρτηση κωδικοποίησης $h : S \longrightarrow \mathcal{E}$ με $h(\mathbf{A}) = 00000$, $h(\mathbf{\Delta}) = 01101$, $h(\mathbf{B}) = 10110$, $h(\mathbf{N}) = 11011$. Παρατηρούμε ότι ο κώδικας $\mathcal{E}$ προέρχεται από τον προηγούμενο κώδικα επισυνάπτοντας δύο επιπλέον ψηφία με τέτοιο τρόπο, ώστε δύο (κωδικο)λέξεις να απέχουν μεταξύ τους απόσταση τουλάχιστον *ίση* με τρία. Υποθέτουμε ότι εστάλη η (κωδικο)λέξη $\mathbf{a} = 01101$ και ελήφθη η λέξη $\mathbf{x} = 01111$. Η ληφθείσα λέξη δεν ανήκει στον κώδικα, αλλά η μικρότερη απόστασή της από τα στοιχεία του κώδικα είναι (μόνο) από την (κωδικο)λέξη $\mathbf{a} = 01101$ που εστάλη. Οπότε σύμφωνα με την Αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη μπορεί ορθώς να αποκωδικοποιηθεί ως η: $\mathbf{a} = 01101$. Δηλαδή, με τη βοήθεια του κώδικα το λάθος όχι απλώς 'ανιχνεύθηκε', αλλά και 'διορθώθηκε'. Αν όμως κατά την αποστολή υπεισήλθαν λάθη σε περισσότερες από μία θέσεις και ελήφθη η λέξη $\mathbf{y} = 11111$, τότε ανιχνεύεται λάθος, αφού η $\mathbf{y} = 11111$ δεν ανήκει στον κώδικα, αλλά αν επιχειρηθεί να αποκωδικοποιηθεί σύμφωνα με την Αρχή ως προς την πλησιέστερη λέξη, τότε αποκωδικοποιείται λανθασμένα ως η $\mathbf{b} = 11011$.

Τα παραπάνω προβλήματα που παρουσιάζονται κατά την αποκωδικοποίηση με αυτό τον τρόπο θα μπορούσαν να εξαλειφθούν, αν μη τι άλλο να περιοριστούν, αν ο κώδικας είχε επιλεγεί ώστε οι λέξεις του να ήταν *αραιά* κατανεμημένες. Για να γίνουμε πιο συγκεκριμένοι χρειαζόμαστε μερικούς

ορισμούς:

Ορισμός 1.3.9. *Έστω $\mathcal{C}$ ένας κώδικας (με τουλάχιστον δύο λέξεις). Η* ***ελάχιστη απόσταση*** *$d(\mathcal{C})$ του $\mathcal{C}$ είναι η μικρότερη απόσταση μεταξύ δύο διακεκριμένων λέξεων. Δηλαδή:* $d(\mathcal{C}) = \min\{\, d(\mathbf{c}, \mathbf{d}) \mid \mathbf{c}, \mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d} \,\}$.

Επομένως, εκτός από το αλφάβητο, το μήκος n και το μέγεθος $M = \mid \mathcal{C} \mid$ ενός κώδικα $\mathcal{C}$, έχουμε μια επιπλέον παράμετρο, την ελάχιστη απόσταση $d = d(\mathcal{C})$ του κώδικα, και για συντομία θα αναφέρεται ως ένας (n, M, d) κώδικας.

Ορισμός 1.3.10. *Ένα διάνυσμα λάθους $\mathbf{e} \in \mathbb{A}^n$* ***ανιχνεύεται*** *από έναν κώδικα $\mathcal{C} \subseteq \mathbb{A}^n$, αν η λέξη $\mathbf{a}+\mathbf{e}$ δεν ανήκει στο κώδικα $\mathcal{C}$ για κάθε (κωδικο)λέξη $\mathbf{a} \in \mathcal{C}$. Αν υπάρχει (τουλάχιστον ένα) $\mathbf{a} \in \mathcal{C}$ έτσι ώστε $\mathbf{a} + \mathbf{e} \in \mathcal{C}$, τότε το διάνυσμα $\mathbf{e}$ είναι* ***μη ανιχνεύσιμο***.

Ένας κώδικας $\mathcal{C}$ ***ανιχνεύει*** *λ το πλήθος λάθη, όπου λ είναι ένας θετικός ακέραιος αριθμός, αν κάθε διάνυσμα λάθους $\mathbf{e}$ βάρους το πολύ λ ανιχνεύεται από τον κώδικα $\mathcal{C}$. Ένας κώδικας $\mathcal{C}$* ***ανιχνεύει ακριβώς*** *λ το πλήθος λάθη, αν ανιχνεύει διανύσματα λάθους με βάρος το πολύ λ, αλλά δεν ανιχνεύει λάθη με βάρος $\lambda + 1$.*

Τονίζουμε, σύμφωνα με τον προηγούμενο ορισμό, όταν λέμε ο κώδικας ανιχνεύει λ λάθη, εννοούμε ότι, αν κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις το πολύ σε λ το πλήθος χαρακτήρες, τότε έχουμε απλώς την ένδειξη ότι η ληφθείσα λέξη δεν ανήκει στον κώδικα, **χωρίς** καμία άλλη πληροφορία για το διάνυσμα λάθους που υπεισήλθε.

Ας φαντασθούμε ότι έχουμε έναν μηχανισμό (π.χ. έναν υπολογιστή), που ελέγχει τις λέξεις που καταφθάνουν και ότι όταν εντοπίζεται μία λέξη που δεν ανήκει στον κώδικα, τότε ανάβει μια κόκκινη λυχνία. Αν ο κώδικας ανιχνεύει λ λάθη, τότε η λυχνία ανάβει (οπωσδήποτε), αν κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις το πολύ σε λ το πλήθος χαρακτήρες. Ενδέχεται όμως η λυχνία να ανάβει (ή να μην ανάβει), όταν υπεισέρχονται διανύσματα λάθους με βάρος μεγαλύτερο του λ. Καθότι, όπως έχουμε παρατηρήσει, ενδέχεται η αποσταλείσα λέξη να έχει υποστεί τόσες πολλές αλλοιώσεις κατά τη μετάδοση, έτσι ώστε να έχουμε λάβει μια άλλη λέξη του κώδικα.

Παράδειγμα 1.3.11. Ο κώδικας $\mathcal{C} = \{\, 0000, 0011, 1000, 1100 \,\}$ δεν ανιχνεύει κανένα λάθος (γιατί;). Ο κώδικας $\mathcal{C} = \{\, 000000, 111000, 111111 \,\}$ ανιχνεύει δύο λάθη (γιατί;), ενώ δεν ανιχνεύει όλα τα (πιθανά) τρία λάθη π.χ. αν έχει σταλεί η λέξη 000000, ανιχνεύει τη λανθασμένη λέξη 010101, αλλά δεν ανιχνεύει τη λανθασμένη λέξη 111000. (Μάλιστα δε, σύμφωνα με την Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη, την αποκωδικοποιεί λανθασμένα).

Ορισμός 1.3.12. *Ένα διάνυσμα λάθους* $\mathbf{e} \in \mathbb{A}^n$ ***διορθώνεται*** *από έναν κώδικα* $\mathcal{C} \subseteq \mathbb{A}^n$ *αν για κάθε σταλθείσα λέξη* $\mathbf{a} \in \mathcal{C}$ *η ληφθείσα λέξη* $\mathbf{a} + \mathbf{e}$*, που δεν ανήκει στον κώδικα* $\mathcal{C}$*, αποκωδικοποιείται, σύμφωνα με την Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη, ως η λέξη* $\mathbf{a} \in \mathcal{C}$*.*

Ένας κώδικας $\mathcal{C}$ ***διορθώνει*** λ *το πλήθος λάθη, όπου* λ *είναι ένας θετικός ακέραιος αριθμός, αν κάθε διάνυσμα λάθους* $\mathbf{e}$ *βάρους το πολύ* λ *διορθώνεται από τον κώδικα* $\mathcal{C}$*. Ένας κώδικας* $\mathcal{C}$ ***διορθώνει ακριβώς*** λ *το πλήθος λάθη, αν διορθώνει διανύσματα λάθους με βάρος το πολύ* λ*, αλλά δεν διορθώνει λάθη με βάρος* $\lambda + 1$*.*

Τονίζουμε, σύμφωνα με τον προηγούμενο ορισμό, όταν λέμε ο κώδικας διορθώνει λ λάθη, εννοούμε ότι, αν κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις το πολύ σε λ το πλήθος χαρακτήρες, τότε ο παραλήπτης είναι σίγουρος ότι κατά την αποκωδικοποίηση θα λάβει την λέξη που έχει σταλεί χωρίς καμία επιπλέον πληροφορία για το διάνυσμα λάθους. Αν όμως κατά τη μετάδοση μιας λέξης έχουν επέλθει αλλοιώσεις σε περισσότερους από λ το πλήθος χαρακτήρες, τότε ο παραλήπτης δεν είναι σίγουρος κατά την αποκωδικοποίηση ότι η λέξη που έλαβε είναι πράγματι η λέξη που έχει σταλεί.

Παρατηρήσεις 1.3.13.

1. Αν θέλουμε να εκφράσουμε τη διόρθωση λαθών με τη βοήθεια της συνάρτησης αποκωδικοποίησης φ, μπορούμε να πούμε ότι το διάνυσμα λάθους $\mathbf{e} \in \mathbb{A}^n$ διορθώνεται, αν για κάθε σταλθείσα λέξη $\mathbf{a} \in \mathcal{C}$ ισχύει $\varphi(\mathbf{a} + \mathbf{e}) = \mathbf{a}$.

2. Όταν λέμε ότι ένας κώδικας δεν διορθώνει λάθη βάρους $\lambda + 1$, εννούμε ότι υπάρχει τουλάχιστον ένα $\mathbf{e} \in \mathbb{A}^n$ με βάρος $\lambda + 1$ και, τουλάχιστον,

μία (κωδικο)λέξη $\mathbf{a} \in \mathcal{C}$ έτσι ώστε, αν έχει σταλεί η (κωδικο)λέξη $\mathbf{a}$ και έχει ληφθεί η λέξη $\mathbf{x} = \mathbf{a} + \mathbf{e}$, να έχουμε $\varphi(\mathbf{a} + \mathbf{e}) \neq \mathbf{a}$.

3. Όταν ένας κώδικας διορθώνει λ λάθη, τότε αμέσως παρατηρούμε ότι ισχύει $d(\mathcal{C}) \geq \lambda + 1$. (γιατί;) Συγκεκριμένα ισχύει κάτι πολύ ισχυρότερο (Βλέπε Θεώρημα 1.3.16).

Μπορούμε να αναδιατυπώσουμε τον ορισμό πότε ένας κώδικας ανιχνεύει ένα λάθος, χρησιμοποιώντας την έννοια της ελάχιστης απόστασης ενός κώδικα.

Θεώρημα 1.3.14. *Ένας κώδικας $\mathcal{C}$ ανιχνεύει λ το πλήθος λάθη, αν και μόνο αν* $d(\mathcal{C}) \geq \lambda + 1$.

Απόδειξη. Όπως προείπαμε, η απόδειξη αποτελεί αναδιατύπωση του ορισμού και αφίεται ως άσκηση. ό.έ.δ.

Πρόταση 1.3.15. *Ένας κώδικας $\mathcal{C}$ ανιχνεύει ακριβώς λ το πλήθος λάθη αν και μόνο αν* $d(\mathcal{C}) = \lambda + 1$.

Απόδειξη. Άσκηση. ό.έ.δ.

Όπως 'διαισθανόμαστε', ένας κώδικας για να διορθώνει λάθη, και όχι απλώς να ανιχνεύει, πρέπει να είναι αρκετά 'αραιός'. Συγκεκριμένα, ισχύει το εξής θεώρημα.

Θεώρημα 1.3.16. *Ένας κώδικας $\mathcal{C}$ διορθώνει λ το πλήθος λάθη αν και μόνο αν* $d(\mathcal{C}) \geq 2\lambda + 1$.

Απόδειξη. Υποθέτουμε ότι $d(\mathcal{C}) \geq 2\lambda + 1$. Έστω ότι εστάλη η λέξη $\mathbf{a} \in \mathcal{C}$ και ελήφθη η λέξη $\mathbf{b} = \mathbf{a} + \mathbf{e}$, που δεν ανήκει στον κώδικα $\mathcal{C}$, όπου $\mathbf{e}$ είναι το διάνυσμα λάθους που υπεισήλθε και επέφερε αλλοιώσεις σε λ (το πολύ) χαρακτήρες. Τότε, προφανώς, $1 \leq d(\mathbf{a}, \mathbf{b}) \leq \lambda$. Η λέξη $\mathbf{b}$ είναι πλησιέστερα στη λέξη $\mathbf{a}$ από κάθε άλλη λέξη του κώδικα. Πράγματι, αν υπήρχε μια άλλη λέξη $\mathbf{c} \in \mathcal{C}$ με $d(\mathbf{b}, \mathbf{c}) \leq d(\mathbf{b}, \mathbf{a})$, τότε από την τριγωνική ιδιότητα έχουμε:

$$d(\mathbf{a}, \mathbf{c}) \leq d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}) \leq \lambda + \lambda < d(\mathcal{C}).$$

Άτοπο. Επομένως, αφού η λέξη **b** που ελήφθη είναι πλησιέστερα προς τη λέξη **a** που εστάλη, αποκωδικοποιείται (ορθώς) ως η λέξη **a** και ο κώδικας διωρθώνει λ λάθη.

Αντίστροφα, υποθέτουμε ότι ο κώδικας $\mathcal{C}$ διορθώνει λ λάθη. Από προηγούμενη παρατήρηση έχουμε ότι $d(\mathcal{C}) \geq \lambda + 1$. Υποθέτουμε ότι $d(\mathcal{C}) \leq 2\lambda$. Έστω δύο λέξεις $\mathbf{a}, \mathbf{b} \in \mathcal{C}$, με $d(\mathbf{a}, \mathbf{b}) = d(\mathcal{C})$. Θα αποδείξουμε ότι ενδέχεται να σταλεί η λέξη **a**, να υπεισέλθουν λ λάθη, ώστε να ληφθεί μια λέξη, έστω **c**, η οποία είτε να ισαπέχει από τις λέξεις **a** και **b** είτε να είναι πλησιέστερα προς τη λέξη **b**. Οπότε, κατά την αποκωδικωποίηση, θα έχουμε αδυναμία αποκωδικοποίησης ή λάθος αποκωδικοποίηση ως η λέξη **b** αντί (του ορθού) ως η λέξη **a**. Αυτό θα είναι άτοπο, καθότι υποθέσαμε ότι ο κώδικας διορθώνει λ λάθη.

Έστω ότι οι λέξεις $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ και $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ συμπίπτουν σε $n - d(\mathcal{C})$ το πλήθος θέσεις. Δηλαδή $a_{i_j} = b_{i_j}$ για $j = 1, 2, \ldots, n - d(\mathcal{C})$. Υποθέτουμε ότι, αντί της λέξης **a** που εστάλη, ελήφθη η λέξη $\mathbf{c} = (c_1, c_2, \ldots, c_n)$, η οποία συμπίπτει στις ίδιες, $n - d(\mathcal{C})$ το πλήθος, θέσεις με τις λέξεις **a** και **b**, δηλαδή $a_{i_j} = b_{i_j} = c_{i_j}$ για $j = 1, 2, \ldots, n - d(\mathcal{C})$. Για τις υπόλοιπες $d(\mathcal{C})$ το πλήθος θέσεις υποθέτουμε ότι η **c** συμπίπτει σε $d(\mathcal{C}) - \lambda$ το πλήθος θέσεις με τη λέξη **a** και σε λ το πλήθος θέσεις με τη λέξη **b**. Τότε η λέξη **c** διαφέρει από τη λέξη **a** σε λ το πλήθος θέσεις και από τη λέξη **b** σε $d(\mathcal{C}) - \lambda$ το πλήθος θέσεις. Άρα, $d(\mathbf{b}, \mathbf{c}) = d(\mathcal{C}) - \lambda \leq d(\mathbf{a}, \mathbf{c}) = \lambda$. Επομένως, κατά την αποκωδικοποίηση αποκλείεται η λέξη να αποκωδικοποιηθεί ως η λέξη **a**. Άτοπο. (Στην καλύτερη περίπτωση θα είχαμε $d(\mathbf{b}, \mathbf{c}) = d(\mathcal{C}) - \lambda = d(\mathbf{a}, \mathbf{c}) = \lambda$, δηλαδή αδυναμία αποκωδικοποίησης). ό.έ.δ.

Πρόταση 1.3.17. *Ένας κώδικας $\mathcal{C}$ διορθώνει ακριβώς λ το πλήθος λάθη, αν και μόνο αν* $d(\mathcal{C}) = 2\lambda + 1$ *ή* $d(\mathcal{C}) = 2\lambda + 2$.

Απόδειξη. Η απόδειξη είναι απλή και αποτελεί μια καλή άσκηση στην κατανόηση της διαφοράς μεταξύ του *ένας κώδικας διορθώνει (μέχρι) λ το πλήθος λάθη* και του *ένας κώδικας διορθώνει ακριβώς λ το πλήθος λάθη*. ό.έ.δ.

Παρατήρηση 1.3.18. Από το προηγούμενα συνάγουμε ότι στη διόρθωση λαθών είναι 'προτιμηταίοι' κώδικες με περιττή ελάχιστη απόσταση. Πράγματι,

έστω $\mathcal{C}$ ένας κώδικας με ελάχιστη απόσταση $d(\mathcal{C}) = 2k+2$. Ο μέγιστος αριθμός λαθών που μπορεί να διορθώσει ο κώδικας, σύμφωνα με το προηγούμενο θεώρημα, είναι ίσος με $\lambda = \left[\frac{2k+2-1}{2}\right] = \left[\frac{2k+1}{2}\right] = k$. Αν 'πλουτίσουμε'[10] τον κώδικα επισυνάπτοντας επιπλέον (κωδικο)λέξεις, έτσι ώστε η ελάχιστη απόσταση του νέου κώδικα να μικρύνει και να γίνει ίση με $2k+1$, τότε ο νέος κώδικας μπορεί να διορθώσει πάλι μέχρι $\lambda = \left[\frac{2k+1-1}{2}\right] = \left[\frac{2k}{2}\right] = k$.

Παράδειγμα 1.3.19. (Ο κώδικας ISBN) Όλοι γνωρίζουμε ότι σε κάθε βιβλίο αντιστοιχεί ένας δεκαψήφιος αριθμός (ο οποίος συνήθως αναγράφεται στο οπισθόφυλλο του βιβλίου) είναι ο γνωστός αριθμός ISBN (International Standard Book Number). Ο αριθμός αυτός αποτελεί την *ταυτότητα* του βιβλίου και περικλείει πληροφορίες για το βιβλίο. Το πρώτο ψηφίο δηλώνει τη γλώσσα στην οποία είναι γραμμένο το βιβλίο, τα επόμενα τρία ψηφία δηλώνουν τον εκδοτικό οίκο, τα επόμενα πέντε ψηφία δίνονται από τον εκδότη και το τελευταίο ψηφίο υπολογίζεται από τα προηγούμενα ως εξής:

Υποθέτουμε ότι έχουμε τον αριθμό $a_1a_2\cdots a_9a_{10}$, όπου τα ψηφία a_i, $i = 1, \ldots, 9$ λαμβάνουν τιμές από το σύνολο $\{0, 1, \ldots, 9\}$. Εφόσον έχουν επιλεγεί τα a_i, $i = 1, \ldots, 9$, για το τελευταίο ψηφίο απαιτούμε να ισχύει:

$$a_{10} \equiv \left(\sum_{i=1}^{9} i \cdot a_i\right) \mod 11.$$

Δηλαδή το a_{10} είναι το υπόλοιπο της διαίρεσης του αθροίσματος $\sum_{i=1}^{9} i \cdot a_i$ με το 11. Το υπόλοιπο αυτό ενδέχεται να λαμβάνει και την τιμή 10. Επειδή το 'ψηφίο' 10 έχει δύο χαρακτήρες, για διαχειριστικούς καθαρά λόγους, έχει συμφωνηθεί στην περίπτωση αυτή να γράφουμε τον χαρακτήρα X.

Για παράδειγμα, οι αριθμοί 0 387 94704 3 και 0 201 02988 X ικανοποιούν τις παραπάνω απαιτήσεις, άρα θα μπορούσαν να είναι οι ISBN για κάποια βιβλία.

[10] Στην παράγραφο 1.4 θα αναφερθούμε διεξοδικότερα στο τι σημαίνει 'προτιμιταίος' και τι 'πλουσιώτερος' κώδικας.

Το σύνολο $\mathcal{C}$, το οποίο αποτελείται από όλους τους δεκαψήφιους 'αριθμούς' που υπολογίζονται σύμφωνα με την παραπάνω διαδικασία, είναι ο κώδικας ISBN.

Ο κώδικας αυτός με τον τρόπο που σχεδιάστηκε μπορεί να ανιχνεύει ένα λάθος. Πράγματι, υποθέτουμε ότι εστάλη η (κωδικο)λέξη $\mathbf{a} = a_1a_2\cdots a_9a_{10}$, αλλά ελήφθη η λέξη $\mathbf{x} = x_1x_2\cdots x_9x_{10}$, η οποία συμφωνεί σε όλους τους χαρακτήρες με την $\mathbf{a}$, εκτός από τον χαρακτήρα a_r, όπου αντί αυτού έχουμε τον χαρακτήρα $x_r = a_r + e$ με $e \neq 0$. Από τον τρόπο ορισμού του κώδικα $\mathcal{C}$ έχουμε $\sum_{i=1}^{10} i \cdot a_i \equiv 0 \mod 11$ (γιατί;). Αλλά για την λέξη $\mathbf{x}$ έχουμε:

$$\sum_{i=1}^{10} i \cdot x_i = \left(\sum_{i=1}^{10} i \cdot a_i\right) + r \cdot e \not\equiv 0 \mod 11.$$

Άρα, ανιχνεύθηκε το λάθος.

Παρατηρήσεις 1.3.20. Στο προηγούμενο παράδειγμα θα πρέπει να παρατηρήσουμε τα εξής:

1. Στην τελευταία σχέση ισχυριζόμαστε ότι $r \cdot e \neq 0 \pmod{11}$. Αυτό πράγματι ισχύει, διότι τα r και e είναι θετικοί ακέραιοι μικρότεροι ή ίσοι του 10 διάφοροι του μηδενός, επομένως, επειδή ο πολλαπλασιασμός γίνεται στο σώμα $\mathbb{Z}_{11}$, το γινόμενό τους δεν είναι ίσο με το $0 \pmod{11}$.

2. Το συμπέρασμα ότι ο κώδικας ανιχνεύει ένα λάθος συνάδει με το Θεώρημα 1.3.14. Μάλιστα ανιχνεύει ακριβώς ένα λάθος, καθότι η ελάχιστη απόστασή του είναι ίση με δύο, αφού για παράδειγμα τα 0 387 94704 3 και 2 387 94704 5 είναι στοιχεία του και διαφέρουν σε δύο μόνο χαρακτήρες.

3. Ο κώδικας ISBN δεν διορθώνει κανένα λάθος, παρόλα αυτά είναι *ικανοποιητικός* για τον σκοπό που έχει σχεδιασθεί. Διότι, επιπλέον, έχει τη δυνατότητα να ανιχνεύει τον 'αναγραμματισμό' δύο χαρακτήρων σε μια (κωδικο)λέξη.

   Πράγματι, υποθέτουμε ότι εστάλη η (κωδικο)λέξη $\mathbf{a} = a_1a_2\cdots a_9a_{10}$, αλλά ελήφθη η λέξη $\mathbf{x} = x_1x_2\cdots x_9x_{10}$, της οποίας όλοι οι χαρακτήρες

συμφωνούν με τους χαρακτήρες της $\mathbf{a}$, εκτός από τις θέσεις r και j, όπου οι χαρακτήρες έχουν αλλάξει θέση, δηλαδή $x_r = a_j$ και $x_j = a_r$. Τότε θα έχουμε:

$$\sum_{i=1}^{10} i \cdot x_i = \left(\sum_{i=1}^{10} i \cdot a_i \right) + (r-j)x_j + (j-r)x_r \equiv (r-j)x_j + (j-r)x_r \mod 11.$$

Στην τελευταία σχέση έχουμε ότι, αν $r \neq j$ και $x_r \neq x_j$, τότε:

$$(r-j)x_j + (j-r)x_r = (r-j)(x_j - x_r) \not\equiv 0 \mod 11.$$

Οπότε ανιχνεύουμε τον αναγραμματισμό[11].

4. Επίσης, ο κώδικας έχει την έξης μερική δυνατότητα για τη διόρθωση λαθών. Υποθέτουμε, όπως προηγουμένως, ότι εστάλη η (κωδικο)λέξη $\mathbf{a} = a_1 a_2 \cdots a_9 a_{10}$ και ελήφθη η λέξη $\mathbf{x} = x_1 x_2 \cdots x_9 x_{10}$, η οποία συμφωνεί σε όλους τους χαρακτήρες με την $\mathbf{a}$, εκτός από τον χαρακτήρα a_r, όπου αντί αυτού έχουμε τον χαρακτήρα $x_r = a_r + e$ με $e \neq 0$. Από τη σχέση $\sum_{i=1}^{10} i \cdot x_i = (\sum_{i=1}^{10} i \cdot a_i) + r \cdot e \not\equiv 0 \mod 11$ βλέπουμε ότι αν γνωρίζουμε τη θέση r στην οποία επήλθε η αλλοίωση του χαρακτήρα, τότε μπορούμε να υπολογίσουμε τον σωστό χαρακτήρα a_i, αντί του $x_i = a_i + e$ που λάβαμε. Φυσικά, μπορούμε αντίστροφα να υπολογίσουμε τη θέση στην οποία επήλθε η αλλοίωση, αν γνωρίζουμε το e που προκάλεσε την αλλοίωση.

Τελειώνοντας την παράγραφο, επισημαίνουμε ότι οι δύο τρόποι αποκωδικοποίησης που αναφέραμε, η Αρχή της αποκωδικοποίησης μέγιστης πιθανότητας και η Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη, στην πραγματικότητα αποτελούν τις δύο όψεις του *ιδίου νομίσματος*.

Έστω ότι έχουμε τον δυαδικό κώδικα $\mathcal{C}$ και έναν συμμετρικό δίαυλο με πιθανότητα μετάδοσης λάθους χαρακτήρα ίση με $p < 1/2$, δηλαδή:

$$p(\textit{ελήφθη ο χαρακτήρας } 1 \mid \textit{εστάλη ο χαρακτήρας } 0) =$$
$$= p(\textit{ελήφθη ο χαρακτήρας } 0 \mid \textit{εστάλη ο χαρακτήρας } 1) = p,$$

[11] Αν στις θέσεις που έγινε ο αναγραμματισμός οι χαρακτήρες συνέπιπταν, τότε θα είχαμε $x_r = a_j = a_r = x_j$. Ο αναγραμματισμός δεν θα ανιχνεύετο, διότι στην πραγματικότητα δεν έγινε αναγραμματισμός.

οπότε η πιθανότητα μετάδοσης σωστού χαρακτήρα είναι ίση με $1-p$, δηλαδή:

$$p(\textit{ελήφθη ο χαρακτήρας } 0 \mid \textit{εστάλη ο χαρακτήρας } 0) = \\ = p(\textit{ελήφθη ο χαρακτήρας } 1 \mid \textit{εστάλη ο χαρακτήρας } 1) = 1-p.$$

Υποθέτουμε ότι ο δέκτης λαμβάνει τη λέξη $\mathbf{x} = x_1\, x_2 \cdots x_n$, ενώ εστάλη η λέξη $\mathbf{c} = c_1\, c_2 \cdots c_n$. Θέλουμε να υπολογίσουμε την πιθανότητα:

$$p(\textit{ελήφθη η λέξη } \mathbf{x} \mid \textit{εστάλη η λέξη } \mathbf{c}\,).$$

Αν κατά τη μετάδοση υπεισήλθαν k το πλήθος λάθη (δηλαδή το διάνυσμα λάθους έχει βάρος k), τότε, σύμφωνα με την σχέση (1.1), έχουμε:

$$p(\ \textit{ελήφθη η}\ \ \mathbf{x}\ \mid\ \ \textit{εστάλη η}\ \mathbf{c}\,) = \\ = \prod_{i=1}^{n} p(\textit{ελήφθη ο}\, x_i \mid \textit{εστάλη ο}\ \ c_i) = p^k(1-p)^{n-k}.$$

Επειδή $p < 1/2$,[12] έχουμε $1-p > p$. Επομένως, η προηγούμενη πιθανότητα γίνεται όσο το δυνατόν μεγαλύτερη (Αρχή της μέγιστης πιθανότητας), όταν ο εκθέτης $n-k$ γίνεται όσο το δυνατόν μεγαλύτερος, δηλαδή ο k γίνεται όσο το δυνατόν μικρότερος, άρα όσο η λέξη $\mathbf{x}$ είναι πλησιέστερα στη λέξη $\mathbf{c}$ (Αρχή της πλησιέστερης λέξης). Δηλαδή αποδείξαμε το εξής σημαντικό Θεώρημα.

Θεώρημα 1.3.21. *Σε έναν δυαδικό, συμμετρικό δίαυλο η Αρχή της αποκωδικοποίησης μέγιστης πιθανότητας είναι η ίδια με την Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη.*

Παρατήρηση 1.3.22. Το θεώρημα αυτό ισχύει στη γενική περίπτωση ενός συμμετρικού δίαυλου επικοινωνίας με αλφάβητο $\mathbb{A} = \{\, a_1, a_2, \ldots, a_r\}$ με μόνη προϋπόθεση οι πιθανότητες μετάδοσης:

$$p_{ij} = p(\textit{ελήφθη ο χαρακτήρας}\, a_i \mid \textit{εστάλη ο χαρακτήρας}\, a_j) = p$$

[12] Στην περίπτωση, όπου $p = 1/2$, δεν έχουμε επικοινωνία, καθότι οι πιθανότητες $p(\ \textit{ελήφθη η}\ \ \mathbf{x}\ \mid\ \ \textit{εστάλη η}\, \mathbf{c}\,)$ είναι όλες ίσες, ανεξαρτήτως της απόστασης της λέξης $\mathbf{x}$ από την (κωδικο)λέξη $\mathbf{c}$.

Στην περίπτωση, όπου $p > 1/2$, ακολουθούμε την τακτική που υπαγορεύεται από την Άσκηση 7 της προηγουμένης παραγράφου.

να πληρούν τη σχέση $p < \frac{1}{2(r-1)}$, ούτως ώστε η πιθανότητα:

$$\begin{aligned} p_{ii} &= p(\textit{ελήφθη ο χαρακτήρας } a_i \mid \textit{εστάλη ο χαρακτήρας } a_i) \\ &= 1-(r-1)p > 1-(r-1)\cdot\frac{1}{2(r-1)} = 1/2. \end{aligned}$$

Η απόδειξη, αν και πιο σύνθετη, είναι ακριβώς η ίδια, ως προς την ιδέα, με την προηγούμενη. (Να δώσετε, με κάθε λεπτομέρεια, μια απόδειξη.)

1.3.3 Ταυτόχρονη ανίχνευση και διόρθωση λαθών

Έστω ότι έχουμε έναν κώδικα $\mathcal{C}$ με ελάχιστη απόσταση $d(\mathcal{C}) = d$. Σύμφωνα με τα προηγούμενα, αν ο $\mathcal{C}$ χρησιμοποιηθεί μόνο για ανίχνευση λαθών, θα ανιχνεύει (μέχρι) $d-1$ το πλήθος λάθη. Αν χρησιμοποιηθεί μόνο για διόρθωση λαθών, θα διορθώνει (μέχρι) $\left\lfloor \frac{d-1}{2} \right\rfloor$ το πλήθος λάθη. Συνήθως όμως ένας κώδικας χρησιμοποιείται ταυτόχρονα και για διόρθωση λαθών και για ανίχνευση λαθών.

Η ταυτόχρονη χρήση ενός κώδικα για διόρθωση και ανίχνευση λαθών είναι 'συμφέρουσα' ως προς την εξοικονόμηση ενέργειας, χρόνου, χρημάτων κ.λ.π., αλλά χρειάζεται να είμαστε προσεκτικοί ως προς τον μέγιστο αριθμό λαθών που μπορεί να ανιχνεύσει, εφόσον αυτά δεν έχουν 'διορθωθεί'.

Μια αβασάνιστη σκέψη θα έλεγε ότι αν σε μια (κωδικο)λέξη έχουν υπεισέλθει περισσότερα από $\left\lfloor \frac{d-1}{2} \right\rfloor$, αλλά λιγότερα από $d-1$ το πλήθος λάθη, τότε ο κώδικας θα επισημάνει την ύπαρξη λαθών. Αυτό αποτελεί εσφαλμένη αντίληψη, όπως θα δούμε από το εξής απλό παράδειγμα. Έστω $\mathcal{C}$ ο δυαδικός κώδικας $\{\,000000,\, 111111\,\}$. Υποθέτουμε ότι αποστέλεται η (κωδικο)λέξη $\mathbf{c} = 000000$ και λαμβάνεται η λέξη $\mathbf{x} = 111100$ (έχουν υπησέλθει τέσσερα λάθη). Σύμφωνα με την Αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x} = 111100$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{b} = 111111$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος παρόλο που ο κώδικας ανιχνεύει (μέχρι) πέντε λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών.

Στο παράδειγμα αυτό η ελάχιστη απόσταση είναι 6, άρτιος αριθμός. Πριν προχωρήσουμε στην διατύπωση και απόδειξη ενός γενικού αποτελέσματος, ας δούμε ένα παράδειγμα ενός κώδικα με περιττή ελάχιστη απόσταση. Έστω $\mathcal{C}$ ο

δυαδικός κώδικας $\{\, 1110000,\ 1011111 \,\}$. Ο κώδικας διορθώνει ακριβώς 2 λάθη. Υποθέτουμε ότι αποστέλεται η (κωδικο)λέξη $\mathbf{c} = 1011111$ και λαμβάνεται η λέξη $\mathbf{x} = 1011000$ (έχουν υπησέλθει τρία λάθη). Σύμφωνα με την Αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x} = 1011000$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{b} = 1110000$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος παρόλο που ο κώδικας ανιχνεύει (μέχρι) τέσσερα λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών. Μάλιστα δε, θα μπορούσαμε να πούμε ότι ανιχνεύει τόσα λάθη όσα διορθώνει.

Θεώρημα 1.3.23. *Έστω $\mathcal{C}$ ο κώδικας με ελάχιστη απόσταση $d(\mathcal{C}) = d$.*

1. *Υποθέτουμε ότι $d = 2\lambda+2$. Αν ο κώδικας χρησιμοποιηθεί για διόρθωση και ανίχνευση λαθών, τότε διορθώνει ακριβώς λ το πλήθος λάθη και ανιχνεύει $\lambda+1$ το πλήθος λάθη, αλλά υπάρχουν διανύσματα λάθους με βάρος μεγαλύτερο από $\lambda+1$ τα οποία δεν ανιχνεύονται.*

2. *Υποθέτουμε ότι $d = 2\lambda+1$. Αν ο κώδικας χρησιμοποιηθεί για διόρθωση και ανίχνευση λαθών, τότε διορθώνει ακριβώς λ το πλήθος λάθη και δεν ανιχνεύει $\lambda+1$ το πλήθος λάθη, δηλαδή υπάρχουν διανύσματα λάθους με βάρος $\lambda+1$ τα οποία δεν ανιχνεύονται.*

Απόδειξη. Υποθέτουμε ότι η ελάχιστη απόσταση του κώδικα είναι άρτια της μορφής $d = 2\lambda + 2$. Από τα προηγούμενα (ιδέ Πρόταση 1.3.17) έχουμε ότι ο κώδικας διορθώνει ακριβώς λ το πλήθος λάθη. Έστω τώρα ότι εστάλη η (κωδικο)λέξη $\mathbf{c}$ και ελήφθη η λέξη $\mathbf{x}$ στην οποία έχουν υπεισέλθει $\lambda+1$ λάθη. Κάθε (κωδικο)λέξη απέχει από την $\mathbf{x}$ απόσταση τουλάχιστον ίση με $\lambda+1$. Πράγματι, αν υπήρχε μια (κωδικο)λέξη $\mathbf{d}$ με $d(\mathbf{x}, \mathbf{d}) \leq \lambda$, τότε θα είχαμε $d(\mathbf{c}, \mathbf{d}) \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{d}) \leq \lambda + 1 + \lambda < 2\lambda + 2 = d$, άτοπο. Επομένως, η $\mathbf{x}$ δεν αποκωδικοποιείται και ανιχνεύεται το λάθος.

Έστω τώρα $\mathbf{c}$ και $\mathbf{d}$ δύο (κωδικο)λέξεις με απόσταση ίση με την ελάχιστη απόσταση του κώδικα. Επειδή η ελάχιστη απόσταση είναι ίση με $d = 2\lambda+2$, υπάρχει τουλάχιστον μια λέξη $\mathbf{x}$ η οποία απέχει από την $\mathbf{c}$ απόσταση $\lambda+2$ και από την $\mathbf{d}$ απόσταση λ (γιατί υπάρχει τέτοια λέξη;). Υποθέτουμε ότι εστάλη η λέξη $\mathbf{c}$, υπεισήλθαν $\lambda+2$ το πλήθος λάθη και αντ' αυτής λάβαμε τη λέξη $\mathbf{x}$. Σύμφωνα με την Αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη,

η λέξη $\mathbf{x}$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{d}$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος, παρόλο που ο κώδικας ανιχνεύει (μέχρι) $2\lambda+1$ λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών.

Στην περίπτωση, όπου η ελάχιστη απόσταση του κώδικα είναι περιττή της μορφής $d = 2\lambda+1$, πάλι ο κώδικας διορθώνει ακριβώς λ το πλήθος λάθη. Αν οι (κωδικο)λέξεις $\mathbf{c}$ και $\mathbf{d}$ απέχουν απόσταση ίση με την ελάχιστη απόσταση του κώδικα, τότε υπάρχει τουλάχιστον μια λέξη $\mathbf{x}$ η οποία απέχει από την $\mathbf{c}$ απόσταση $\lambda+1$ και από την $\mathbf{d}$ απόσταση λ (γιατί υπάρχει τέτοια λέξη;). Υποθέτουμε ότι εστάλη η λέξη $\mathbf{c}$, υπεισήλθαν $\lambda+1$ το πλήθος λάθη και αντ' αυτής λάβαμε τη λέξη $\mathbf{x}$. Σύμφωνα με την Αρχή αποκωδικοποίησης ως προς την πλησιέστερη λέξη, η λέξη $\mathbf{x}$ θα αποκωδικοποιηθεί (κακώς) ως η λέξη $\mathbf{d}$ και ο κώδικας **δεν** θα ανιχνεύσει το λάθος, παρόλο που ο κώδικας ανιχνεύει (μέχρι) 2λ λάθη, αν χρησιμοποιηθεί μόνο για ανίχνευση λαθών. ό.έ.δ.

1.3.4 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Υποθέτουμε ότι έχουμε τον δυαδικό κώδικα $\mathcal{C} = \{\,0000,\ 1111\,\}$ και για την μετάδοση χρησιμοποιούμε έναν συμμετρικό δίαυλο επικοινωνίας με πιθανότητα μετάδοσης $p = 0,01$. Αν λάβαμε τις λέξεις 0000, 0010, 1010, εφαρμόστε την Αρχή αποκωδικοποίησης μεγίστης πιθανότητας για να αποκωδικοποιήσετε αυτές τις λέξεις.

   Όμοια για τον κώδικα $\mathcal{C} = \{\,000,\ 001,\ 111\,\}$ και για τις ληφθείσες λέξεις 010, 101, 110.

3. Υποθέτουμε ότι έχουμε τον κώδικα $\mathcal{C} = \{\,000,\ 001,\ 111\,\}$ και τις ληφθείσες λέξεις 010, 101, 110 μέσω ενός δυαδικού διαύλου επικοινωνίας με πιθανότητες μετάδοσης $p(\,\textit{ελήφθη το}\ 0 \mid \textit{εστάλη το}\ \ 0) = 3/4$ και $p(\,\textit{ελήφθη το}\ 1 \mid \textit{εστάλη το}\ \ 1) = 7/8$. Εφαρμόστε την Αρχή αποκωδικοποίησης μεγίστης πιθανότητας για να αποκωδικοποιήσετε αυτές τις λέξεις.

4. Εξετάστε αν υπάρχουν δυαδικοί κώδικες που να διορθώνουν ένα λάθος με παραμέτρους $(5,\, 6),\ (6,\, 9)$.

   Εξετάστε αν υπάρχουν δυαδικοί κώδικες που να διορθώνουν δύο λάθη με παραμέτρους $(8,\ 4),\ (8,\ 5)$.

5. Δείξτε ότι σε έναν τριαδικό κώδικα με παραμέτρους $(3,\, M,\, 2)$ πρέπει να ισχύει $M \leq 9$.

   Κατασκευάστε έναν τριαδικό $(3,\, 9,\, 2)$ κώδικα.

6. Να κατασκευάσετε ή να αποδείξετε ότι δεν υπάρχουν δυαδικοί κώδικες με παραμέτρους $(8, 2, 8)$, $(8, 3, 8), (3, 9, 1), (4, 8, 2), (5, 3, 4)$.

7. Θεωρούμε έναν κώδικα, του οποίου τα στοιχεία είναι όλες οι λέξεις από το $\mathbb{Z}_2^n$ με άρτιο το πλήθος χαρακτήρες ίσον με 1. Να υπολογίσετε το μέγεθος και την ελάχιστη απόσταση αυτού του κώδικα.

8. Να υπολογίσετε την πιθανότητα σωστής αποκωδικοποίησης για τον κώδικα $\mathcal{C} = \{\, 00000,\, 11111 \,\}$, όπου η αποστολή γίνεται μέσω ενός δυαδικού συμμετρικού διαύλου επικοινωνίας με πιθανότητα μετάδοσης ίση με $p = 0,001$.

9. Έστω $\mathcal{C}$ ένας κώδικας με παραμέτρους $(15,\, 2^{11},\, 3)$. Να υπολογίσετε την μέγιστη πιθανότητα σωστής αποκωδικοποίησης, όταν για την μετάδοση χρησιμοποιείται ένας δυαδικός συμμετρικός δίαυλος επικοινωνίας με πιθανότητα μετάδοσης ίση με p.

10. Έστω $\mathcal{C}$ ένας κώδικας με ελάχιστη απόσταση ίση με $d(\mathcal{C}) \geq 2\lambda + \mu + 1$. Δείξτε ότι ο $\mathcal{C}$ μπορεί ταυτόχρονα να διορθώνει λ και να ανιχνεύει μ το πλήθος λάθη.

11. Οι λέξεις $0\,8218\,26 - 8\,X$, $- - 87\,94703\,3$ αποτελούν στοιχεία του κώδικα ISBN, αλλά κατά τη διάρκεια της μετάδοσης 'χάθηκαν' ορισμένοι χαρακτήρες (οι παύλες δηλώνουν τη θέση, όπου ο αντίστοιχος χαρακτήρας χάθηκε). Μπορείτε να εκτιμήσετε τους χαρακτήρες που χάθηκαν;

12. Έστω $\mathcal{C}$ ο κώδικας, του οποίου τα στοιχεία είναι λέξεις μήκους δέκα και το άθροισμα των χαρακτήρων μιας λέξης είναι πολλαπλάσιο του 11. Δηλαδή: $\mathcal{C} = \{\, x_1x_2\cdots x_{10} \mid x_i = 0, 1, \ldots, 9,\ \sum_{i=1}^{10} x_i \equiv 0 \bmod 11 \,\}$. Δείξτε ότι ο $\mathcal{C}$ ανιχνεύει ένα λάθος.

    Σε τι μειονεκτεί έναντι του κώδικα ISBN;

1.4 Κώδικες που προέρχονται από άλλους κώδικες

Έστω $\mathcal{C}$ ένας κώδικας επί του αλφάβητου $\mathbb{A}$ με παραμέτρους (n, M, d). Όπως έχουμε παρατηρήσει κάθε μία από τις παραμέτρους n, M και d έχει τη σημασία της ως προς την *αποτελεσματικότητα* του κώδικα. Το μήκος n των (κωδικο)λέξεων έχει σχέση με το *μέγεθος* της πληροφορίας που μπορεί να μεταδοθεί μέσω μιας (κωδικο)λέξης, αλλά υπόκειται σε *φυσικούς* περιορισμούς, όπως είναι ο χρόνος που απαιτείται για τη μετάδοση μιας λέξης ή η απαιτούμενη μνήμη για την αποθήκευση μιας λέξης. Το πλήθος M των *διαθέσιμων* (κωδικο)λέξεων έχει σχέση με το *πλήθος* των πληροφοριών που μπορούν να μεταδοθούν μέσω του κώδικα. Η ελάχιστη απόσταση d έχει σχέση με την δυνατότητα που έχει ο κώδικας να ανιχνεύει και να διορθώνει λάθη, αλλά έχει και άμεση σχέση τόσο με το μήκος του κώδικα, όσο και με το μέγεθός του. Οι τρεις αυτές παράμετροι βρίσκονται *αντιμέτωπες* και ο προσδιορισμός του *καταλληλότερου* κώδικα εξαρτάται τόσο από τη φύση των μεταδιδόμενων μηνυμάτων, όσο και από τα διαθέσιμα μέσα.

1.4.1 Μερικές περιπτώσεις 'μετασκευής' κωδίκων

Στην παράγραφο αυτή θα δούμε, σε πολύ λίγες περιπτώσεις, πώς από έναν δεδομένο κώδικα μπορούμε να κατασκευάσουμε έναν *βελτιωμένο* κώδικα, ο οποίος να πληροί ορισμένες προϋποθέσεις που δεν πληροί ο προηγούμενος κώδικας.

Σημείωση: Η έκφραση βελτιωμένος κώδικας είναι σχετική και επιδέχεται πολλές ερμηνείες, για τον λόγο αυτό στα επόμενα, τις περισσότερες φορές, θα γίνεται προσπάθεια κατά περίπτωση να διευκρινίζεται ως προς τι έγκειται η βελτίωση.

Ισοδύναμοι κώδικες

Όπως σε όλους τους κλάδους των Μαθηματικών, η έννοια της ισοδυναμίας είναι θεμελιώδης. Έτσι και στη θεωρία κωδίκων, η έννοια των ισοδυνάμων κωδίκων είναι πολύ βασική. Δεδομένου ότι ισοδύναμοι κώδικες είναι στην πραγματικότητα 'ίδιοι', όσον αφορά το μήκος, το μέγεθος, την ελάχιστη απόσταση και συνεπώς την ικανότητα να ανιχνεύουν/διορθώνουν λάθη.

Ορισμός 1.4.1. *Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας επί του αλφάβητου $\mathbb{A}$. Θεωρούμε την εξής διαδικασία* μετασχηματισμού *του $\mathcal{C}$.*

1. Για μια δεδομένη μετάθεση σ στα σύμβολα $\{1, 2, ..., n\}$ αντικαθιστούμε κάθε (κωδικο)λέξη $\mathbf{c} = c_1 c_2 \cdots c_n$ με την λέξη $c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}$, οπότε προκύπτει ένας νέος κώδικας, έστω $\mathcal{D}$.

2. Σε κάθε θέση i των χαρακτήρων (κάθε) μιας (κωδικο)λέξης εφαρμόζουμε μια μετάθεση π_i στους χαρακτήρες του αλφάβητου $\mathbb{A}$, οπότε μια (κωδικο)λέξη, έστω $\mathbf{d} = d_1 d_2 \cdots d_n$ την αντικαθιστούμε με την λέξη $\pi_1(d_1)\pi_2(d_2) \cdots \pi_n(d_n)$. Συνεπώς, προκύπτει ένας νέος κώδικας, έστω $\mathcal{F}$.

Ο κώδικας που προκύπτει σύμφωνα με την παραπάνω διαδικασία ονομάζεται ***ισοδύναμος*** *προς τον κώδικα $\mathcal{C}$.*

Παρατήρηση 1.4.2. Πρέπει να παρατηρήσουμε ότι κατά το πρώτο στάδιο σε κάθε (κωδικο)λέξη γίνεται μετάθεση των χαρακτήρων της, δηλαδή ένας *αναγραμματισμός*, ο οποίος *υπαγορεύεται* από την ίδια μετάθεση σε όλες τις (κωδικο)λέξεις.

Κατά το δεύτερο στάδιο, εφαρμόζονται n το πλήθος μεταθέσεις στα στοιχεία του αλφάβητου και μετά, από κάθε (κωδικο)λέξη κατασκευάζεται η νέα (κωδικο)λέξη αντικαθιστώντας σε κάθε θέση τον αντίστοιχο χαρακτήρα.

Επειδή κάθε μετάθεση είναι μια αντιστρέψιμη απεικόνιση, προφανώς, αν ο κώδικας $\mathcal{E}$ είναι ισοδύναμος προς τον κώδικα $\mathcal{C}$, τότε και ο κώδικας $\mathcal{C}$ είναι ισοδύναμος προς τον κώδικα $\mathcal{E}$. Επομένως, στο εξής μπορούμε να λέμε οτι οι δύο κώδικες είναι ισοδύναμοι χωρίς διάκριση.

Μάλιστα μπορούμε να αποδείξουμε ότι στο σύνολο των κωδίκων μήκους n επί ενός αλφάβητου $\mathbb{A}$ η ισοδυναμία κωδίκων αποτελεί σχέση ισοδυναμίας. (γιατί;)

Το ότι ισοδύναμοι κώδικες είναι ίδιοι, όπως προείπαμε, φαίνεται από το ακόλουθο θεώρημα.

Θεώρημα 1.4.3. *Ισοδύναμοι κώδικες έχουν τις ίδιες παραμέτρους (μήκος, μέγεθος και ελάχιστη απόσταση).*

Απόδειξη. Η απόδειξη αποτελεί μια απλή εφαρμογή του ορισμού και αφίεται ως άσκηση. ό.έ.δ.

Παράδειγμα 1.4.4. Έστω $\mathcal{C}$ ο τριαδικός κώδικας $\{\,120,\,102,\,210,\,110,\,212\,\}$. Επιλέγουμε τις μεταθέσεις $\pi_1 : (0 \to 1, 1 \to 0, 2 \to 2)$, $\pi_2 : (0 \to 2, 1 \to 1, 2 \to 0)$, $\pi_3 = (0 \to 0, 1 \to 1, 2 \to 2)$ και τις εφαρμόζουμε στα στοιχεία του κώδικα σύμφωνα με το δεύτερο βήμα της παραπάνω διαδικασίας. Δεν είναι δύσκολο να δούμε ότι ο ισοδύναμος κώδικας που προκύπτει είναι ο κώδικας $\mathcal{F} = \{\,000,\,022,\,210,\,010,\,212\,\}$.

Στο προηγούμενο παράδειγμα βλέπουμε ότι στον κώδικα $\mathcal{F}$ υπάρχει η (κωδικο)λέξη 000, όπου όλοι οι χαρακτήρες είναι ίδιοι. Αυτό μπορούμε να το πετύχουμε σε οποιονδήποτε κώδικα. Συγκεκριμένα ισχύει η εξής σημαντική πρόταση.

Πρόταση 1.4.5. *Έστω $\mathcal{C}$ ένας (n, M) κώδικας επί του αλφάβητου $\mathbb{A}$. Επιλέγουμε και σταθεροποιούμε ένα γράμμα $a \in \mathbb{A}$. Τότε υπάρχει κώδικας ισοδύναμος με τον κώδικα $\mathcal{C}$, ο οποίος περιέχει την (κωδικο)λέξη $\mathbf{a} = (a, a, \ldots, a)$*

Απόδειξη. Η απόδειξη είναι απλή και αφίεται ως άσκηση, αρκεί να προσέξουμε καλά το προηγούμενο παράδειγμα. ό.έ.δ.

Εδώ είναι σκόπιμο να αναφέρουμε ότι, αν θέλουμε να εφαρμόσουμε το πρώτο βήμα μετασχηματισμού ενός κώδικα σε έναν ισοδύναμό του, μπορούμε να ενεργήσουμε ως εξής:
Έστω σ μια μετάθεση των στοιχείων του συνόλου $\{\,1, 2, \ldots, n\,\}$ και I_n ο ταυτοτικός $n \times n$ πίνακας. Στις γραμμές του I_n εφαρμόζουμε την μετάθεση σ. Για παράδειγμα, αν $\sigma(i) = j_i$, μεταθέτουμε την i-γραμμή στη θέση της j_i-γραμμής κ.ο.κ.. Οπότε προκύπτει ένας $n \times n$ πίνακας P_σ, όπου στις (j_i, i)

θέσεις, για $i = 1, 2, \ldots, n$ έχει 1 και σε όλες τις υπόλοιπες 0. Ο πίνακας P_σ ονομάζεται, συνήθως, **πίνακας μετάθεση** (ως προς τη μετάθεση σ). Υποθέτουμε τώρα ότι έχουμε την (κωδικο)λέξη $\mathbf{c} = c_1 c_2 \cdots c_n$. Δεν είναι δύσκολο να δούμε ότι αν θεωρήσουμε την $\mathbf{c}$ σαν έναν πίνακα γραμμή και κάνουμε τον πολλαπλασιασμό $\mathbf{c}P_\sigma$, τότε έχουμε ως αποτέλεσμα $\mathbf{c}P_\sigma = c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}$. Δηλαδή έχουμε αποδείξει την εξής πρόταση.

Πρόταση 1.4.6. *Για κάθε μετάθεση σ και κάθε κώδικα $\mathcal{C}$ μπορούμε να κατασκευάσουμε έναν ισοδύναμο κώδικα:* $\mathcal{C}_\sigma = \{\, \mathbf{c}P_\sigma \mid \mathbf{c} \in \mathcal{C} \,\}$.

Θα δούμε τη χρησιμότητα αυτής της πρότασης αργότερα, όταν ασχοληθούμε με γραμμικούς κώδικες.

Οι κώδικες $\mathcal{C}$ και $\mathcal{C}_\sigma$ θα λέγονται μεταθετικά ισοδύναμοι.

Έστω S_n η ομάδα όλων των μεταθέσεων σε n σύμβολα.
Έστω $\mathcal{C}$ ένας κώδικας μήκους n, το σύνολο $\mu Aut(\mathcal{C}) = \{\, \sigma \in S_n$ με την ιδιότητα $\mathcal{C}_\sigma = \mathcal{C} \,\}$ προφανώς (γιατί;) αποτελεί υποομάδα της S_n και ονομάζεται **ομάδα μεταθετικών αυτομορφισμών** του κώδικα $\mathcal{C}$.

Ο προσδιορισμός της ομάδας $\mu Aut(\mathcal{C})$ για έναν κώδικα αποτελεί δύσκολο πρόβλημα. Θα επανέλθουμε αργότερα στην περίπτωση των γραμμικών κωδίκων.

Αν και δεν έχουμε ορίσει τους Golay κώδικες, θα αναφέρουμε ένα παράδειγμα *μοναδικότητας* κωδίκων, επικαλούμενοι ότι ισοδύναμοι κώδικες είναι ίδιοι, σύμφωνα με το Θεώρημα 1.4.3.

Θεώρημα 1.4.7. *Κάθε δυαδικός* $(24, 4096, 8)$*-κώδικας είναι ισοδύναμος με τον* $\mathcal{G}_{24}$ *Golay κώδικα.*

Απόδειξη. Η απόδειξη απαιτεί γνώσεις από τους γραμμικούς κώδικες.

Βλέπε τη σχετική συζήτηση στην Παράγραφο 4.3 και το Θεώρημα 4.3.3.

ό.έ.δ.

Επέκταση ενός κώδικα

Έστω $\mathcal{C}$ ένας κώδικας. Μπορούμε να αυξήσουμε το μήκος κάθε (κωδικο)λέξης παρεμβάλλοντας, π.χ. μεταξύ της i και $i+1$ συντεταγμένης, έναν

χαρακτήρα. Τότε προκύπτει ένας νέος κώδικας $\widehat{\mathcal{C}}$ με το ίδιο πλήθος στοιχείων, ο οποίος ονομάζεται **επέκταση** του $\mathcal{C}$.

Η κατάσταση που μόλις περιγράψαμε είναι τελείως γενική, καθότι η *αυθαιρεσία* στην παρεμβολή επιπλέον χαρακτήρων, παρόλο που αυξάνει το μήκος του, δεν προσφέρει στη βελτίωση του αρχικού κώδικα. Στην πράξη έχει επικρατήσει ο επιπλέον χαρακτήρας να επισυνάπτεται στο τέλος κάθε (κωδικο)λέξης, να μην είναι τυχαίος, αλλά να εξαρτάται από τους προηγούμενους χαρακτήρες. Συγκεκριμένα, μια επέκταση ενός κώδικα $\mathcal{C}$ μήκους n είναι ο κώδικας $\widehat{\mathcal{C}} = \{\, c_1c_2\cdots c_nc_{n+1} \mid c_1c_2\cdots c_n \in \mathcal{C} \text{ και } \sum_{i=1}^{n+1} c_i = 0 \,\}$.

Ο επιπλέον χαρακτήρας c_{n+1} που επισυνάπεται ονομάζεται **ψηφίο ελέγχου ισοτιμίας**.

Προφανώς, ο κώδικας $\widehat{\mathcal{C}}$ έχει μήκος ίσο με $n+1$, μέγεθος ίσο με το μέγεθος του $\mathcal{C}$ και ελάχιστη απόσταση ίση με d ή $d+1$ (γιατί;), όπου d είναι η ελάχιστη απόσταση του κώδικα $\mathcal{C}$.

Γενικά, ένας κώδικας με την ιδιότητα το άθροισμα των χαρακτήρων σε κάθε (κωδικο)λέξη να είναι ίσον με μηδέν ονομάζεται κώδικας **μηδενικού αθροίσματος**.

Παραδείγματα 1.4.8. 1. Έστω $\mathcal{C}$ ο δυαδικός κώδικας: $\{\, 00,\, 01,\, 10,\, 11 \,\}$. Προσθέτοντας ένα ψηφίο ελέγχου ισοτιμίας, η επέκταση του $\mathcal{C}$ είναι ο κώδικας $\widehat{\mathcal{C}} = \{\, 000,\, 011,\, 101,\, 110 \,\}$, ο οποίος έχει ελάχιστη απόσταση δύο, ενώ ο $\mathcal{C}$ έχει ελάχιστη απόσταση ένα.

2. Έστω $\mathcal{C}$ ο τριαδικός κώδικας $\{\, 102,\, 210,\, 021 \,\}$, η επέκτασή του είναι ο κώδικας $\widehat{\mathcal{C}} = \{\, 1020,\, 2100,\, 0210 \,\}$, ο οποίος έχει ελάχιστη απόσταση τρία, εδώ όμως και ο $\mathcal{C}$ έχει ελάχιστη απόσταση τρία.

Για δυαδικούς κώδικες ισχύει η επομένη πρόταση.

Πρόταση 1.4.9. *Έστω $\mathcal{C}$ ένας δυαδικός κώδικας. Η ελάχιστη απόσταση της επέκτασης $\widehat{\mathcal{C}}$ είναι πάντα άρτια. Επομένως, ο $\widehat{\mathcal{C}}$ διορθώνει τόσα λάθη όσα και ο αρχικός, αλλά ενδέχεται να ανιχνεύει ένα επιπλέον λάθος απ' ότι ο αρχικός κώδικας.*

Απόδειξη. Η απόδειξη είναι απλή, αρκεί να παρατηρήσουμε ότι στην επέκταση όλες οι λέξεις είναι αρτίου βάρους και να εφαρμόσουμε τα Θεωρήματα 1.3.14 και 1.3.16. ό.έ.δ.

Σύμπτυξη ενός κώδικα

Η αντίστροφη διαδικασία της επέκτασης ενός κώδικα είναι η **σύμπτυξη**.

Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας. Κατασκευάζουμε έναν $M \times n$ πίνακα του οποίου οι γραμμές είναι τα στοιχεία του κώδικα $\mathcal{C}$ και διαγράφουμε μία στήλη του. Δηλαδή διαγράφουμε από όλες τις (κωδικο)λέξεις τον χαρακτήρα σε μια συγκεκριμένη συντεταγμένη. Στον πίνακα που προκύπτει ενδέχεται να έχουμε γραμμές που είναι ίδιες. Οι διαφορετικές γραμμές του πίνακα αυτού αποτελούν τα στοιχεία ενός **συνεπτυγμένου** κώδικα με παραμέτρους $(n-1, \overline{M}, \bar{d})$, όπου $\overline{d} = d$ ή $d-1$ (γιατί;).

Η πλέον συνηθισμένη περίπτωση σύμπτυξης κώδικα είναι, όταν σε όλες τις (κωδικο)λέξεις σε μια συγκεκριμένη θέση εμφανίζεται ο ίδιος χαρακτήρας. Τότε ο χαρακτήρας αυτός **δεν** προσφέρει τίποτε στην μετάδοση πληροφοριών, οπότε συμπτύσσουμε τον κώδικα ως προς αυτή τη συντεταγμένη και λαμβάνουμε τον *ίδιο* κώδικα, αλλά σε *οικονομικότερη* μορφή.[13]

Με τη βοήθεια των διαδικασίων επέκτασης/σύμπτυξης ενός κώδικα μπορούμε να αποδείξουμε το εξής Θεώρημα.

Θεώρημα 1.4.10. *Υπάρχουν δυαδικοί $(n, M, 2t+1)$ κώδικες, αν και μόνο αν υπάρχουν $(n+1, M, 2t+2)$ δυαδικοί κώδικες.*

Απόδειξη. Υποθέτουμε ότι έχουμε έναν δυαδικό $(n, M, 2t+1)$ κώδικα. Τον επεκτείνουμε προσθέτοντας ένα ψηφίο ελέγχου ισοτιμίας. Από την Πρόταση 1.4.9 έχουμε ότι η ελάχιστη απόσταση, του κώδικα που προκύπτει, είναι άρτια. Άρα έχουμε έναν $(n+1, M, 2t+2)$ κώδικα.

Αντίστροφα, υποθέτουμε ότι έχουμε έναν $(n+1, M, 2t+2)$ κώδικα. Έστω $\mathbf{c}, \mathbf{d}$ δύο (κωδικο)λέξεις του, οι οποίες απέχουν μεταξύ τους απόσταση ίση με την ελάχιστη απόσταση του κώδικα ($d(\mathbf{c}, \mathbf{d}) = 2t+2$). Επιλέγουμε μια

[13] Για τον λόγο, αυτό πολλοί στον ορισμό του κώδικα απαιτούν στις (κωδικο)λέξεις να μην υπάρχει κοινή συντεταγμένη.

συντεταγμένη στην οποία οι δύο λέξεις διαφέρουν και συμπτύσσουμε ως προς αυτή τη συντεταγμένη. Ο κώδικας που προκύπτει είναι ένας $(n, M, 2t+1)$ κώδικας. ό.έ.δ.

(Αποδελτίωση) Σμίκρυνση/Αύξηση ενός κώδικα

Ορισμένες φορές από έναν κώδικα διαγράφουμε ορισμένες (κωδικο)λέξεις, οπότε προκύπτει ένας νέος (υπο)κώδικας. Ο νέος κώδικας έχει το ίδιο μήκος με τον αρχικό κώδικα, αλλά μικρότερο μέγεθος, επομένως *φτωχώτερος* ως προς την μετάδοση πληροφοριών. Η ελάχιστη όμως απόσταση είναι μεγαλύτερη ή ίση από την ελάχιστη απόσταση του αρχικού κώδικα.

Η αντίστροφη διαδικασία, όπου σε έναν κώδικα επισυνάπτουμε νέες (κωδικο)λέξεις οδηγεί σε **αύξηση** του κώδικα και ο νέος κώδικας ονομάζεται **επαυξημένος**.

Παρατηρήσεις 1.4.11. 1. Η διαγραφή ορισμένων (κωδικο)λέξεων για να πετύχουμε μια σμίκρυνση ενός κώδικα (αντίστοιχα, η προσθήκη λέξεων για να πετύχουμε μια αύξηση) δεν γίνεται τυχαία αλλά βάσει ορισμένων κανόνων. Αργότερα θα μας δοθεί η ευκαιρία να μελετήσουμε διαδικασίες σμίκρυνσης/αύξησης κωδίκων.

2. Τις περισσότερες φορές σε έναν κώδικα μια σμίκρυνση ακολουθείται από μια σύμπτυξη. Συγκεκριμένα, σε έναν κώδικα κρατάμε όλες τις (κωδικο)λέξεις που έχουν μια κοινή συντεταγμένη και διαγράφουμε τις υπόλοιπες. Κατόπιν, συμπτύσσουμε τον (νέο) κώδικα διαγράφοντας την κοινή συντεταγμένη. Η όλη διαδικασία ονομάζεται **συμπύκνωση**.

   Για παράδειγμα, έστω $\mathcal{C}$ ο κώδικας $\{\,0000,\, 0110,\, 1010,\, 0011,\, 1110\,\}$. Σε πρώτη φάση κάνουμε μια σμίκρυνση διαγράφοντας τις λέξεις 1010 και 1110. Οι εναπομείνουσες λέξεις έχουν όλες στην πρώτη συντεταγμένη το μηδέν, οπότε το διαγράφουμε και έχουμε ως τελικό αποτέλεσμα τον συμπυκνωμένο κώδικα $\mathcal{D} = \{\,000,\, 110,\, 011\,\}$.

Θα περιγράψουμε μια συνηθισμένη αύξηση σε δυαδικούς κώδικες.

Καταρχήν, έστω $\mathbf{c}$ μια δυαδική λέξη μήκους n ($\mathbf{c} \in \mathbb{Z}_2^n$). Το **συμπλήρωμά** της $\mathbf{c}^c$ είναι μια λέξη μήκους n που προκύπτει από την $\mathbf{c}$ αν μετατρέψουμε τα

0 σε 1 και τα 1 σε 0. Δηλαδή το συμπλήρωμα της $\mathbf{c} = 10011$ είναι $\mathbf{c}^c = 01100$. Προφανώς, δύο λέξεις $\mathbf{c}$ και $\mathbf{d}$ είναι η μια συμπλήρωμα της άλλης αν και μόνο αν $\mathbf{c} + \mathbf{d} = \mathbf{1}$, όπου $\mathbf{1} = 11\cdots1$. Δηλαδή $\mathbf{c}^c = \mathbf{c} + \mathbf{1}$.

Έστω τώρα $\mathcal{C}$ ένας δυαδικός κώδικας μήκους n και $\mathcal{C}^c$ ο συμπληρωματικός του, δηλαδή $\mathcal{C}^c = \{\, \mathbf{c}^c \mid \mathbf{c} \in \mathcal{C} \,\}$. Το σύνολο $\mathcal{C} \cup \mathcal{C}^c$ αποτελεί μια αύξηση του κώδικα $\mathcal{C}$ (και του $\mathcal{C}^c$). Ας προσπαθήσουμε να υπολογίσουμε την ελάχιστη απόσταση του $\mathcal{C} \cup \mathcal{C}^c$.

Μια πρώτη παρατήρηση είναι ότι $d(\mathcal{C}) = d(\mathcal{C}^c)$ και για $\mathbf{c}, \mathbf{d} \in \mathbb{Z}_2^n$ ισχύει $d(\mathbf{c}, \mathbf{d}^c) = n - d(\mathbf{c}, \mathbf{d})$ (γιατί;).

Από τον ορισμό της ελάχιστης απόστασης έχουμε:

$$d(\mathcal{C} \cup \mathcal{C}^c) = min\{\, d(\mathcal{C}), d(\mathcal{C}^c), min\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{C}^c \,\} \,\}.$$

Αλλά:

$$min\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c} \in \mathcal{C}, \mathbf{d} \in \mathcal{C}^c \,\} = min\{\, d(\mathbf{c}, \mathbf{d}^c), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\}$$

(βάσει της προηγούμενης παρατήρησης)

$$\begin{aligned} &= min\{\, n - d(\mathbf{c}, \mathbf{d}), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\} \\ &= n - max\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\}. \end{aligned}$$

Επομένως:

$$d(\mathcal{C} \cup \mathcal{C}^c) = min\{\, d(\mathcal{C}), n - max\{\, d(\mathbf{c}, \mathbf{d}), \mathbf{c}, \mathbf{d} \in \mathcal{C} \,\} \,\}.$$

Στα επόμενα, όταν ασχοληθούμε με γραμμικούς κώδικες θα επανέλθουμε στο παράδειγμα αυτό (βλέπε Πρόταση 2.1.4).

Στο παράδειγμα 1.3.19 είχαμε ασχοληθεί με τον γνωστό κώδικα **ISBN**. Εδώ θα δούμε πώς ο κώδικας αυτός μπορεί να προέλθει ως σμίκρυνση ενός άλλου κώδικα.

Έστω $\mathcal{C} = \{\, \mathbf{c} = x_1x_2\cdots x_{10} \in \mathbb{Z}_{11}^{10} \mid x_{10} = x_1 + 2x_2 + 3x_3 + \cdots + 9x_9 \,\}$. Δεν είναι δύσκολο να αποδείξουμε ότι ο $\mathcal{C}$ είναι ένας $(\,10, 11^9, 2\,)$ κώδικας (γιατί;). Μάλιστα μπορούμε να αποδείξουμε ότι ο $\mathcal{C}$ είναι διανυσματικός χώρος επί του σώματος $\mathbb{Z}_{11}$ (αποδείξτε το!) με διάσταση 9. Από τον κώδικα

αυτό διαγράφουμε όλες τις (κωδικο)λέξεις στις οποίες σε μια από τις θέσεις $i = 1, 2, \ldots, 9$ εμφανίζεται "10", ενώ επιτρέπεται στην τελευταία θέση να εμφανίζεται το "10", οπότε προκύπτει ένας κώδικας, έστω $\mathcal{E}$. Δηλαδή $\mathcal{E} = \{\, \mathbf{c} = x_1x_2 \cdots x_{10} \in \mathcal{C} \mid x_1, x_2 \ldots, x_9 \neq 10 \,\}$. Επειδή ο χαρακτήρας "10" είναι διψήφιος, προς αποφυγήν σύγχυσης, συμφωνούμε να τον συμβολίζουμε με "X". Ο κώδικας $\mathcal{E}$ είναι ο γνωστός κώδικας **ISBN** (γιατί;).

Επαναληπτικοί κώδικες

Πολλές φορές, όταν μεταδίδουμε ένα μήνυμα, για να αισθανθούμε *περισσότερο βέβαιοι* ότι ο παραλήπτης θα είναι σε θέση να αποκωδικοποιήσει το μήνυμα σωστά, επαναλαμβάνουμε κάθε (κωδικο)λέξη περισσότερες από μια φορές. Για παράδειγμα, ας υποθέσουμε ότι θέλουμε να αποστείλουμε την (κωδικο)λέξη 1011. Αντ' αυτής αποστέλλουμε, επαναληπτικά, την λέξη 1011 1011 1011 (σκόπιμα στη γραφή παρεμβάλαμε κενά), οπότε αν έχει υπεισέλθει μόνο ένα λάθος, αυτό θα βρίσκεται σε μία από τις τρείς (υπο)λέξεις. Οι άλλες δύο (υπο)λέξεις είναι οι ίδιες και επομένως το λάθος εύκολα εντοπίζεται και διορθώνεται. Προφανώς, αν θέλουμε να διορθώσουμε δύο λάθη, τότε κάθε (κωδικο)λέξη κατά την αποστολή της πρέπει να επαναλαμβάνεται πέντε φορές. Γενικά, αν θέλουμε, με αυτό τον τρόπο, να διορθώνουμε λ το πλήθος λάθη, κάθε (κωδικο)λέξη κατά την αποστολή της πρέπει να επαναλαμβάνεται $2\lambda+1$ φορές.

Ορισμός 1.4.12. *Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας και k ένας θετικός ακέραιος. Ο κώδικας:*

$$\mathcal{C}_k = \{\ \underbrace{\mathbf{cc}\cdots\mathbf{c}}_{k-\text{φορές}} \mid \mathbf{c} \in \mathcal{C} \,\}$$

λέγεται k-επαναληπτικός κώδικας του $\mathcal{C}$.

Προφανώς, ο κώδικας $\mathcal{C}_k$ έχει μήκος $k \cdot n$, μέγεθος M και ελάχιστη απόσταση $k \cdot d$.

Η πλέον συνηθισμένη περίπτωση επαναληπτικού κώδικα είναι η εξής. Έστω $\mathbb{F} = \{\, a_1, a_2, \ldots, a_q \,\}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία

και k ένας θετικός ακέραιος. Ο κώδικας:

$$\mathcal{R}_q(k) = \{\underbrace{a_1a_1\cdots a_1}_{k-\text{φορές}}, \underbrace{a_2a_2\cdots a_2}_{k-\text{φορές}}, \ldots, \underbrace{a_qa_q\cdots a_q}_{k-\text{φορές}}\}$$

είναι ένας k-επαναληπτικός κώδικας. (Ποίου κώδικα είναι επαναληπτικός;)[14]

Παρατήρηση 1.4.13. Ένας επαναληπτικός κώδικας δεν είναι πλουσιώτερος του κώδικα από τον οποίο προέρχεται (και οι δύο έχουν το ίδιο μέγεθος), αλλά έχει την δυνατότητα να διορθώνει πολύ περισσότερα λάθη. Η δυνατότητα αυτή στην πράξη συνεκτιμάται με το γεγονός ότι το μήκος του είναι πολλαπλάσιο από το αντίστοιχο μήκος του αρχικού κώδικα, γεγονός που αυξάνει το κόστος σε χώρο, χρόνο, χρήμα.

Παράδειγμα 1.4.14. Έστω ότι εκτελούμε το πείραμα της ρίψης ενός νομίσματος και συμφωνούμε να μεταδίδουμε τα αποτελέσματα των ρίψεων χρησιμοποιώντας τον κώδικα $\mathcal{C} = \{0, 1\}$. Αν το αποτέλεσμα είναι γράμματα, αποστέλλουμε 0, ενώ αν το αποτέλεσμα είναι κεφαλή, αποστέλλουμε 1. Προφανώς, κάθε αλλοίωση του (μοναδικού) μεταδιδόμενου χαρακτήρα δίνει εσφαλμένο αποτέλεσμα κατά την αποκωδικοποίηση. (Ο κώδικας που χρησιμοποιούμε διορθώνει μηδέν το πλήθος λάθη, αφού έχει ελάχιστη απόσταση ένα). Αν τώρα συμφωνήσουμε να μεταδίδουμε τα αποτελέσματα των ρίψεων αποστέλλοντας 000 για το αποτέλεσμα γράμματα και 111 για το αποτέλεσμα κεφαλή χρησιμοποιώντας τον 3- επαναληπτικό κώδικα $\mathcal{C}_3 = \{000, 111\}$, τότε μπορούμε να ανιχνεύσουμε και να διορθώσουμε (μέχρι) ένα λάθος, αλλά δεν μπορούμε να ανιχνεύσουμε περισσότερα λάθη (βλέπε Θεώρημα 1.3.23).

Η $(\mathbf{u}, \mathbf{u}+\mathbf{v})$- κατασκευή

Θα τελειώσουμε την παράγραφο αναφέροντας έναν τρόπο κατασκευής ενός κώδικα από δύο άλλους κώδικες, είναι μια μέθοδος που εφαρμόζεται στην κατασκευή της οικογένειας των Reed-Muller κωδίκων (ιδέ στη σελίδα 257).

[14] Πολλοί συγγραφείς ορίζουν έτσι τους επαναληπτικούς κώδικες. Στα επόμενα και εμείς, όταν αναφερόμαστε σε επαναληπτικούς κώδικες, θα εννοούμε τους κώδικες $\mathcal{R}_q(k)$.

Έστω $\mathcal{C}_1, \mathcal{C}_2$ δύο κώδικες επί του ιδίου αλφάβητου, το οποίο είναι ένα πεπερασμένο σώμα, με παραμέτρους (n, M_1, d_1) και (n, M_2, d_2) αντίστοιχα. Για $\mathbf{c} \in \mathcal{C}_1$ και $\mathbf{d} \in \mathcal{C}_2$ λαμβάνουμε το άθροισμα $\mathbf{c}+\mathbf{d}$ (το άθροισμα ορίζεται κατά συντεταγμένες, καθότι οι δύο κώδικες είναι ισομήκεις και ορίσθηκαν επί του ιδίου αλφάβητου, το οποίο είναι σώμα). Κατόπιν, από την παράθεση των λέξεων $\mathbf{c}$ και $\mathbf{c}+\mathbf{d}$ προκύπει η λέξη $\mathbf{c}(\mathbf{c}+\mathbf{d})$. Εφαρμόζουμε τη διαδικασία αυτή για όλα τα στοιχεία των $\mathcal{C}_1$ και $\mathcal{C}_2$. Το σύνολο $\mathcal{C}_1 \odot \mathcal{C}_2 = \{\, \mathbf{c}(\mathbf{c}+\mathbf{d}) \mid \mathbf{c} \in \mathcal{C}_1, \mathbf{d} \in \mathcal{C}_2 \,\}$ είναι ένας $(2n, M_1 \cdot M_2, \bar{d}\,)$ κώδικας.

Ας υπολογίσουμε την ελάχιστη απόσταση $\bar{d}$. Θεωρούμε δύο (κωδικο)λέξεις $\mathbf{v}_1 = \mathbf{c}_1(\mathbf{c}_1+\mathbf{d}_1)$ και $\mathbf{v}_2 = \mathbf{c}_2(\mathbf{c}_2+\mathbf{d}_2)$. Διακρίνουμε περιπτώσεις, αν $\mathbf{d}_1 = \mathbf{d}_2$, τότε $d(\mathbf{v}_1, \mathbf{v}_2) = 2d(\mathbf{c}_1, \mathbf{c}_2) \geq 2d_1$. (Υπάρχουν (κωδικο)λέξεις $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_1$ που η προηγούμενη ανισότητα γίνεται ισότητα). Στην περίπτωση, όπου $\mathbf{d}_1 \neq \mathbf{d}_2$ έχουμε από την Πρόταση 1.2.11 ότι:

$$\begin{aligned} d(\mathbf{v}_1, \mathbf{v}_2) &= w(\mathbf{v}_1 - \mathbf{v}_2) \\ &= w(\mathbf{c}_1 - \mathbf{c}_2) + w(\mathbf{c}_1 - \mathbf{c}_2 + \mathbf{d}_1 - \mathbf{d}_2) \\ &\geq w(\mathbf{d}_1 - \mathbf{d}_2) \\ &= d(\mathbf{d}_1, \mathbf{d}_2) \geq d_2. \end{aligned}$$

Για $\mathbf{c}_1 = \mathbf{c}_2$ και $\mathbf{d}_1, \mathbf{d}_2 \in \mathcal{C}_2$, έτσι ώστε $d(\mathbf{d}_1, \mathbf{d}_2) = d_2$ οι προηγούμενες ανισότητες γίνονται ισότητες, οπότε έχουμε αποδείξει την εξής πρόταση.

Πρόταση 1.4.15. *Με τις προηγούμενες υποθέσεις έχουμε* $d(\mathcal{C}_1 \odot \mathcal{C}_2) = min\{\, 2d_1, d_2 \,\}$.

1.4.2 Μεγιστικοί κώδικες

Θεωρούμε, για παράδειγμα, τον δυαδικό κώδικα $\mathcal{C} = \{\, 0000, 1111, 0011 \,\}$ μήκους 4, μεγέθους 3 και ελάχιστης απόστασης 2. Ο κώδικας αυτός διορθώνει μηδέν το πλήθος λάθη (π.χ. Αν λάβουμε τη λέξη 0010, αυτή ισαπέχει από τις (κωδικο)λέξεις 0000 και 0011, άρα δεν διορθώνεται, παρόλο που διαφέρει από αυτές μόνο κατά ένα χαρακτήρα). Αυτό δεν σημαίνει ότι δεν μπορεί να διορθώσει καμία λέξη (π.χ. αν λάβουμε τη λέξη 1000, τότε αυτή κατά την αποκωδικοποίηση διορθώνεται και αποκωδικοποιείται ως η λέξη 0000). Αν

στον προηγούμενο κώδικα επισυνάψουμε τη λέξη 1100, τότε ο επαυξημένος κώδικας $\overline{\mathcal{C}} = \{\, 0000,\, 1111,\, 0011,\, 1100 \,\}$ έχει το ίδιο μήκος και την ίδια ελάχιστη απόσταση με τον κώδικα $\mathcal{C}$, αλλά δεν διορθώνει καμία λέξη με ένα λάθος (γιατί;). Πολύ δε περισσότερο πολλές λέξεις που λαμβάνονται και εμπεριέχουν δύο λάθη συμπίπτουν με (κωδικο)λέξεις, οπότε αποκωδικοποιούνται λανθασμένα (π.χ. αν έχει σταλεί η λέξη 0000 και λάβουμε τη λέξη 1100, τότε αυτή ανήκει στον κώδικα και επομένως θεωρείται, λανθασμένα, ότι εστάλη αυτή).

Επομένως, αναρωτιέται κάποιος, προς τι η αύξηση του δοθέντος κώδικα; Πέραν του ότι ο νέος κώδικας είναι *πλουσιώτερος* σε λέξεις, μπορούμε να διαχειρισθούμε αποτελεσματικότερα την πιθανότητα λανθασμένης αποκωδικοποίησης.

Ορισμός 1.4.16. *Ένας* $(n,\, M,\, d)$ *κώδικας* $\mathcal{C}$, *επί του αλφάβητου* $\mathbb{A}$, *θα λέγεται μεγιστικός, αν δεν υπάρχει ένας* $(n,\, M+1,\, d)$ *κώδικας* $\overline{\mathcal{C}}$, *επί του ιδίου αλφάβητου, έτσι ώστε* $\mathcal{C} \subseteq \overline{\mathcal{C}}$

Προφανώς, κάθε κώδικας περιέχεται σε (τουλάχιστον) ένα μεγιστικό κώδικα. Επίσης, ένας $(n,\, M,\, d)$ κώδικας $\mathcal{C}$ είναι μεγιστικός, αν και μόνο αν για κάθε λέξη $\mathbf{x} \in \mathbb{A}^n$ υπάρχει μια (κωδικο)λέξη $\mathbf{c} \in \mathcal{C}$, τέτοια ώστε $d(\mathbf{x},\, \mathbf{c}) < d$ (γιατί;).

Έστω $\mathcal{C}$ ένας μεγιστικός κώδικας, υποθέτουμε ότι εστάλη η (κωδικο)λέξη $\mathbf{c}$ και ελήφθη λέξη $\mathbf{x}$ στην οποία έχουν υπεισέλθει τουλάχιστον d το πλήθος λάθη (δηλαδή το διάνυσμα λάθους $\mathbf{x} - \mathbf{c}$ έχει βάρος τουλάχιστον d και επομένως $d(\mathbf{x},\, \mathbf{c}) \geq d$). Επειδή ο κώδικας είναι μεγιστικός, υπάρχει σίγουρα μια (κωδικο)λέξη, η οποία είναι πλησιέστερη στη $\mathbf{x}$ απότι η $\mathbf{c}$. Επομένως, αν κατά την αποκωδικοποίηση εφαρμόσουμε την Αρχή της πλησιέστερης λέξης, τότε οπωσδήποτε θα έχουμε λανθασμένη αποκωδικοποίηση.

Έστω ότι έχουμε έναν δυαδικό συμμετρικό δίαυλο επικοινωνίας, όπου η πιθανότητα μετάδοσης λάθους χαρακτήρα είναι ίση με p, δηλαδή:

$$\begin{aligned} &p(\textit{ελήφθη ο χαρακτήρας } 1 \mid \textit{εστάλη ο χαρακτήρας } 0) = \\ &\quad = p(\textit{ελήφθη ο χαρακτήρας } 0 \mid \textit{εστάλη ο χαρακτήρας } 1) = p. \end{aligned}$$

Η πιθανότητα να μεταδοθούν k το πλήθος λανθασμένοι χαρακτήρες είναι ίση με $\binom{n}{k}p^k(1-p)^{n-k}$. Επομένως, για την πιθανότητα λανθασμένης αποκωδικοποίησης μιας λέξης έχουμε:

$$p(\textit{λανθασμένης αποκωδικοποίησης}) \geq \sum_{k=d}^{n} \binom{n}{k} p^k (1-p)^{n-k} .$$

Από την άλλη πλευρά όμως, σε οποιονδήποτε κώδικα με ελάχιστη απόσταση ίση με d, το πλήθος των λαθών που μπορούν να διορθωθούν είναι ίσον με $\left[\frac{d-1}{2}\right]$. Συνεπώς, για την πιθανότητα σωστής αποκωδικοποίσης έχουμε:

$$p(\textit{σωστής αποκωδικοποίησης}) \geq \sum_{k=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{k} p^k (1-p)^{n-k} .$$

Δηλαδή:

$$\begin{aligned} p(\textit{λανθασμένης αποκωδικοποίησης}) &= 1 - p(\textit{σωστής αποκωδικοποίησης}) \\ &\leq 1 - \sum_{k=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{k} p^k (1-p)^{n-k}. \end{aligned}$$

Άρα τελικά:

$$\begin{aligned} \sum_{k=d}^{n} \binom{n}{k} p^k (1-p)^{n-k} &\leq p(\textit{λανθασμένης αποκωδικοποίησης}) \\ &\leq 1 - \sum_{k=0}^{\left[\frac{d-1}{2}\right]} \binom{n}{k} p^k (1-p)^{n-k} . \end{aligned}$$

Επομένως, έχουμε αποδείξει το επόμενο θεώρημα.

Θεώρημα 1.4.17. *Υποθέτουμε ότι έχουμε έναν δυαδικό μεγιστικό κώδικα και χρησιμοποιούμε έναν συμμετρικό δίαυλο επικοινωνίας. Τότε υπάρχει άνω και κάτω φράγμα για την πιθανότητα λανθασμένης αποκωδικοποίησης.*

Πρέπει να παρατηρήσουμε ότι το άνω φράγμα λανθασμένης αποκωδικοποίησης ισχύει για κάθε δυαδικό κώδικα (όχι κατ' ανάγκη μεγιστικό), ενώ το κάτω φράγμα λανθασμένης αποκωδικοποίησης δεν ισχύει για μη μεγιστικούς κώδικες.

Συνοψίζοντας, ένας μεγιστικός κώδικας υπερτερεί έναντι των κωδίκων που περιέχει ως (υπο)κώδικες (πλουσιώτερο λεξιλόγιο), αλλά υστερεί στο γεγονός ότι έχει αυξημένη πιθανότητα λανθασμένης αποκωδικοποίησης (λέξεις που περιέχουν τουλάχιστον d το πλήθος λάθη αποκωδικοποιούνται οπωσδήποτε λανθασμένα).

1.4.3 Ασκήσεις

1. Έστω $\mathcal{E}_n$ ο δυαδικός κώδικας που αποτελείται από όλες τις λέξεις μήκους n με άρτιο βάρος. Έστω $\mathcal{D}$ ο κώδικας $\mathbb{Z}_2^{n-1}$. Δείξτε ότι ο $\mathcal{E}_n$ προέρχεται από τον $\mathcal{D}$ με την επισύναψη ενός ψηφίου ελέγχου ισοτιμίας. Ποίες είναι οι παράμετροι του κώδικα $\mathcal{E}_n$;

2. Κατασκευάστε έναν δυαδικό κώδικα με παραμέτρους $(7, 6, 2)$ και κατόπιν εφαρμόζοντας μια σμίκρυνση και μια σύμπτυξη να προέλθει ένας $(6, 4, 3)$ κώδικας.

3. Έστω $\mathcal{C}$ ένας κώδικας με παραμέτρους (n, M, d). Δείξτε ότι μπορούμε να κατασκευάσουμε έναν άλλο κώδικα $\mathcal{D}$ με παραμέτρους $(n+1, M+2, 1)$, έτσι ώστε ο κώδικας $\mathcal{C}$ να προέρχεται από τον $\mathcal{D}$ εφαρμόζοντας διαδοχικά μια σμίκρυνση και μια σύμπτυξη.

4. Έστω $\mathcal{C}$ ένας δυαδικός κώδικας του οποίου όλα τα στοιχεία έχουν άρτιο βάρος. Δείξτε ότι η απόσταση δύο οποιωνδήποτε (κωδικο)λέξεων είναι άρτια. Τί συμπεραίνετε για την ελάχιστη απόσταση ένος κώδικα που προέρχεται από έναν δυαδικό κώδικα με την επισύναψη ένος ψηφίου ελέγχου ισοτιμίας;

5. Δείξτε ότι αν υπάρχει ένας δυαδικός (n, M, d) κώδικας με d άρτιο, τότε υπάρχει ένας δυαδικός (n, M, d) κώδικας, του οποίου όλες οι (κωδικο)λέξεις έχουν άρτιο βάρος.

6. Έστω $\mathcal{C}$ ένας δυαδικός κώδικας.

   i) Στον κώδικα $\mathcal{C}$ εφαρμόζουμε διαδοχικά δύο φορές την διαδικασία

της επισύναψης ενός ψηφίου ελέγχου ισοτιμίας. Τι κώδικας θα προκύψει; Έχει νόημα η δεύτερη επισύναψη ψηφίου ελέγχου ισοτιμίας;

ii) Στον κώδικα $\mathcal{C}$ επισυνάπτουμε ένα ψηφίο ελέγχου ισοτιμίας και κατόπιν, στο τέλος κάθε λέξης έναν χαρακτήρα, έτσι ώστε το βάρος κάθε λέξης που προκύπτει να είναι περιττό. Να συγκρίνετε την ελάχιστη απόσταση του αρχικού κώδικα $\mathcal{C}$ με την ελάχιστη απόσταση του κώδικα $\mathcal{D}$ που προκύπτει από την παραπάνω διαδικασία.

Αν στον αρχικό κώδικα $\mathcal{C}$ εφαρμόσουμε αντίστροφη διαδικασία, δηλαδή πρώτα στο τέλος κάθε στοιχείου επισυνάψουμε έναν χαρακτήρα, έτσι ώστε το βάρος κάθε λέξης που προκύπτει να είναι περιττό και κατόπιν επισυνάψουμε ένα ψηφίο ελέγχου ισοτιμίας, ο κώδικας $\mathcal{E}$ που προκύπτει τι σχέση έχει με τους προηγούμενους κώδικες $\mathcal{C}$ και $\mathcal{D}$;

7. Πόσοι μη ισοδύναμοι δυαδικοί κώδικες μήκους n με δύο μόνο στοιχεία υπάρχουν;

8. Εφαρμόζοντας την $(\mathbf{u},\ \mathbf{u}+\mathbf{v})$- κατασκευή να κατασκευάσετε τον κώδικα $\mathcal{C}_1 \odot \mathcal{C}_2$ στις ακόλουθες περιπτώσεις:

   i) $\mathcal{C}_1 = \{000, 001, 111\}$, $\mathcal{C}_2 = \{100, 011, 001\}$

   ii) Ο $\mathcal{C}_1$ είναι ο δυαδικός $(4,\ 8,\ 2)$ κώδικας που αποτελείται από τις οκτώ (κωδικο)λέξεις μήκους 4 και είναι αρτίου βάρους και ο $\mathcal{C}_2$ είναι ο επαναληπτικός κώδικας $\mathcal{R}_2(4)$.

   Στις παραπάνω περιπτώσεις να υπολογίσετε τις παραμέτρους του κώδικα $\mathcal{C}_1 \odot \mathcal{C}_2$.

9. Έστω $\mathcal{C}$ και $\mathcal{D}$ δύο κώδικες επί ενός πεπερασμένου σώματος $\mathbb{F}$, οι οποίοι είναι μεταθετικά ισοδύναμοι, δηλαδή υπάρχει μια μετάθεση σ, έτσι ώστε $\mathcal{D} = \mathcal{C}_\sigma$. Αν $\overline{\mathcal{C}}$ και $\overline{\mathcal{D}}$ είναι οι κώδικες που προκύπτουν επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας, δείξτε ότι $\overline{\mathcal{C}}$ και $\overline{\mathcal{D}}$ είναι, επίσης, μεταθετικά ισοδύναμοι.

10. Έστω $\mathcal{C}$ ο δυαδικός κώδικας $\{00000, 110000, 00111, 11111\}$. Συμπτύσσουμε τον κώδικα μια φορά ως προς την πρώτη συντεταγμένη και μια φορά ως προς την τελευταία συντεταγμένη και λαμβάνουμε τους αντίστοιχους συνεπτυγμένους κώδικες $\mathcal{C}_1 = \{0000, 10000, 0111, 1111\}$ και $\mathcal{C}_2 = \{0000, 11000, 0011, 1111\}$.

    Γιατί οι δύο συνεπτυγμένοι κώδικες δεν είναι μεταθετικά ισοδύναμοι;

11. Έστω $\mathcal{C}$ ένας κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ και $\overline{\mathcal{C}}$ ο κώδικας που προκύπτει από τον $\mathcal{C}$ επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας. Τι σχέση έχουν οι ελάχιστες αποστάσεις των κωδίκων $\mathcal{C}$ και $\overline{\mathcal{C}}$;

    Να δώσετε ένα παράδειγμα, όπου οι δύο κώδικες έχουν την ίδια ελάχιστη απόσταση και ένα παράδειγμα, όπου οι δύο κώδικες έχουν διαφορτικές ελάχιστες αποστάσεις.

12. Έστω $\mathcal{C}$ ένας κώδικας, ο οποίος δεν είναι μεγιστικός. Πώς μπορούμε να επισυνάψουμε στοιχεία στον $\mathcal{C}$ έως ότου να επιτύχουμε έναν μεγιστικό κώδικα;

1.5 Τέλειοι κώδικες

Στην Αρχή ορίζοντας την απόσταση Hamming είχαμε παρατηρήσει (Παρατήρηση 1.2.4) ότι μπορούμε να κάνουμε *Γεωμετρία* στο σύνολο $\mathbb{A}^n$, όπου $\mathbb{A}$ είναι ένα αλφάβητο (συνήθως το $\mathbb{Z}_p$ ή γενικότερα ένα πεπερασμένο σώμα). Εδώ θα δούμε μια *Γεωμετρική* θεώρηση των κωδίκων ως προς την ικανότητά τους να διορθώνουν λάθη.

Αυτό θα μας οδηγήσει σε μια σημαντική κατηγορία κωδίκων, τους τέλειους κώδικες.

1.5.1 Σφαίρες ομαδοποίησης και τέλειοι κώδικες

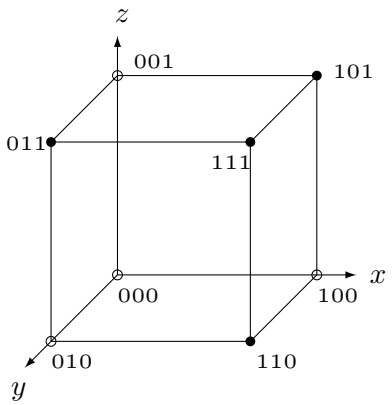
Ορισμός 1.5.1. *Έστω $\mathbb{A}$ ένα αλφάβητο με q το πλήθος στοιχεία και n ένας φυσικός ακέραιος. Για κάθε $\mathbf{x} \in \mathbb{A}^n$ και κάθε πραγματικό μη αρνητικό*

αριθμό r ορίζουμε την ***σφαίρα*** *(διάστασης n με κέντρο το στοιχείο $\mathbf{x}$ και ακτίνα ίση με r) ως το σύνολο:* $S_q^n(\mathbf{x}, r) = \{\mathbf{y} \in \mathbb{A}^n \mid d(\mathbf{x}, \mathbf{y}) \leq r\}$.[15]

Παραδείγματα 1.5.2. 1. Η σφαίρα $S_2^3(101, 2)$ στο $\mathbb{Z}_2^3$ αποτελείται από όλες τις δυαδικές λέξεις μήκους 3 οι οποίες απέχουν απόσταση τουλάχιστον 2 από την 101, και προφανώς:

$$S_2^3(101, 2) = \{101, 001, 111, 100, 011, 000, 110\}.$$

2. Στο σχήμα 1.3 παρίσταται γεωμετρικά η σφαίρα $S_2^3(111, 1)$ στο $\mathbb{Z}_2^3$, όπου τα στοιχεία που ανήκουν σ' αυτή είναι οι κορυφές του κύβου με την έντονη στίξη.



Σχήμα 1.3: Η σφαίρα $S_2^3(111, 1)$ στο $\mathbb{Z}_2^3$.

Δυστυχώς είναι δύσκολο να κάνουμε σχεδιαστική αναπαράσταση μιας σφαίρας στην περίπτωση όπου η διάσταση είναι $n \geq 4$.

Άμεσα συνδεδεμένη με την έννοια της σφαίρας είναι η έννοια του **όγκου** της. Ο όγκος μιας σφαίρας $S_q^n(\mathbf{x}, r)$ είναι ο αριθμός των λέξεων οι οποίες περιέχονται μέσα στη σφαίρα. Προφανώς (γιατί;), ο όγκος μιας σφαίρας δεν εξαρτάται από την επιλογή του κέντρου της $\mathbf{x}$, για τον λόγο αυτό συνήθως συμβολίζεται $V_q(n, r)$.

[15] Όταν δεν υπάρχει κίνδυνος σύγχυσης ως προς το q και το n, αντί για $S_q^n(\mathbf{x}, r)$, θα γράφουμε $S(\mathbf{x}, r)$.

Μπορούμε να υπολογίσουμε εύκολα τον όγκο μιας σφαίρας. Θεωρούμε μια λέξη $\mathbf{x} \in \mathbb{A}^n$. Για $0 \leq k \leq n$ ο αριθμός των λέξεων, οι οποίες διαφέρουν σε k θέσεις από την $\mathbf{x}$ (έχουν απόσταση ίση με k από την $\mathbf{x}$), είναι προφανώς ίσος με $\binom{n}{k}(q-1)^k$. Επομένως, αθροίζοντας από 0 έως r έχουμε για τον όγκο της σφαίρας

$$V_q(n, r) = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k .$$

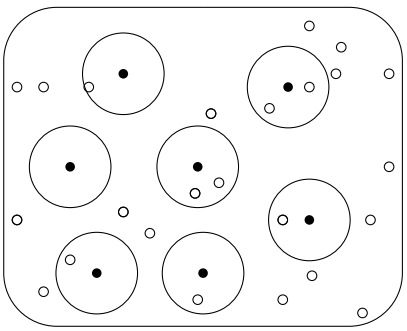
(Ο αριθμός r είναι πραγματικός, αλλά στο προηγούμενο άθροισμα, όπου ο k είναι ακέραιος δεν υπάρχει σύγχυση, καθότι το k λαμβάνει τιμές από 0 έως $[r]$.)

Αξίζει να σημειωθεί ότι στην περίπτωση όπου το αλφάβητο $\mathbb{A}$ είναι το $\mathbb{Z}_2$, τότε ο όγκος μιας σφαίρας ακτίνας r είναι το άθροισμα των r πρώτων διωνυμικών συντελεστών, δηλαδή

$$V_2(n, r) = \sum_{k=0}^{r} \binom{n}{k} .$$

Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας (n, M, d) κώδικας. Σκοπός μας είναι με κέντρο κάθε (κωδικο)λέξη να κατασκευάσουμε σφαίρες με όσο το δυνατόν μεγαλύτερη κοινή ακτίνα, αλλά να μην τέμνονται μεταξύ τους.

Στο σχήμα 1.4 οι • αναπαριστούν τις (κωδικο)λέξεις, ενώ οι ◦ αναπαριστούν τα υπόλοιπα στοιχεία του $\mathbb{A}^n$.



Σχήμα 1.4: Ξένες μεταξύ τους σφαίρες του $\mathbb{A}^n$ με κοινή ακτίνα.

Υποθέτουμε ότι η ελάχιστη απόσταση του κώδικα είναι άρτια ίση με $d = 2\lambda + 2$ και $\mathbf{c}$, $\mathbf{d}$ είναι δύο (κωδικο)λέξεις που απέχουν μεταξύ τους απόσταση

ίση με την ελάχιστη απόσταση του κώδικα. Τότε υπάρχει μια (τουλάχιστον) λέξη $\mathbf{x} \in \mathbb{A}^n$ η οποία ισαπέχει από τις $\mathbf{c}$ και $\mathbf{d}$ (γιατί;). Αν πάρουμε σφαίρες με κέντρα τις $\mathbf{c}$ και $\mathbf{d}$ και ακτίνα ίση με $\lambda+1$, τότε οι δύο σφαίρες *εφάπτονται* στη λέξη $\mathbf{x}$. Αν όμως οι σφαίρες έχουν ακτίνα ίση με λ, τότε αυτές είναι ξένες μεταξύ τους.

Υποθέτουμε τώρα ότι η ελάχιστη απόσταση του κώδικα είναι περιττή ίση με $d = 2\lambda + 1$ και $\mathbf{c}$, $\mathbf{d}$ είναι δύο (κωδικο)λέξεις που απέχουν μεταξύ τους απόσταση ίση με την ελάχιστη απόσταση του κώδικα. Τότε δεν υπάρχει λέξη $\mathbf{x} \in \mathbb{A}^n$ η οποία να ισαπέχει από τις $\mathbf{c}$ και $\mathbf{d}$ απόσταση ίση με λ (γιατί;). Αν πάρουμε σφαίρες με κέντρα τις $\mathbf{c}$ και $\mathbf{d}$ και ακτίνα ίση με $\lambda + 1$, τότε οι δύο σφαίρες *τέμνονται* σε μια (τουλάχιστον) λέξη (γιατί;). Αν όμως οι σφαίρες έχουν ακτίνα ίση με λ, τότε αυτές είναι ξένες μεταξύ τους.

Η προηγούμενη συζήτηση θα μπορούσε να αναπαρασταθεί στο σχήμα 1.5.

$d = 2\lambda + 2$ $\qquad$ $d = 2\lambda + 1$

Σχήμα 1.5: Απόσταση και τομή σφαιρών.

Όπως βλέπουμε, και στις δύο περιπτώσεις, σφαίρες με κέντρα (κωδικο)λέξεις και ακτίνα ίση με $\lambda = \left[\frac{d-1}{2}\right]$ είναι ξένες μεταξύ τους και η ακτίνα αυτή είναι η μεγαλύτερη δυνατή με την ιδιότητα αυτή.

Ορισμός 1.5.3. *Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας (n, M, d) κώδικας. Ο μεγαλύτερος ακέραιος αριθμός r για τον οποίο οι σφαίρες $S_q^n(\mathbf{c}, r)$ με κέντρο οποιαδήποτε (κωδικο)λέξη $\mathbf{c}$ είναι ξένες μεταξύ τους, λέγεται* ***ακτίνα ομαδοποίησης*** *και συμβολίζεται με $pr(\mathcal{C})$. Οι δε αντίστοιχες σφαίρες $S_q^n(\mathbf{c}, r)$ ονομάζονται σφαίρες* ***ομαδοποίησης****.*

Πρόταση 1.5.4. *Σε έναν (n, M, d) κώδικα $\mathcal{C} \subseteq \mathbb{A}^n$ η ακτίνα ομαδοποίησης είναι ίση με $pr(\mathcal{C}) = \left[\frac{d-1}{2}\right]$.*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Θεώρημα 1.5.5. *Ένας κώδικας $\mathcal{C}$ διορθώνει λ το πλήθος λάθη, αν και μόνο αν για κάθε (κωδικο)λέξη $\mathbf{c}$ οι σφαίρες $S_q^n(\mathbf{c}, \lambda)$ είναι ξένες.*

Απόδειξη. Υποθέτουμε ότι ο κώδικας διορθώνει λ το πλήθος λάθη και επιπλέον, ότι υπάρχουν δύο (κωδικο)λέξεις $\mathbf{c}$ και $\mathbf{d}$ για τις οποίες υπάρχει λέξη $\mathbf{x} \in S_q^n(\mathbf{c}, \lambda) \cap S_q^n(\mathbf{d}, \lambda)$. Επομένως, έχουμε ότι $d(\mathbf{c}, \mathbf{d}) \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{d}) \leq \lambda + \lambda = 2\lambda$. Αλλά από το Θεώρημα 1.3.16 έχουμε ότι $d(\mathcal{C}) \geq 2\lambda + 1$, άτοπο.

Το αντίστροφο είναι προφανές. ό.έ.δ.

Πόρισμα 1.5.6. *Ένας κώδικας διορθώνει ακριβώς λ το πλήθος λάθη, αν και μόνο αν η ακτίνα ομαδοποίησης είναι ίση με λ.*

Παρατηρήσεις 1.5.7.

1. Από τα προηγούμενα βλέπουμε *γεωμετρικά* ότι για κάθε κωδικολέξη η αντίστοιχη σφαίρα ομαδοποίησης έχει *αιχμαλωτίσει* όλες τις λέξεις, οι οποίες σύμφωνα με την Αρχή της αποκωδικοποίησης ως προς την πλησιέστερη λέξη *έλκονται* από το κέντρο της σφαίρας και *ταυτίζονται* μ' αυτό.

2. Λαμβάνοντας την (διακεκριμένη) ένωση των σφαιρών ομαδοποίησης για κάθε (κωδικο)λέξη έχουμε $\bigcup_{i=1}^{M} S_q^n(\mathbf{c}_i, \lambda) \subseteq \mathbb{A}^n$.

Θεώρημα 1.5.8. Το φράγμα ομαδοποίησης σφαιρών ή φράγμα Hamming
Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας επί του αλφάβητου $\mathbb{A}$ με $|\,\mathbb{A}\,| = q$. Τότε ισχύει $M \leq q^n/V$, όπου $V = V_q(n, r) = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k$ και $r = pr(\mathcal{C}) = \left[\frac{d-1}{2}\right]$ είναι η ακτίνα ομαδοποίησης.

Απόδειξη. Η απόδειξη απορρέει από τα προηγούμενα, εδώ απλώς την επαναλαμβάνουμε.

Αν για κάθε (κωδικο)λέξη πάρουμε την αντίστοιχη σφαίρα ομαδοποίησης, έχουμε M το πλήθος ξένες σφαίρες όλες με την ίδια ακτίνα ομαδοποίησης $r = pr(\mathcal{C}) = \left[\frac{d-1}{2}\right]$. Το πλήθος των λέξεων που περιέχονται σε κάθε σφαίρα δεν εξαρτάται από το κέντρο της, αλλά μόνο από την (κοινή) ακτίνα και για όλες είναι ίσο με τον όγκο μιας απ' αυτές, ο οποίος έχουμε δείξει ότι είναι ίσος με $V = V_q(n, r) = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k$. Επομένως, το πλήθος των λέξεων που περιέχεται σε όλες τις σφαίρες ομαδοποίησης είναι ίσο με $M \cdot V$, που φυσικά

δεν υπερβαίνει το συνολικό πλήθος των λέξεων μήκους n με χαρακτήρες από το αλφάβητο $\mathbb{A}$ με τα q το πλήθος στοιχεία. ό.έ.δ.

Ορισμός 1.5.9. *Έστω $\mathcal{C} \subseteq \mathbb{A}^n$ ένας (n, M, d) κώδικας. Ο μικρότερος ακέραιος αριθμός r για τον οποίο οι σφαίρες $S_q^n(\mathbf{c}, r)$ με κέντρα τις (κωδικο)λέξεις $\mathbf{c} \in \mathcal{C}$ **καλύπτουν** το σύνολο $\mathbb{A}^n$ λέγεται **ακτίνα κάλυψης** και συμβολίζεται με $cr(\mathcal{C})$. Οι δε αντίστοιχες σφαίρες $S_q^n(\mathbf{c}, r)$ ονομάζονται σφαίρες **κάλυψης**.*

Προφανώς, οι σφαίρες κάλυψης δεν είναι κατ' ανάγκη ξένες μεταξύ τους. Από την άλλη πλευρά έχουμε δει ότι οι σφαίρες ομαδοποίησης είναι μεν ξένες μεταξύ τους, αλλά δεν καλύπτουν κατ' ανάγκην ολόκληρο το $\mathbb{A}^n$. Επομένως, γεννάται το ερώτημα:
Υπάρχει περίπτωση να μπορούμε να καλύψουμε το $\mathbb{A}^n$ με ξένες σφαίρες; Με άλλα λόγια, υπάρχει περίπτωση οι σφαίρες κάλυψης να συμπίπτουν με τις σφαίρες ομαδοποίησης;

Ορισμός 1.5.10. *Ένας (n, M, d) κώδικας $\mathcal{C} \subseteq \mathbb{A}^n$ ονομάζεται **τέλειος**, αν η ακτίνα ομαδοποίησης είναι ίση με την ακτίνα κάλυψης ($pr(\mathcal{C}) = cr(\mathcal{C})$).*

Παράδειγμα 1.5.11. Ο επαναληπτικός δυαδικός κώδικας $\mathcal{C} = \{\,000, 111\,\}$ είναι προφανώς τέλειος.

Μια άμεση συνέπεια του ορισμού είναι η εξής πρόταση, η οποία αποτελεί έναν ισοδύναμο ορισμό για τους τέλειους κώδικες.

Πρόταση 1.5.12. *Ένας (n, M, d) κώδικας $\mathcal{C} \subseteq \mathbb{A}^n$ με $|\,\mathbb{A}\,| = q$ είναι τέλειος, αν και μόνο αν η ελάχιστη απόσταση είναι περιττή $d = 2r + 1$ και ισχύει*

$$M = \frac{q^n}{\sum_{k=0}^{r} \binom{n}{k}(q-1)^k}. \tag{1.2}$$

Απόδειξη. Το ότι ένας τέλειος κώδικας αναγκαστικά έχει περιττή ελάχιστη απόσταση έπεται από τον ορισμό και την συζήτηση που προηγήθηκε του Ορισμού 1.5.3. Τα υπόλοιπα έπονται άμεσα από τον ορισμό και το Θεώρημα 1.5.8. ό.έ.δ.

Όπως βλέπουμε από τον ορισμό, ένας τέλειος κώδικας με παραμέτρους (n, M, d) έχει την ιδιότητα να αποκωδικοποιεί κάθε λέξη $\mathbf{x} \in \mathbb{A}^n$. Μάλιστα δε αν έχουν υπεισέλθει μέχρι $\left[\frac{d-1}{2}\right]$ το πλήθος λάθη, τότε, σύμφωνα με την Αρχή αποκωδικοποίησης ως προς τη πλησιέστερη λέξη, η αποκωδικοποίηση είναι σωστή.

Το πρόβλημα της ανακάλυψης όλων των τέλειων κωδίκων παραμένει ανοικτό. Η σημαντικότερη πρόοδος έχει γίνει στην περίπτωση όπου το μέγεθος του κώδικα ισούται με τη δύναμη ενός πρώτου αριθμού. Επ' αυτού θα επανέλθουμε αργότερα.

Προς το παρόν θα περιορισθούμε σε μια απλή προσέγγιση του προβλήματος αναζητώντας θετικούς ακεραίους q, n, M και $d = 2r+1$ που ικανοποιούν τη σχέση 1.2. Πριν προχωρήσουμε πρέπει να τονίσουμε ότι η υπάρξη τέτοιων αριθμών **δεν** συνεπάγεται την ύπαρξη κωδίκων με αυτές τις παραμέτρους, όπως θα δούμε αργότερα.

Είναι εύκολο (και αφίεται ως άσκηση) να επαληθεύσουμε ότι κώδικες (αν υπάρχουν) με τις παρακάτω οικογένειες παραμέτρων είναι τέλειοι.

1. $(n, M, d) = (n, q^n, 1)$
2. $(n, M, d) = (n, 1, ?)$
3. $(n, M, d) = (2r+1, 2, 2r+1)$
4. $(n, M, d) = (\frac{q^r-1}{q-1}, q^{n-r}, 3),\ r \geq 2$
5. $(n, M, d) = (23, 2^{11}, 7)$
6. $(n, M, d) = (11, 3^6, 5)$
7. $(n, M, d) = (90, 2^{78}, 5)$

Οι κώδικες που ανήκουν στην πρώτη και δεύτερη οικογένεια αποτελούν ακραίες περιπτώσεις, όπου στην μεν πρώτη περίπτωση ο κώδικας αποτελείται από όλες τις λέξεις μήκους n και δεν διορθώνει κανένα λάθος, στην δε δεύτερη περίπτωση ο κώδικας αποτελείται από μία μόνο λέξη (μάλιστα δε, δεν ορίζεται καν η ελάχιστη απόσταση). Στην τρίτη περίπτωση ανήκουν

οι δυαδικοί επαναληπτικοί κώδικες περιττού μήκους οι οποίοι αποτελούνται από δύο μόνο λέξεις. Η τέταρτη οικογένεια περιλαμβάνει μια σημαντική κατηγορία κωδίκων, γνωστούς ως κώδικες Hamming, στους οποίους θα αναφερθούμε διεξοδικότερα στην Παράγραφο 4.1. Οι περιπτώσεις πέντε και έξι αντιστοιχούν στους περίφημους κώδικες Golay, στους οποίους, επίσης, θα αναφερθούμε αργότερα στην Παράγραφο 4.2. Τέλος, έχει αποδειχθεί (βλέπε Θεώρημα 4.3.1 και Πρόταση 4.3.2) ότι δεν υπάρχουν κώδικες με παραμέτρους που να αντιστοιχούν στην τελευταία περίπτωση.

Οι κώδικες που ανήκουν στις τρεις πρώτες οικογένειες αναφέρονται ως **τετριμμένοι** τέλειοι κώδικες. Όπως θα δούμε στην Παράγραφο 4.3 (αλλά δεν θα αποδείξουμε) οι μέχρι σήμερα γνωστοί τέλειοι κώδικες, στην ουσία[16] ανήκουν σε μια από τις παραπάνω οικογένειες.

1.5.2 Φράγματα κωδίκων

Προηγουμένως ασχοληθήκαμε με τους μεγιστικούς κώδικες και είδαμε σε τι υπερέχουν και σε τι υστερούν. Εδώ ενδιαφερόμαστε για κώδικες οι οποίοι περιέχουν όσο το δυνατόν περισότερες (κωδικο)λέξεις, με δεδομένη την ελάχιστη απόσταση d και το μήκος n.

Ορισμός 1.5.13. *Έστω $\mathbb{A}$ ένα αλφάβητο με q το πλήθος στοιχεία, n και d φυσικοί αριθμοί και $A_q(n,d) = \max\{\, M \mid$ υπάρχει (n, M, d) κώδικας $\}$. Ένας κώδικας $\mathcal{C}$ με μέγεθος ίσο με $A_q(n,d)$ θα λέγεται **βέλτιστος**.*

Προφανώς, ένας βέλτιστος κώδικας είναι μεγιστικός, το αντίστροφο προφανώς (γιατί;) δεν ισχύει.

Ο προσδιορισμός των αριθμών $A_q(n,d)$ για τις διάφορες τιμές των παραμέτρων q, n και d έχει αναχθεί σε κεντρικό πρόβλημα στην Θεωρία Κωδίκων. Για μικρές τιμές των ανωτέρω παραμέτρων έχουν προσδιορισθεί (επακριβώς) οι αντίστοιχες τιμές $A_q(n,d)$, ο πίνακας 1.2 περιλαμβάνει μερικές τιμές για δυαδικούς κώδικες.

[16] Επισημαίνουμε ότι αν βρούμε έναν κώδικα με κάποιες παραμέτρους, αυτό δεν σημαίνει ότι δεν υπάρχουν και άλλοι κώδικες με τις ίδιες παραμέτρους (βλέπε για παράδειγμα τους ισοδύναμους κώδικες)

n	$d = 3$	$d = 5$	$d = 7$
5	4	2	–
6	8	2	–
7	16	2	2
8	20	4	2
9	40	6	2
10	$72 - 79$	12	2
11	$144 - 158$	24	4
12	256	32	4
13	512	64	8
14	1024	128	16
15	2048	256	32
16	$2560 - 3276$	$256 - 340$	$36 - 37$

Πίνακας 1.2: Μερικές τιμές του $A_2(n, d)$.

Γενικά όμως οι προσπάθειες έχουν επικεντρωθεί στην εύρεση καλών (άνω και κάτω) φραγμάτων. Επίσης, έχει μελετηθεί η ασυμπτωτική συμπεριφορά των τιμών $A_q(n, d)$ ως προς τον λόγο $\delta = \frac{d}{n}$, καθώς το $n \longrightarrow \infty$.

Προφανώς, στις ακραίες (και προφανείς) περιπτώσεις έχουμε:

$$A_q(n, d) \leq q^n,$$
$$A_q(n, 1) = q^n,$$
$$A_q(n, n) = q.$$

Θεώρημα 1.5.14. *Για δυαδικούς κώδικες ισχύει:*

$$A_2(n, 2\lambda + 1) = A_2(n + 1, 2\lambda + 2).$$

Απόδειξη. Η απόδειξη έπεται άμεσα από το Θεώρημα 1.4.10. ό.έ.δ.

Παρατήρηση 1.5.15. Όπως θα έχετε παρατηρήσει ο προηγούμενος πίνακας αναφέρεται σε βέλτιστους κώδικες με περιττή ελάχιστη απόσταση. Από το

προηγούμενο θεώρημα βλέπουμε ότι είναι αρκετό να υπολογίσουμε τις τιμές $A_2(n, d)$ μόνο για περιττές (ή μόνο για άρτιες) τιμές του d.

Θεώρημα 1.5.16. $A_q(n, d) \leq q \cdot A_q(n-1, d)$.

Απόδειξη. Έστω $\mathcal{C}$ ένας βέλτιστος (n, M, d) κώδικας (δηλαδή $M = A_q(n, d)$). Διαμερίζουμε το σύνολο των (κωδικο)λέξεων σε υποκώδικες, έτσι ώστε κάθε υποκώδικας να περιέχει σε μια συγκεκριμένη συντεταγμένη (π.χ. στην τελευταία) τον ίδιο χαρακτήρα. Επομένως, έχουμε το πολύ q το πλήθος τέτοιους υποκώδικες. Τουλάχιστον ένας απ' αυτούς τους υποκώδικες περιέχει τουλάχιστον M/q το πλήθος στοιχεία (γιατί;). Από έναν τέτοιο υποκώδικα διαγράφουμε τον κοινό χαρακτήρα από τη συγκεκριμένη θέση, οπότε προκύπτει ένας κώδικας μήκους $n-1$ και με ελάχιστη απόσταση τουλάχιστον ίση με d. Τελικά, βλέπουμε ότι βέλτιστοι κώδικες μήκους $n-1$ περιέχουν τουλάχιστον M/q το πλήθος στοιχεία και το αποτέλεσμα έπεται. ό.έ.δ.

Η διαδικασία που ακολουθήσαμε στο προηγούμενο θεώρημα αποτελεί συμπύκνωση του αρχικού κώδικα, βλέπε παρατηρήσεις 1.4.11, σελ. 47.

Θεώρημα 1.5.17. ***(Φράγμα επικάλυψης σφαιρών ή κάτω φράγμα Gilbert-Varshamov).***

Για το μέγεθος ενός βέλτιστου κώδικα ισχύει $A_q(n, d) \geq q^n / V_q(n, d-1)$.

Απόδειξη. Έστω $\mathcal{C}$ ένας (n, M, d) βέλτιστος κώδικας επί του αλφάβητου $\mathbb{A}$ με $|\,\mathbb{A}\,| = q$ και $\mathbf{y} \in \mathbb{A}^n \setminus \mathcal{C}$. Τότε υπάρχει (κωδικο)λέξη $\mathbf{a} \in \mathcal{C}$, έτσι ώστε η $\mathbf{y}$ να ανήκει στη σφαίρα $S_q^n(\mathbf{a}, d-1)$. Πράγματι, αν η $\mathbf{y}$ δεν ανήκε σε καμία σφαίρα με κέντρο μια (κωδικο)λέξη και ακτίνα ίση με $d-1$, τότε θα είχαμε $d(\mathbf{x}, \mathbf{y}) \geq d$ για κάθε $\mathbf{x} \in \mathcal{C}$. Επομένως, ο κώδικας $\mathcal{C} \cup \{\, y \,\}$ θα είχε ελάχιστη απόσταση ίση με d και μέγεθος $M+1$, άτοπο, διότι ο $\mathcal{C}$ είναι βέλτιστος. Επομένως, έχουμε αποδείξει ότι οι σφαίρες με κέντρα τα στοιχεία του $\mathcal{C}$ και ακτίνα ίση με $d-1$ καλύπτουν το $\mathbb{A}^n$. Άρα $|\,\mathbb{A}\,|^n = q^n \leq M \cdot V_q(n, d-1)$. Οπότε έπεται το αποτέλεσμα. ό.έ.δ.

Επειδή

$$V_q(n, d-1) = \sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k$$

τη σχέση στο προηγούμενο Θεώρημα την συναντάμε και ως:

$$A_q(n, d) \geq q^n / \sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k .$$

Πόρισμα 1.5.18. *Ένας βέλτιστος κώδικας με μέγεθος $A_q(n, d)$ έχει ακτίνα κάλυψης το πολύ ίση με $d-1$.*

Απόδειξη. Προφανώς, από την προηγούμενη ανισότητα, έχουμε ότι οι $A_q(n, d)$ το πλήθος σφαίρες η καθεμία όγκου $V_q(n, d-1)$ καλύπτουν όλο τον χώρο $\mathbb{A}^n$. ό.έ.δ.

Συνδυάζοντας το Θεώρημα 1.5.8 με το προηγούμενο θεώρημα έχουμε:

Θεώρημα 1.5.19. $q^n / V_q(n, d-1) \leq A_q(n, d) \leq q^n / V_q(n, [\frac{d-1}{2}])$.

Πόρισμα 1.5.20. *Ένας τέλειος κώδικας είναι βέλτιστος.*

Απόδειξη. Η απόδειξη είναι άμεση, δεδομένου ότι η δεύτερη ανισότητα στο προηγούμενο θεώρημα είναι ισότητα στην περίπτωση ενός τέλειου κώδικα. ό.έ.δ.

Τα παραπάνω (άνω και κάτω) φράγματα για το μέγεθος βέλτιστων κωδίκων δεν είναι τα καλύτερα δυνατά.

Όπως θα δούμε στην περίπτωση των Γραμμικών Κωδίκων (βλέπε Πρόταση 2.2.28) μπορούμε να βελτιώσουμε το παραπάνω κάτω φράγμα.

Εδώ θα περιορισθούμε αναφέροντας μόνο δύο άλλα άνω φράγματα.

Θεώρημα 1.5.21. ***(Φράγμα Singleton)***
Για βέλτιστους κώδικες επί ενός αλφάβητου $\mathbb{A}$ με $|\mathbb{A}| = q$ ισχύει $A_q(n, d) \leq q^{n-d+1}$.

Απόδειξη. Έστω $\mathcal{C}$ ένας (n, M, d) κώδικας. Συμπτύσσουμε τον κώδικα διαγράφοντας τις τελευταίες $d-1$ συντεταγμένες από όλες τις (κωδικο)λέξεις (ή γενικότερα τις ίδιες $d-1$ συντεταγμένες από κάθε (κωδικο)λέξη). Οι M το πλήθος λέξεις που προκύπτουν είναι διαφορετικές μεταξύ τους. Πράγματι, αν δύο από αυτές συνέπιπταν, τότε οι αρχικές λέξεις από τις οποίες προέρχονται θα διέφεραν στα διαγραφέντα τμήματα μήκους $d-1$, δηλαδή η μεταξύ

τους απόσταση θα ήταν το πολύ ίση με $d-1$, άτοπο (γιατί;). Δηλαδή έχουμε κατασκευάσει έναν κώδικα μεγέθους M και μήκους $n-d+1$. Επομένως, $M \leq q^{n-d+1}$. ό.έ.δ.

Παρατηρήσεις 1.5.22. 1. Αν συγκρίνουμε το φράγμα Hamming και το φράγμα Singleton βλέπουμε ότι στην μεν πρώτη περίπτωση έχουμε $A_q(4,3) \leq \frac{q^4}{4q-3}$, ενώ στη δεύτερη έχουμε $A_q(n,d) \leq q^{n-d+1}$. Οπότε για $q \geq 4$ το φράγμα Singleton είναι πολύ καλύτερο.

2. Υπάρχουν περιπτώσεις, όπου το φράγμα Singleton είναι το καλύτερο δυνατόν. Πράγματι, ο κώδικας:

$$\mathcal{C} = \{\, aaa,\, abc,\, acd,\, adb,\, bca,\, cda, dba,\, cab,\, dac,\, bad,\, bdc,\, cbd,\, dcb,\, bbb,\, ccc,\, ddd \,\}$$

είναι ένας $(3,\, 16,\, 2)$ κώδικας επί του αλφάβητου $\mathbb{A} = \{\, a,\, b,\, c,\, d \,\}$, επομένως για έναν βέλτιστο κώδικα με τις ίδιες παραμέτρους πρέπει να έχουμε $A_4(3,2) \geq 16$. Αλλά σύμφωνα με το φράγμα Singleton πρέπει να έχουμε $A_4(3,2) \leq 4^{3-2+1} = 16$. Δηλαδή τελικά έχουμε ισότητα.

3. Αργότερα, όταν μελετήσουμε τους BCH κώδικες, θα δούμε κατηγορίες κωδίκων που ικανοποιούν το φράγμα Singleton.

Θεώρημα 1.5.23. *Έστω $\mathcal{C}$ ένας $(n,\, M,\, d)$ κώδικας επί του αλφάβητου $\mathbb{A} = \{\, a_0, a_1, \ldots, a_{q-1} \,\}$. Υποθέτουμε ότι $d > \vartheta \cdot n$, όπου $\vartheta = \frac{q-1}{q}$. Για το μέγεθος M του κώδικα ισχύει $M \leq \frac{d}{d-\vartheta \cdot n}$.*

Απόδειξη. Έστω $S = \sum d(\mathbf{x}, \mathbf{y})$, όπου το άθροισμα εκτείνεται σε όλα τα διατεταγμένα ζεύγη $(\mathbf{x}, \mathbf{y})$ (διαφορετικών μεταξύ τους) (κωδικο)λέξεων. Το πλήθος αυτών των ζευγών ως γνωστόν είναι ίσο με $2\binom{M}{2} = M(M-1)$ και επειδή η απόσταση μεταξύ δύο (διαφορετικών) (κωδικο)λέξεων είναι τουλάχιστον ίση με d, έχουμε ότι $S \geq M(M-1)d$.

Θα υπολογίσουμε τώρα ένα άνω φράγμα για το άθροισμα S. Σχηματί-

ζουμε έναν $M \times n$ πίνακα του οποίου οι γραμμές είναι τα στοιχεία του $\mathcal{C}$:

$$\begin{array}{ccccccc} \mathbf{c}_1 & = & c_{11} & c_{12} & \cdots & c_{1n} \\ \mathbf{c}_2 & = & c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ \mathbf{c}_M & = & c_{M1} & c_{M2} & \cdots & c_{Mn} \end{array} .$$

Επιλέγουμε μία (τυχαία) στήλη του πίνακα και έναν τυχαίο χαρακτήρα $a \in \mathbb{A}$. Έστω m_a το πλήθος των εμφανίσεων του χαρακτήρα a σ' αυτή τη στήλη. Τότε, προφανώς, $\sum_{a\in\mathbb{A}} m_a = M$. Επίσης σε $M - m_a$ το πλήθος από τις (κωδικο)λέξεις σ' αυτή τη στήλη εμφανίζεται ένας άλλος χαρακτήρας διαφορετικός από τον a. Επομένως, η *συμβολή* αυτής της στήλης στο άθροισμα των αποστάσεων όλων των διατεταγμένων ζευγών (διαφορετικών μεταξύ τους) (κωδικο)λέξεων είναι ίση με $\sum_{a\in\mathbb{A}} m_a(M - m_a) = M^2 - \sum_{a\in\mathbb{A}} m_a^2$. Η διαδικασία αυτή επαναλαμβάνεται για όλες (n το πλήθος) στήλες του πίνακα, οπότε έχουμε $S \leq n(M^2 - \sum_{a\in\mathbb{A}} m_a^2)$. Το άθροισμα $\sum_{a\in\mathbb{A}} m_a^2$ λαμβάνει την ελάχιστη τιμή αν όλα τα m_a είναι ίσα με M/q (γιατί;). Επομένως, από την προηγούμενη σχέση έχουμε ότι $S \leq n(M^2 - M^2/q)$.

Συνδυάζοντας το κάτω φράγμα του S, που βρήκαμε παραπάνω με την τελευταία σχέση, έχουμε $M(M-1)d \leq S \leq n(M^2 - M^2/q)$. Αγνοώντας το S και λύνοντας ως προς M έχουμε την αποδεικτέα σχέση. ό.έ.δ.

Πόρισμα 1.5.24. ***(Φράγμα Plotkin)*** *Δεδομένου ότι ισχύει $d > \vartheta \cdot n$ έχουμε:*

$$A_q(n, d) \leq \frac{d}{d - \vartheta \cdot n}.$$

Όπως παρατηρούμε, το άνω φράγμα Plotkin εφαρμόζεται όταν ο κώδικας είναι αρκετά *αραιός*. Στην περίπτωση μάλιστα που το μέγεθος q του αλφάβητου είναι πολύ μεγάλο, τότε το $\vartheta = \frac{q-1}{q}$ *πλησιάζει* να γίνει 1, οπότε, για να εφαρμόσουμε το προηγούμενο πόρισμα, η ελάχιστη απόσταση του κώδικα πρέπει να είναι *σχεδόν* ίση με το μήκος n του κώδικα.

Ενδιαφέρον παρουσιάζει η περίπτωση των δυαδικών κωδίκων, όπου εκεί $\vartheta = \frac{q-1}{q} = \frac{1}{2}$. Εδώ θα δούμε πώς το προηγούμενο αποτέλεσμα εφαρμόζεται ακόμα και σε περιπτώσεις, όπου δεν ισχύει κατ' ανάγκη $d > \frac{1}{2}n$, διακρίνοντας αν η ελάχιστη απόσταση είναι άρτια ή περιττή.

Θεώρημα 1.5.25. ***(Το φράγμα Plotkin σε δυαδικούς κώδικες)***

Έστω $\mathcal{C}$ ένας δυαδικός (n, M, d) κώδικας.

1. Υποθέτουμε ότι η ελάχιστη απόσταση d είναι άρτια. Τότε για $d > \frac{1}{2}n$ έχουμε $A_2(n, d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$ και για $n = 2d$ (οπότε $d = \frac{1}{2}n$) έχουμε $A_2(2d, d) \leq 4d$.

2. Υποθέτουμε ότι η ελάχιστη απόσταση d είναι περιττή. Τότε για $d > \frac{1}{2}(n-1)$ έχουμε $A_2(n, d) \leq 2\lfloor \frac{d+1}{2d+1-n} \rfloor$ και για $d = \frac{1}{2}(n-1)$ έχουμε $A_2(2d+1, d) \leq 4(d+1)$.

Απόδειξη. 1. Αν $d > \frac{1}{2}n$, τότε στο προηγούμενο πόρισμα απλώς θέτουμε $\vartheta = \frac{1}{2}$ και έχουμε $A_2(n, d) \leq 2\lfloor \frac{d}{2d-n} \rfloor$.

Στην περίπτωση, όπου $d = 2k$ και $n = 2d = 4k$, από το Θεώρημα 1.5.16 έχουμε $A_2(n, d) = A_2(4k, 2k) \leq 2A_2(4k-1, 2k)$. Εφαρμόζοντας τώρα το προηγούμενο αποτέλεσμα η προηγούμενη σχέση συνεχίζεται ως:

$$A_2(n, d) = A_2(4k, 2k) \leq 2A_2(4k-1, 2k) \leq 4\lfloor \frac{2k}{4k-(4k-1)} \rfloor = 8k = 4d.$$

2. Εδώ έχουμε υποθέσει ότι η ελάχιστη απόσταση είναι περιττή. Από το Θεώρημα 1.5.14 έχουμε ότι $A_2(n, d) = A_2(n+1, d+1) \leq 2\lfloor \frac{d+1}{2d+1-n} \rfloor$.

Στην περίπτωση όπου $d = \frac{1}{2}(n-1)$, δηλαδή $n = 2d+1$, έχουμε, πάλι από το Θεώρημα 1.5.14 και τη δεύτερη σχέση της πρώτης περίπτωσης (αφού $d+1$ είναι άρτιος), ότι $A_2(n, d) = A_2(n+1, d+1) = A_2(2d+2, d+1) \leq 4(d+1)$. ό.έ.δ.

Παρατήρηση 1.5.26. Όπως είδαμε στην προηγούμενη απόδειξη, τα Θεωρήματα 1.5.14 και 1.5.16 είναι πολύ χρήσιμα στην εφαρμογή του φράγματος Plotkin και στην περίπτωση όπου $d \leq \frac{q-1}{q}n$.

Παραδείγματα 1.5.27. 1. Εφαρμόζοντας πρώτα διαδοχικά το Θεώρημα 1.5.16 και κατόπιν το προηγούμενο θεώρημα έχουμε:

$$A_2(13, 5) = 2^3 A_2(10, 5) \leq 8 \cdot 2\lfloor \frac{6}{11-10} \rfloor = 96.$$

2. Από το φράγμα ομαδοποίησης σφαιρών (Θεώρημα 1.5.8) έχουμε ότι $A_2(17, 9) \leq 65536/1607 \simeq 40$. Συνεπώς από το Θεώρημα 1.5.14 έχουμε

$A_2(18,10) = A_2(17,9) \leq 40$. Από το προηγούμενο όμως θεώρημα έχουμε ότι $A_2(18,10) \leq 10$.

3. Το φράγμα ομαδοποίησης σφαιρών δίνει ότι $A_2(14,7)$ είναι $8192/235 \simeq 34$. Συνεπώς, από το Θεώρημα 1.5.14 έχουμε $A_2(15,8) = A_2(14,7) \leq 34$. Από το προηγούμενο όμως θεώρημα έχουμε ότι $A_2(14,7) \leq 16$.

Η μελέτη των φραγμάτων, την οποία παρουσιάσαμε στην παράγραφο αυτή, δεν είναι εξαντλητική. Πολύ δε περισσότερο δεν ασχολούμαστε με την ασυμπτωτική συμπεριφορά τους. Για μια πληρέστερη μελέτη παραπέμπουμε στο αντίστοιχο κεφάλαιο του βιβλίου του Roman, S. "Coding and Information Theory". Springer-Verlag, 1992 Roman, S. [1992].

1.5.3 Ασκήσεις

1. Έστω $\mathcal{C}$ ένας κώδικας, ο οποίος δεν είναι βέλτιστος. Είναι δυνατόν να επισυνάψουμε στοιχεία στον $\mathcal{C}$, έτσι ώστε να προκύψει ένας βέλτιστος κώδικας;

2. Έστω $\mathbb{A}$ ένα αλφάβητο και $\mathbf{a}, \mathbf{b} \in \mathbb{A}^n$. Δείξτε ότι τα σύνολα:

$$S = \{\mathbf{x} \in \mathbb{A}^n \mid d(\mathbf{x},\mathbf{a}) < d(\mathbf{x},\mathbf{b})\} \quad \text{και} \quad T = \{\mathbf{x} \in \mathbb{A}^n \mid d(\mathbf{x},\mathbf{b}) < d(\mathbf{x},\mathbf{a})\}$$

έχουν το ίδιο πλήθος στοιχείων.

3. Δείξτε ότι, για $d_1 \geq d_2$, ισχύει: $A_q(n,d_1) \leq A_q(n,d_2)$.

4. Δείξτε ότι $A_2(n,2) = 2^{n-1}$.

5. Υπάρχει δυαδικός κώδικας με παραμέτρους $(8,29,3)$;

6. Να υπολογίσετε το κάτω και άνω φράγμα που αναφέρονται στο Θεώρημα 1.5.19 για τις ακόλουθες περιπτώσεις: $A_2(7,3)$, $A_2(10,5)$, $A_2(13,7)$, $A_2(14,7)$, $A_2(15,7)$. Συγκρίνετε με τις τιμές του πίνακα της σελίδας 64.

7. Να συγκρίνετε τα τρία άνω φράγματα Hamming, Singleton, Plotkin στις ακόλουθες περιπτώσεις:

$$A_2(7,5), \quad A_2(8,5), \quad A_2(9,5), \quad A_2(15,9).$$

8. Δείξτε ότι: $A_{10}(10, 3) \leq 100.000.000$.

9. Δείξτε ότι: $A_q(q+1, 3) \leq q^{q-1}$ και $A_q(q+1, 5) \leq \dfrac{2q^{q-2}}{q-1}$.

10. Δείξτε ότι αν το d είναι ίσο με μια δύμανη του 2, τότε $A_2(2d, d) = 4d$.

11. Έστω $\mathcal{C}$ ένας τέλειος δυαδικός κώδικας με παραμέτρους $(n, M, 7)$. Δείξτε ότι $n = 7$ ή $n = 23$.

12. Να δώσετε μια άλλη αποδειξη για το Πόρισμα 1.5.18. Δηλαδή δείξτε απευθείας ότι σε έναν βέλτιστο κώδικα, με ελάχιστη απόσταση ίση με d, η ακτίνα κάλυψης είναι το πολύ ίση με $d-1$.

13. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

Βιβλιογραφία

Hall, J.I. *Notes on Coding Theory*. (σε ηλεκτρονική μορφή). www.math.msu.edu/~jhall.

Herstein, I. N. *"Abstract Algebra"*. New York: Macmillan, 1990.

Hill, R. *"A First Course in Coding Theory"*. Oxford University Press, Oxford, 1986.

Justesen, J. and Hoholdt, T. *"A Course In Error-Correcting Codes"*. European Mathematical Society, 2004.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Pretzel, O. *"Error-Correcting Codes and Finite Fields"*. Oxford University Press, Oxford, 1992.

Roman, S. *"Coding and Information Theory"*. Springer-Verlag, 1992.

Vermani, L. *"Elements of Algebraic Coding Theory"*. Chapman and Hall, London, 1996.

Σ. Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1993.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

ΚΕΦΑΛΑΙΟ 2

Γραμμικοί Κώδικες

2.1 Η έννοια του Γραμμικού κώδικα

Μέχρι τώρα θεωρούσαμε έναν κώδικα $\mathcal{C}$ με παραμέτρους $(n,\, M,\, d)$ απλώς ως ένα υποσύνολο του συνόλου $\mathbb{A}^n$, όπου $\mathbb{A}$ είναι ένα αλφάβητο. Είχαμε, όμως, πει ότι συνήθως ως αλφάβητο θεωρούμε το σύνολο $\mathbb{A} = \mathbb{F}$, όπου $\mathbb{F}$ είναι ένα πεπερασμένο σώμα. Στην περίπτωση, όμως, αυτή το σύνολο $\mathbb{A}^n$ έχει αλγεβρική δομή, είναι διανυσματικός χώρος επί του σώματος $\mathbb{F}$. Επομένως, λογικό είναι να απαιτήσουμε ένας κώδικας, ως υποσύνολο του $\mathbb{A}^n$, να έχει και αυτός αλγεβρική δομή, να είναι διανυσματικός υπόχωρος του $\mathbb{A}^n$.

Ορισμός 2.1.1. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα, το οποίο στο εξής θα το θεωρούμε ως αλφάβητο. Ένας κώδικας $\mathcal{C} \subseteq \mathbb{F}^n$ θα λέγεται* ***γραμμικός*** *αν είναι διανυσματικός υπόχωρος του διανυσματικού χώρου $\mathbb{F}^n$.*

Παραδείγματα 2.1.2. 1. Ο δυαδικός κώδικας:

$$\mathcal{C} = \{\, 0000,\, 1011,\, 0110,\, 1101 \,\} \subseteq \mathbb{Z}_2^4$$

είναι γραμμικός (γιατί;).

2. Ο δυαδικός κώδικας $\mathcal{C} = \{0001, 1011, 0110, 1111\} \subseteq \mathbb{Z}_2^4$ δεν είναι γραμμικός (γιατί;).

3. Το σύνολο $\mathrm{B} = \{1000011, 0100101, 0010110, 0001111\}$ είναι γραμμικά ανεξάρτητο επί του $\mathbb{Z}_2$ (γιατί;). Επομένως, παράγει έναν δυαδικό γραμμικό κώδικα διάστασης 4.

4. Ο n-επαναληπτικός $\mathcal{R}_q(n)$ κώδικας είναι ένας γραμμικός κώδικας διάστασης ένα, για οποιοδήποτε μήκος n και για οποιοδήποτε πεπερασμένο σώμα $\mathbb{F}$ ως αλφάβητο[1] (γιατί;).

5. Έστω $\mathcal{E}_n$ το υποσύνολο του $\mathbb{F}^n$ που αποτελείται από όλες τις λέξεις $\mathbf{c} = c_1c_2\cdots c_n \in \mathbb{F}^n$ των οποίων το άθροισμα των χαρακτήρων ισούται με μηδέν, δηλαδή $\sum_{i=1}^{n} c_i = 0$. Δεν είναι δύσκολο να δούμε ότι το $\mathcal{E}_n$ είναι ένας γραμμικός κώδικας. Προφανώς, κάθε κώδικας μηδενικού αθροίσματος είναι υποσύνολο του $\mathcal{E}_n$.

Έστω k η διάσταση ενός γραμμικού κώδικα $\mathcal{C}$ ως διανυσματικού χώρου. Τότε, ως γνωστόν, το μέγεθός του είναι ίσο με $|\mathcal{C}| = q^k$, όπου q είναι το πλήθος του αλφάβητου (σώματος) $\mathbb{F}$. Δηλαδή η διάσταση ενός γραμμικού κώδικα καθορίζει και το μέγεθός του. Επομένως, στη συνέχεια, όταν αναφερόμαστε στις παραμέτρους ενός γραμμικού κώδικα αντί να λέμε ο κώδικας (n, q^k, d), θα λέμε ο κώδικας $[n, k, d]$. (Προσοχή στο συμβολισμό, οι παρενθέσεις γίνονται αγκύλες, όταν αντί για το μέγεθος του κώδικα χρησιμοποιούμε την διάστασή του. Επίσης, δεν σημαίνει ότι κάθε κώδικας μεγέθους μιας δύναμης ενός πρώτου αριθμού είναι γραμμικός).

Σημείωση: Ο μηδενικός κώδικας (που αποτελείται μόνο από τη μηδενική (κωδικο)λέξη) είναι προφανώς γραμμικός κώδικας με διάσταση μηδέν. Στα επόμενα, θα θεωρούμε, χωρίς ιδιαίτερη μνεία, μη μηδενικούς γραμμικούς κώδικες.

Το ότι ένας κώδικας είναι γραμμικός είναι πολύ σημαντικό, γι' αυτό, όπως θα δούμε παρακάτω, οι περισσότεροι *καλοί* κώδικες είναι γραμμικοί. Ως μια πρώτη συνέπεια της γραμμικότητας ενός κώδικα έχουμε:

[1] Ο δείκτης q δηλώνει το πλήθος των στοιχείων του σώματος $\mathbb{F}$.

Θεώρημα 2.1.3. *Έστω $\mathcal{C}$ ένας γραμμικός κώδικας. Η ελάχιστη απόστασή του ισούται με την ελάχιστη απόσταση των μη μηδενικών (κωδικο)λέξεων από τη μηδενική (κωδικο)λέξη* $\mathbf{0}$*. Δηλαδή* $d(\mathcal{C}) = \min\{\, d(\mathbf{c}, \mathbf{0}), \mathbf{c} \in \mathcal{C} \setminus \{\, \mathbf{0} \,\}\}$.

Απόδειξη. Προφανώς (γιατί προφανώς;) ισχύει:

$$d(\mathcal{C}) \leq \min\{\, d(\mathbf{c}, \mathbf{0}), \mathbf{c} \in \mathcal{C} \setminus \{\, \mathbf{0} \,\}\}.$$

Αντίστροφα, έστω $\mathbf{a}$, $\mathbf{b}$ δύο (κωδικο)λέξεις, τότε, ως γνωστόν, $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{a} - \mathbf{b}, \mathbf{0}) \geq \min\{\, d(\mathbf{c}, \mathbf{0}), \mathbf{c} \in \mathcal{C} \setminus \{\, \mathbf{0} \,\}\}$, διότι η διαφορά $\mathbf{c} = \mathbf{a} - \mathbf{b}$ ανήκει στον κώδικα $\mathcal{C}$, αφού ο κώδικας είναι γραμμικός. ό.έ.δ.

Η ελάχιστη απόσταση των λέξεων ενός γραμμικού κώδικα από τη μηδενική λέξη λέγεται **ελάχιστο βάρος** του κώδικα και συμβολίζεται με $w(\mathcal{C})$. Δηλαδή:

$$w(\mathcal{C}) = \min\{\, d(\mathbf{c}, \mathbf{0}), \mathbf{c} \in \mathcal{C} \setminus \{\, \mathbf{0} \,\}\}.$$

Το προηγούμενο θεώρημα έχει μεγάλη σημασία στην πράξη. Αρκεί να αναλογιστούμε την οικονομία χρόνου που επιτυγχάνουμε για τον υπολογισμό της ελάχιστης απόστασης ενός γραμμικού κώδικα μεγέθους M. Αντί για τον υπολογισμό της απόστασης $\binom{M}{2}$ ζευγών λέξεων, αρκεί να υπολογίσουμε μόνο την απόσταση $M - 1$ ζευγών λέξεων. Για παράδειγμα, υπολογίστε την ελάχιστη απόσταση στα προηγούμενα παραδείγματα γραμμικών κωδίκων.

Στη σελίδα 47 είχαμε δει πώς παίρνουμε μια αύξηση ενός δυαδικού κώδικα $\mathcal{C}$ επισυνάπτοντας το συμπλήρωμά του. Στην περίπτωση, όπου ο κώδικας $\mathcal{C}$ είναι γραμμικός, έχουμε ότι και ο κώδικας $\mathcal{C} \cup \mathcal{C}^c$ είναι γραμμικός. Συγκεκριμένα έχουμε.

Πρόταση 2.1.4. *Έστω $\mathcal{C}$ ένας (n, M, d) δυαδικός γραμμικός κώδικας. Η λέξη $\mathbf{1} = 1\,1 \cdots 1$ ανήκει στον κώδικα $\mathcal{C}$, αν και μόνο αν $\mathcal{C} = \mathcal{C}^c$. (Στην περίπτωση αυτή ο κώδικας ονομάζεται* ***συμπληρωματικά αναλλοίωτος****.)*

Αν η λέξη $\mathbf{1} = 1\,1 \cdots 1$ δεν ανήκει στον κώδικα $\mathcal{C}$, τότε:

Ο κώδικας $\mathcal{C}^c$ δεν είναι γραμμικός.

$\mathcal{C} \cap \mathcal{C}^c = \emptyset$.

Η ένωση $\mathcal{C} \cup \mathcal{C}^c$ *είναι γραμμικός κώδικας με παραμέτρους* $(n, 2M, \bar{d})$, *όπου:*

$$\bar{d} = min\{\, d(\mathcal{C}),\, n - max\{\, d(\mathbf{c}, \mathbf{d}),\, \mathbf{c}, \mathbf{d} \in \mathcal{C}\,\}\,\}.$$

Απόδειξη. Η απόδειξη είναι εύκολη και αφίεται ως άσκηση, αρκεί να ανατρέξουμε στη σελίδα 47 και παράλληλα να εφαρμόσουμε τον ορισμό του γραμμικού κώδικα. (Δείξτε ότι, αν $\{\, \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k \,\}$ είναι μια βάση του κώδικα $\mathcal{C}$, τότε το σύνολο $\{\, \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_k \,\} \cup \{\, \mathbf{1} = 11\cdots 1 \,\}$ είναι βάση του $\mathcal{C} \cup \mathcal{C}^c$.) ό.έ.δ.

2.1.1 Γεννήτορες πίνακες ενός Γραμμικού κώδικα

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{F}$. Ο κώδικας $\mathcal{C}$, ως διανυσματικός υπόχωρος του $\mathbb{F}^n$, έχει μια βάση $\mathbf{B} = \{\, \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k} \,\}$. Για κάθε (κωδικο)λέξη $\mathbf{c}$ υπάρχουν (μοναδικά) $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}$, έτσι ώστε $\mathbf{c} = \lambda_1\mathbf{b_1} + \lambda_2\mathbf{b_2} + \cdots + \lambda_k\mathbf{b_k}$. Αντίστροφα για κάθε $\mathbf{r} = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k$ το στοιχείο $\lambda_1\mathbf{b_1} + \lambda_2\mathbf{b_2} + \cdots + \lambda_k\mathbf{b_k}$ ανήκει στον κώδικα $\mathcal{C}$.

Έστω τώρα G ο $k \times n$ πίνακας, του οποίου οι γραμμές αποτελούνται από τα στοιχεία της βάσης $\mathbf{B}$. Τότε, εφαρμόζοντας τον ορισμό του πολλαπλασιασμού πινάκων, από τα προηγούμενα έχουμε ότι $\mathcal{C} = \{\, \mathbf{r} \cdot \mathrm{G} \mid \mathbf{r} \in \mathbb{F}^k \,\}$.

Ορισμός 2.1.5. *Έστω* $\mathcal{C}$ *ένας* $[n, k, d]$ *γραμμικός κώδικας επί του σώματος* $\mathbb{F}$. *Ένας* $k \times n$ *πίνακας, του οποίου οι γραμμές αποτελούν μια βάση του* $\mathcal{C}$, *ονομάζεται* ***γεννήτορας πίνακας*** *του* $\mathcal{C}$.

Παραδείγματα 2.1.6.

1. Ένας γεννήτορας πίνακας του δυαδικού γραμμικού κώδικα $\mathcal{C} = \{\, 0000, 1011, 0110, 1101 \,\} \subseteq \mathbb{Z}_2^4$ είναι ο πίνακας $\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$ (γιατί;).
2. Το σύνολο $\mathrm{B} = \{\, 1000011, 0100101, 0010110, 0001111 \,\}$ είναι γραμμικά ανεξάρτητο επί του $\mathbb{Z}_2$ (γιατί;). Επομένως, ο παραγόμενος δυαδικός γραμμικός κώδικας έχει ως γεννήτορα πίνακα τον πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

3. Ο $n-$επαναληπτικός κώδικας $\mathcal{R}_r(n)$ $r-$αδικός κώδικας έχει ως γεννήτορα πίνακα τον $1 \times n$ πίνακα $\mathrm{G} = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}$ (γιατί;).

Προφανώς, σε έναν γραμμικό κώδικα, όταν λαμβάνουμε μια άλλη βάση, τότε έχουμε και έναν άλλο γεννήτορα πίνακα.

Από την Γραμμική Άλγεβρα είναι γνωστό το επόμενο αποτέλεσμα, που αναφέρεται στο πώς σχετίζονται δύο γεννήτορες πίνακες ενός γραμμικού κώδικα.

Λήμμα 2.1.7. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και* R *ένας $k \times k$ αντιστρέψιμος πίνακας με στοιχεία από το αλφάβητο $\mathbb{F}$. Τότε για κάθε γεννήτορα πίνακα* G *του κώδικα, το γινόμενο* RG *είναι γεννήτορας πίνακας του κώδικα. Αντίστροφα, έστω* G_1 *και* G_2 *δύο γεννήτορες πίνακες του κώδικα, τότε υπάρχει ένας $k \times k$ αντιστρέψιμος πίνακας* R *με στοιχεία από το αλφάβητο $\mathbb{F}$, τέτοιος ώστε* $\mathrm{G}_2 = \mathrm{RG}_1$.

Απόδειξη. Έστω $\{ \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k} \}$ μία βάση του $\mathcal{C}$ της οποίας τα στοιχεία αποτελούν τις γραμμές του γεννήτορα πίνακα G. Δηλαδή:

$$\mathrm{G} = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_k} \end{pmatrix}.$$

Επίσης, έστω R ο αντιστρέψιμος πίνακας $(\lambda_{ij})_{k \times k}$. Τότε η $i-$γραμμή του γινομένου RG είναι ίση με $\lambda_{i1}\mathbf{b_1} + \lambda_{i2}\mathbf{b_2} + \cdots + \lambda_{ik}\mathbf{b_k}$. Επομένως, οι γραμμές του πίνακα RG παράγουν έναν υπόχωρο του $\mathcal{C}$. Αλλά ως γνωστόν η τάξη του γινομένου RG είναι μικρότερη ή ίση από την τάξη του πίνακα G. Επίσης, η τάξη του πίνακα $\mathrm{G} = \mathrm{R}^{-1}(\mathrm{RG})$ είναι μικρότερη ή ίση από την τάξη του πίνακα RG, άρα οι δύο πίνακες G και RG έχουν την ίδια τάξη. Δηλαδή οι γραμμές του πίνακα είναι γραμμικώς ανεξάρτητες και, επομένως, ο υπόχωρος του $\mathcal{C}$ που παράγουν είναι ολόκληρος ο κώδικας $\mathcal{C}$. Άρα, ο πίνακας RG είναι γεννήτορας πίνακας του κώδικα.

Αντίστροφα, έστω G_1 και G_2 δύο γεννήτορες πίνακες του κώδικα οι γραμ-

μές των οποίων αποτελούν βάσεις του κώδικα. Δηλαδή:

$$\mathrm{G}_1 = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_k} \end{pmatrix} \quad \text{και} \quad \mathrm{G}_2 = \begin{pmatrix} \mathbf{c_1} \\ \mathbf{c_2} \\ \vdots \\ \mathbf{c_k} \end{pmatrix}.$$

Εκφράζουμε τα στοιχεία της βάσης $\{\, \mathbf{c_1}, \mathbf{c_2}, \dots, \mathbf{c_k} \,\}$ ως γραμμικό συνδυασμό των στοιχείων της βάσης $\{\, \mathbf{b_1}, \mathbf{b_2}, \dots, \mathbf{b_k} \,\}$. Δηλαδή $\mathbf{c_i} = \lambda_{i1}\mathbf{b_1} + \lambda_{i2}\mathbf{b_2} + \cdots + \lambda_{ik}\mathbf{b_k}$ για $i = 1, 2, \dots, k$. Ο $k \times k$ πίνακας $\mathrm{R} = (\lambda_{ij})$ προφανώς έχει την ιδιότητα $\mathrm{G}_2 = \mathrm{RG}_1$ και, επιπλέον, είναι αντιστρέψιμος, αφού αποτελεί τον πίνακα αλλαγής βάσης. ό.έ.δ.

Παράδειγμα 2.1.8. Για τους κώδικες που αναφέρονται στα τρία προηγούμενα παραδείγματα μπορείτε να κατασκευάσετε άλλους γεννήτορες πίνακες εφαρμόζοντας το προηγούμενο λήμμα.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και $\sigma \in S_n$ μια μετάθεση n-συμβόλων. Εφαρμόζοντας την σ στους χαρακτήρες κάθε (κωδικο)λέξης $\mathbf{c} = (\, a_1, a_2, \dots, a_n \,) \in \mathcal{C}$ λαμβάνουμε, ως γνωστόν έναν ισοδύναμο κώδικα, έστω $\mathcal{C}_\sigma$. Δηλαδή $\mathcal{C}_\sigma = \{\, \sigma(\mathbf{c}) = (\, a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)} \,) \mid \mathbf{c} \in \mathcal{C} \,\}$.

Έστω τώρα P_σ ο πίνακας μετάθεσης, ο οποίος προκύπτει από τον ταυτοτικό πίνακα $\mathrm{I}_{n\times n}$ αν εφαρμόσουμε μια μετάθεση $\sigma \in S_n$ στις γραμμές του. Προφανώς, ο πίνακας P_σ είναι αντιστρέψιμος (έχει τάξη n). Δεν είναι δύσκολο να δούμε ότι για κάθε $\mathbf{c} = (\, a_1, a_2, \dots, a_n \,) \in \mathcal{C}$ ισχύει $(\, a_1, a_2, \dots, a_n \,)\mathrm{P}_\sigma = (\, a_{\sigma(1)}, a_{\sigma(2)}, \dots, a_{\sigma(n)} \,)$. Δηλαδή $\mathcal{C}_\sigma = \{\, \mathbf{c}\,\mathrm{P}_\sigma \mid \mathbf{c} \in \mathcal{C} \,\}$ (Πρόταση 1.4.6). Αυτό είναι ισοδύναμο με το ότι αν ο πίνακας G είναι γεννήτορας πίνακας του κώδικα $\mathcal{C}$, τότε ο πίνακας GP_σ είναι γεννήτορας πίνακας του κώδικα $\mathcal{C}_\sigma$.

Από τα προηγούμενα έπεται η επόμενη πρόταση.

Πρόταση 2.1.9. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και $\sigma \in S_n$ μια μετάθεση $n-$συμβόλων. Τότε και ο μεταθετικά ισοδύναμος κώδικας $\mathcal{C}_\sigma$ είναι γραμμικός.*

Απόδειξη. Είναι εύκολο να ελέγξουμε ότι ο κώδικας $\mathcal{C}_\sigma$ είναι ένας διανυσματικός χώρος, αφού ο $\mathcal{C}$ είναι διανυσματικός χώρος (άσκηση).

Διαφορετικά θα μπορούσαμε να πούμε ότι:
Ως γνωστόν σε κάθε πίνακα αντιστοιχεί μια γραμμική απεικόνιση (γιατί;), και γραμμικές απεικονίσεις απεικονίζουν διανυσματικούς χώρους σε διανυσματικούς χώρους. ό.έ.δ.

Ως γνωστόν οι ισοδύναμοι κώδικες $\mathcal{C}$ και $\mathcal{C}_\sigma$ έχουν τις ίδιες παραμέτρους (μήκος, μέγεθος και ελάχιστη απόσταση). Δηλαδή είναι *εξίσου αποτελεσματικοί*. Επομένως, το επόμενο θεώρημα αποκτά ιδιαίτερη σημασία στη θεωρία των γραμμικών κωδίκων.

Θεώρημα 2.1.10. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$. Τότε υπάρχει ένας ισοδύναμος γραμμικός κώδικας $\bar{\mathcal{C}}$, ο οποίος έχει ως γεννήτορα πίνακα έναν $k \times n$ πίνακα του οποίου οι k πρώτες στήλες σχηματίζουν τον ταυτοτικό πίνακα I_k.*

Απόδειξη. Έστω G ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}$. Ο πίνακας αυτός έχει k το πλήθος γραμμικώς ανεξάρτητες στήλες. Έστω $\sigma \in S_n$ μια μετάθεση, η οποία μεταθέτει τις στήλες του πίνακα G κατά τέτοιο τρόπο, ώστε οι k το πλήθος γραμμικώς ανεξάρτητες στήλες να καταλάβουν τις k πρώτες θέσεις στις στήλες του πίνακα G. Έστω P_σ ο πίνακας της μετάθεσης σ και M ο πίνακας που προκύπτει από τον πίνακα G σύμφωνα με την προηγούμενη διαδικασία. Τότε είναι εύκολο να παρατηρήσουμε ότι ισχύει $\mathrm{M} = \mathrm{GP}_\sigma$.

Έστω $\bar{\mathcal{C}}$ ο γραμμικός κώδικας που έχει ως γεννήτορα πίνακα τον πίνακα M. Δηλαδή:

$$\begin{aligned}\bar{\mathcal{C}} &= \{\, (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{M} \mid (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k \,\} \\ &= \{\, (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{GP} \mid (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k \,\} = \{\, \mathbf{c}\mathrm{P}_\sigma \mid \mathbf{c} \in \mathcal{C} \,\}.\end{aligned}$$

Ο κώδικας $\bar{\mathcal{C}}$ είναι ισοδύναμος ως προς τον κώδικα $\mathcal{C}$ και οι k πρώτες στήλες του γεννήτορα πίνακα M είναι γραμμικώς ανεξάρτητες. Έστω R ο $k \times k$ (υπο)πίνακας που σχηματίζουν οι k πρώτες στήλες του πίνακα M και S ο $k \times n - k$ (υπο)πίνακας που σχηματίζουν οι $n - k$ υπόλοιπες στήλες του πίνακα M. Δηλαδή ο πίνακας M έχει τη μορφή $\mathrm{M} = [\mathrm{R} \quad \mathrm{S}]$. Ο πίνακας R είναι αντιστρέψιμος (γιατί;), επομένως από το Λήμμα 2.1.7 έχουμε ότι ο πίνακας

$\mathrm{R}^{-1}\mathrm{M}$ είναι γεννήτορας πίνακας του κώδικα $\bar{\mathcal{C}}$. Αλλά $\mathrm{R}^{-1}\mathrm{M} = \mathrm{R}^{-1}[\mathrm{R} \quad \mathrm{S}] = [\mathrm{R}^{-1}\mathrm{R} \quad \mathrm{R}^{-1}\mathrm{S}] = [\mathrm{I}_k \quad \mathrm{R}^{-1}\mathrm{S}]$.

Ο πίνακας $\mathrm{N} = [\mathrm{I}_k \quad \mathrm{R}^{-1}\mathrm{S}]$ είναι ο γεννήτορας πίνακας του κώδικα $\bar{\mathcal{C}}$ με την απαιτούμενη ιδιότητα. ό.έ.δ.

Ορισμός 2.1.11. *Ένας $k \times n$ πίνακας* A *με τάξη k θα λέγεται* ***ανηγμένος κλιμακωτός*** *αν είναι της μορφής* $\mathrm{A} = [\mathrm{I}_k \quad \mathrm{B}]$.

Τα προηγούμενα συνοψίζονται στο επόμενο πόρισμα.

Πόρισμα 2.1.12. *Για κάθε γραμμικό κώδικα υπάρχει ένας μεταθετικά ισοδύναμος γραμμικός κώδικας με γεννήτορα πίνακα έναν ανηγμένο κλιμακωτό πίνακα.*

Όπως έχουμε επισημάνει ισοδύναμοι κώδικες έχουν τις ίδιες παραμέτρους, επομένως έχουν την ίδια αποτελεσματικότητα στην ανίχνευση/διόρθωση λαθών. Για τον λόγο αυτό, πολλές φορές είναι προτιμότερο, αντί του αρχικού κώδικα, να εργαζόμαστε με έναν ισοδύναμο κώδικα που έχει γεννήτορα πίνακα σε ανηγμένη κλιμακωτή μορφή. Ως παράδειγμα θα δώσουμε μια άλλη απόδειξη του φράγματος Singleton (Θεώρημα 1.5.21) στην περίπτωση των γραμμικών κωδίκων.

Πρόταση 2.1.13. *Αν $\mathcal{C}$ είναι ένας $[n, k, d]$ γραμμικός κώδικας, τότε:*

$$d \leq n - k + 1.$$

Απόδειξη. Από τα προηγούμενα μπορούμε να υποθέσουμε ότι ο κώδικας έχει γεννήτορα πίνακα G σε ανηγμένη κλιμακωτή μορφή. Δηλαδή $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{B}]$. Κάθε γραμμή του πίνακα G είναι μια (κωδικο)λέξη με 0 σε τουλάχιστον $k-1$ το πλήθος θέσεις. Επομένως, έχει βάρος το πολύ ίσον με $n - (k - 1)$. Οπότε από το Θεώρημα 2.1.3 έχουμε ότι $d \leq n - k + 1$. ό.έ.δ.

Θα επανέλθουμε στην μελέτη ισοδυνάμων γραμμικών κωδίκων (ιδέ Παράγραφο 2.3.1

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ με γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ σε ανηγμένη κλιμακωτή μορφή. Επειδή:

$$\mathcal{C} = \{ (\lambda_1, \lambda_2, \dots, \lambda_k) \cdot \mathrm{G} \mid (\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{F}^k \},$$

κάθε (κωδικο)λέξη μπορεί να χωρισθεί σε δύο τμήματα. Το πρώτο τμήμα που αποτελείται από τους k πρώτους χαρακτήρες μπορεί να είναι οποιοδήποτε στοιχείο $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k$, ενώ το υπόλοιπο τμήμα της των $n-k$ χαρακτήρων προσδιορίζεται από το πρώτο τμήμα βάσει του κανόνα $(\lambda_1, \lambda_2, \ldots, \lambda_k)\mathrm{A}$. Για τον λόγο αυτό, συνήθως, το πρώτο τμήμα το ονομάζουμε **τμήμα πληροφορίας** και το υπόλοιπο το ονομάζουμε **τμήμα ελέγχου ισοτιμίας**, καθότι οι k πρώτοι χαρακτήρες *περικλείουν* τη μεταδιδόμενη πληροφορία, ενώ οι υπόλοιποι $n-k$ χαρακτήρες *ελέγχουν* τη σωστή μετάδοση της πληροφορίας. Γενικά, τέτοιοι κώδικες ονομάζονται **συστηματικοί κώδικες** ή **διαχωρίσιμοι κώδικες**.

Η χρήση συστηματικών κωδίκων προσφέρει πολλά πλεονεκτήματα. Αρκεί να αναλογισθούμε την οικονομία χρόνου που επιτυγχάνουμε, καθότι μπορούμε να αποστέλλουμε το τμήμα πληροφορίας, ενώ ταυτόχρονα υπολογίζουμε το τμήμα ελέγχου ισοτιμίας.

Υπάρχει μια διαδικασία (αλγόριθμος) με την οποία, για δεδομένο γραμμικό κώδικα, μπορούμε να προδιορίσουμε τον αντίστοιχο ισοδύναμο κώδικα του οποίου ο γεννήτορας πίνακας είναι σε ανηγμένη κλιμακωτή μορφή.

Έστω ένας $m \times n$ πίνακας A με στοιχεία από ένα σώμα $\mathbb{F}$, στις γραμμές και στις στήλες του πίνακα μπορούμε να πραγματοποιήσουμε τους εξής μετασχηματισμούς.

1. Να αντιμεταθέσουμε δύο γραμμές του πίνακα.
2. Να πολλαπλασιάσουμε μια γραμμή του πίνακα με ένα μη μηδενικό στοιχείο του σώματος.
3. Να προσθέσουμε ένα πολλαπλάσιο μιας γραμμής σε μια άλλη γραμμή.
4. Να αντιμεταθέσουμε δύο στήλες του πίνακα.
5. Να πολλαπλασιάσουμε μια στήλη του πίνακα με ένα μη μηδενικό στοιχείο του σώματος.

Οι παραπάνω πέντε μετασχηματισμοί λέγονται **στοιχειώδεις μετασχηματισμοί** του πίνακα.

Το επόμενο θεώρημα, το οποίο παραθέτουμε χωρίς απόδειξη, αποτελεί τη γνωστή (σχεδόν) σε όλους μας *Μέθοδο απαλοιφής του Gauss*.

Θεώρημα 2.1.14. *Εφαρμόζοντας μια πεπερασμένη ακολουθία στοιχειωδών μετασχηματισμών, κάθε $m \times n$ πίνακας* A, *με στοιχεία από ένα σώμα* $\mathbb{F}$, *μπορεί να λάβει τη μορφή:*

$$\left(\begin{array}{c|c} \mathrm{I}_r & \mathrm{B} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right).$$

Όπου r είναι η τάξη του πίνακα A, *ο* B *είναι ένας $r \times (n-r)$ πίνακας και* $\mathbf{0}$ *μηδενικοί πίνακες αντίστοιχων διαστάσεων.*

Απόδειξη. Η ιδέα της απόδειξης είναι απλούστατη και μπορεί ο καθένας μας από μόνος του να τη συλλάβει. Άλλωστε σε όλα τα βιβλία Γραμμικής Άλγεβρας υπάρχει μια απόδειξη αντίστοιχου θεωρήματος.

ό.έ.δ.

Παρατηρήσεις 2.1.15.

1. Ίσως αναρωτηθεί κάποιος. Γιατί στους στοιχειώδεις μετασχηματισμούς αναφέρεται ότι μπορούμε να προσθέσουμε ένα πολλαπλάσιο μιας γραμμής σε μια άλλη γραμμή, ενώ δεν αναφέρεται ότι μπορούμε να προσθέσουμε ένα πολλαπλάσιο μιας στήλης σε μια άλλη στήλη; Προσπαθήστε να δώσετε μια απάντηση.

2. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας με γεννήτορα πίνακα $\mathrm{G} = (\,\mathbf{b_1}\ \mathbf{b_2}\ \cdots\ \mathbf{b_n}\,)$, όπου τα $\mathbf{b_i}$ είναι στήλες του πίνακα. Μπορεί ο πίνακας G να μην είναι σε ανηγμένη κλιμακωτή μορφή, αλλά ενδέχεται να υπάρχουν δείκτες $i_1, i_2, \ldots, i_k$, έτσι ώστε οι αντίστοιχες k το πλήθος στήλες $\mathbf{b_{i_j}}$ να σχηματίζουν τον ταυτοτικό $k \times k$ πίνακα. Στην περίπτωση αυτή, για κάθε $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k$, από τη σχέση $(\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G}$ έπεται ότι η μεταδιδόμενη πληροφορία *διαχέεται* στην αντίστοιχη (κωδικο)λέξη παραμένοντας όμως αναλλοίωτη.

2.1.2 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Έστω ο n-επαναληπτικός $\mathcal{R}_q(n)$ κώδικας. Να υπολογίσετε έναν γεννήτορα πίνακά του.

3. Έστω $\mathcal{A}_n$ το σύνολο όλων των λέξεων του $\mathbb{Z}_2^n$ αρτίου βάρους. Δείξτε ότι το $\mathcal{A}_n$ είναι γραμμικός κώδικας. Υπολογίστε τις παραμέτρους του. Υπολογίστε μια βάση του και γράψτε έναν γεννήτορα πίνακα σε κανονική μορφή.

4. Έστω $\mathcal{E}_n$ το υποσύνολο του $\mathbb{F}^n$ που αποτελείται από όλες τις λέξεις $\mathbf{c} = c_1c_2\cdots c_n \in \mathbb{F}^n$ των οποίων το άθροισμα των χαρακτήρων ισούται με μηδέν, δηλαδή $\sum_{i=1}^{n} c_i = 0$. Στο Παράδειγμα 2.1.2$_5$ είχαμε δει ότι το $\mathcal{E}_n$ είναι ένας γραμμικός κώδικας. Να υπολογίσετε τις παραμέτρους του και έναν γεννήτορα πίνακα.

5. Να δείξετε ότι σε έναν δυαδικό γραμμικό κώδικα $\mathcal{C}$ είτε όλες οι (κωδικο)λέξεις έχουν άρτιο βάρος είτε ακριβώς οι μισές το πλήθος έχουν περιττό βάρος.

   Υποθέτουμε ότι ο κώδικας περιέχει μια (κωδικο)λέξη $\mathbf{c}$ περιττού βάρους. Δείξτε ότι κάθε άλλη (κωδικο)λέξη περιττού βάρους είναι της μορφής $\mathbf{c}+\mathbf{x}$, όπου $\mathbf{x}$ είναι (κωδικο)λέξη αρτίου βάρους.

   Ισχύει κάτι ανάλογο σε τριαδικούς κώδικες;

6. Δείξτε ότι σε έναν γραμμικό κώδικα μεγέθους M επί του σώματος $\mathbb{Z}_p$ είτε όλες οι (κωδικο)λέξεις αρχίζουν με 0, είτε ακριβώς M/p το πλήθος αρχίζουν με μηδέν.

7. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Δείξτε ότι, αν i είναι μια σταθερή συντεταγμένη, τότε είτε όλες οι (κωδικο)λέξεις έχουν 0 σε αυτή την συντεταγμένη είτε το υποσύνολο που αποτελείται από όλες τις (κωδικο)λέξεις, οι οποίες έχουν 0 στην i συντεταγμένη είναι ένας $[n, k-1, d]$ γραμμικός υποκώδικας του κώδικα $\mathcal{C}$.

8. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{F}$ με q το πλήθος στοιχεία.

Κατασκευάζουμε έναν $q^k \times n$ πίνακα του οποίου οι γραμμές είναι τα στοιχεία του κώδικα $\mathcal{C}$. Δείξτε ότι κάθε στοιχείο του σώματος $\mathbb{F}$ εμφανίζεται σε κάθε μη μηδενική στήλη του πίνακα ακριβώς q^{k-1} το πλήθος φορές.

Υπόδειξη: Έστω $(a_1, a_2, \ldots, a_k)$ ένα μη μηδενικό στοιχείο του $\mathbb{F}^k$. Δείξτε ότι η απεικόνιση $f : \mathbb{F}^k \longrightarrow \mathbb{F}$ με $f(x_1, x_2, \ldots, x_k) = \sum_{i=1}^{k} a_i x_i$ είναι γραμμική, επί και να υπολογίσετε τον πυρήνα της.

9. Να επανεξετάσετε τις ασκήσεις 4, 5, 6 υπό το πρίσμα της προηγουμένης άσκησης.

10. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{Z}_p$. Δείξτε ότι το άθροισμα των βαρών όλων των στοιχείων του $\mathcal{C}$ είναι το πολύ ίσο με $n(p-1)p^{k-1}$.

11. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του σώματος $\mathbb{F}$ με q το πλήθος στοιχεία.

    Δείξτε ότι το πλήθος των διακεκριμένων γεννητόρων πινάκων του $\mathcal{C}$ ισούται με $\prod_{i=0}^{k-1}(q^k - q^i)$.

    Υπόδειξη: Αν έχουμε ένα σύνολο με i το πλήθος γραμμικά ανεξάρτητα διανύσματα στον διανυσματικό χώρο $\mathbb{F}^k$, με πόσους τρόπους μπορούμε να επιλέξουμε ένα επιπλέον διάνυσμα, ώστε να έχουμε $i+1$ το πλήθος γραμμικά ανεξάρτητα διανύσματα;

12. Έστω $\mathcal{C} \subseteq \mathbb{Z}_5^4$ ο $5-$αδικός γραμμικός κώδικας, ο οποίος παράγεται από το σύνολο $\{\, 0123,\ 0314,\ 0432 \,\}$. Να υπολογίσετε έναν γεννήτορα πίνακα σε κανονική μορφή και κατόπιν να υπολογίσετε τις παραμέτρους του.

13. Έστω $\mathcal{C}_1$, $\mathcal{C}_2$ δύο (μη μηδενικοί) γραμμικοί κώδικες του ιδίου μήκους n επί του σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Ορίζουμε τους εξής κώδικες:

$$\begin{aligned}
\mathcal{C}_3 &= \mathcal{C}_1 \cup \mathcal{C}_2, \\
\mathcal{C}_4 &= \mathcal{C}_1 \cap \mathcal{C}_2, \\
\mathcal{C}_5 &= \mathcal{C}_1 + \mathcal{C}_2 = \{\, \mathbf{c}_1 + \mathbf{c}_2 : \mathbf{c}_1 \in \mathcal{C}_1 \text{ και } \mathbf{c}_2 \in \mathcal{C}_2 \,\}.
\end{aligned}$$

Για κάθε $i = 1, 2, \ldots, 5$ ορίζουμε $k_i = \log_q \mid \mathcal{C}_i \mid$ και d_i να είναι η ελάχιστη απόσταση του $\mathcal{C}_i$.

Δείξτε οτι:

i) Ο κώδικας $\mathcal{C}_3$ είναι γραμμικός, αν και μόνο αν είτε $\mathcal{C}_1 \subseteq \mathcal{C}_2$ είτε $\mathcal{C}_2 \subseteq \mathcal{C}_1$.

ii) Οι κώδικες $\mathcal{C}_4, \mathcal{C}_5$ είναι γραμμικοί.

iii) Αν $k_4 \neq 0$, τότε $d_4 \geq \max(d_1, d_2)$.

iv) $k_5 = k_1 + k_2 - k_4$.

v) $d_5 \leq \min(d_1, d_2)$.

vi) Έστω G ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}_4 = \mathcal{C}_1 \cap \mathcal{C}_2$. Δείξτε ότι υπάρχουν πίνακες G_1 και G_2 με n το πλήθος στήλες, ώστε ο πίνακας:

$$\Gamma = \begin{pmatrix} \mathrm{G} \\ \mathrm{G}_1 \\ \mathrm{G}_2 \end{pmatrix}$$

να είναι γεννήτορας πίνακας του κώδικα $\mathcal{C}_5 = \mathcal{C}_1 + \mathcal{C}_2$.

14. Έστω $\mathcal{C}_1$, $\mathcal{C}_2$ δύο (μη μηδενικοί) γραμμικοί κώδικες επί του σώματος $\mathbb{F}$ με q το πλήθος στοιχεία με αντίστοιχα μήκη n_1 και n_2. Ορίζουμε τον εξής κώδικα:

$$\mathcal{C}_6 = \mathcal{C}_1 \mid \mathcal{C}_2 = \{\, \mathbf{c}_1 \mid \mathbf{c}_2 \,:\, \mathbf{c}_1 \in \mathcal{C}_1 \text{ και } \mathbf{c}_2 \in \mathcal{C}_2 \,\},$$

όπου με $\mathbf{c}_1 \mid \mathbf{c}_2$ συμβολίζουμε την παράθεση των $\mathbf{c}_1$ και $\mathbf{c}_2$.[2]

Υποθέτουμε ότι οι πίνακες $\mathrm{G}_1, \mathrm{G}_2$ είναι γεννήτορες των $\mathcal{C}_1$ και $\mathcal{C}_2$ αντίστοιχα. Δείξτε ότι ο πίνακας:

$$\begin{pmatrix} \mathrm{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathrm{G}_2 \end{pmatrix}$$

[2] Ο κώδικας $\mathcal{C}_1 \mid \mathcal{C}_2$ στην βιβλιογραφία αναφέρεται ως ευθύ άθροισμα των δύο κωδίκων και δεν πρέπει να γίνεται σύγχυση με τον κώδικα $\mathcal{C}_5$ της προηγούμενης άσκησης, ο οποίος είναι το άθροισμα δύο κωδίκων (του ιδίου μήκους n) ως υποχώρων του διανυσματικού χώρου $\mathbb{F}^n$.

είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}_1 \mid \mathcal{C}_2$.

Επομένως $k_6 = k_1 + k_2$ και $d_6 = \min(d_1, d_2)$.

15. Έστω $\mathcal{C}$, $\mathcal{D}$ γραμμικοί κώδικες του ιδίου μήκους. Δείξτε ότι ο κώδικας που προκύπτει από μια $(\mathbf{u}, \mathbf{u}+\mathbf{v})$- κατασκευή είναι, επίσης, γραμμικός. Υπολογίστε τις παραμέτρους του. Αν G, D είναι γεννήτορες πίνακες των $\mathcal{C}$ και $\mathcal{D}$ αντίστοιχα, να δείξετε ότι ένας γεννήτορας πίνακας του νέου κώδικα είναι ο:
$$\begin{pmatrix} \mathrm{G} & \mathrm{G} \\ \mathbf{0} & \mathrm{D} \end{pmatrix}.$$

16. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ γραμμικοί κώδικες, επί του ιδίου σώματος $\mathbb{F}$, με παραμέτρους $[n_1, k_1, d_1]$ και $[n_2, k_2, d_2]$ αντίστοιχα και γεννήτορες πίνακες G_1 και G_2 αντίστοιχα. Έστω $\mathcal{C}$ ο γραμμικός κώδικας με γεννήτορα πίνακα:
$$\mathrm{G} = \begin{pmatrix} \mathbf{0} & \mathrm{G}_1 \\ \mathrm{G}_2 & * \end{pmatrix},$$
όπου στη θέση του $*$ είναι ένας τυχαίος $k_2 \times n_1$ πίνακας με στοιχεία από το σώμα. Δείξτε ότι η ακτίνα κάλυψης του κώδικα $\mathcal{C}$ είναι μικρότερη ή ίση από το άθροισμα των ακτίνων κάλυψης των κωδίκων $\mathcal{C}_1$ και $\mathcal{C}_2$. Δηλαδή $cr(\mathcal{C}) \leq cr(\mathcal{C}_1) + cr(\mathcal{C}_2)$. (Για την ακτίνα κάλυψης ιδέ τον Ορισμό 1.5.9).

17. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας με παραμέτρους $[n, k, d]$. Δείξτε ότι μπορούμε να επιλέξουμε έναν γεννήτορα πίνακα του κώδικα της μορφής:
$$\mathrm{G} = \begin{pmatrix} 1 & \cdots & 1 & 0 & \cdots & 0 \\ & \mathrm{G}_1 & & & \mathrm{G}_2 & \end{pmatrix},$$
όπου το πλήθος των 1 στην πρώτη γραμμή ισούται με d και G_1, G_2 είναι πίνακες με διαστάσεις $(k-1) \times d$ και $(k-1) \times (n-d)$ αντίστοιχα.

Δείξτε ότι ο γραμμικός κώδικας $\mathcal{C}_2$, που έχει ως γεννήτορα πίνακα τον πίνακα G_2, έχει ελάχιστη απόσταση $d_2 \geq d/2$.

2.2 Δυϊκοί κώδικες

Στα προηγούμενα είδαμε ότι η Γεωμετρική έννοια της απόστασης αποτελεί το βασικότερο συστατικό στην κατασκευή και στον χειρισμό ενός κώδικα. Εδώ θα δούμε πώς μια άλλη Γεωμετρική έννοια, η καθετότητα, αποβαίνει σημαντική για τους κώδικες και ιδιαίτερα για τους γραμμικούς κώδικες.

Θα ξεκινήσουμε με μερικούς γενικούς ορισμούς.

Ορισμός 2.2.1. *Έστω* $\mathbb{F}$ *ένα σώμα,* n *ένας φυσικός αριθμός και* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathbb{F}^n$. *Το* ***εσωτερικό γινόμενο*** *των διανυσμάτων* $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ *ορίζεται να είναι το στοιχείο* $\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n \in \mathbb{F}$

Παράδειγμα 2.2.2. Έστω $\mathbf{x} = (1, 2, 3)$, $\mathbf{y} = (2, 3, 1) \in \mathbb{Z}_5^3$, τότε:

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}\,\mathbf{y}^t = (1, 2, 3) \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} = 1 \cdot 2 + 2 \cdot 3 + 3 \cdot 1 = 1$$

Οι κυριώτερες ιδιότητες του εσωτερικού γινομένου συνοψίζονται στην επόμενη πρόταση.

Πρόταση 2.2.3. *Για κάθε* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{F}^n$ *και κάθε* $\lambda \in \mathbb{F}$ *ισχύει:*

1. $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.
2. $\langle\, (\mathbf{x} + \mathbf{y}), \mathbf{z}\, \rangle = \langle \mathbf{x}, \mathbf{z} \rangle + \langle \mathbf{y}, \mathbf{z} \rangle$.
3. $\langle (\lambda \mathbf{x}), \mathbf{y} \rangle = \langle \mathbf{x}, (\lambda \mathbf{y}) \rangle = \lambda(\langle \mathbf{x}, \mathbf{y} \rangle)$.

Απόδειξη. Άσκηση. ό.έ.δ.

Ορισμοί 2.2.4.

1. *Έστω* $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$. *Τα διανύσματα* $\mathbf{x}, \mathbf{y}$ *λέγονται* ***κάθετα*** *ή* ***ορθογώνια*** *αν* $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle = \mathbf{0}$.

2. *Έστω* S *ένα μη κενό υποσύνολο του* $\mathbb{F}^n$. *Το σύνολο:*

$$S^{\perp} = \{\, \mathbf{x} \in \mathbb{F}^n \mid \langle \mathbf{x}, \mathbf{s} \rangle = 0 \text{ για όλα τα } s \in S \,\}$$

ονομάζεται ***ορθογώνιο συμπλήρωμα*** *του* S.

Παραδείγματα 2.2.5. 1. Έστω $\mathbf{x} = (1, 2, 3), \mathbf{y} = (2, 3, 4) \in \mathbb{Z}_5^3$. Τότε $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, άρα τα $\mathbf{x}$ και $\mathbf{y}$ είναι κάθετα.

2. Αν $\mathbf{x} = (1, 2, 3) \in \mathbb{Z}_7^3$, τότε $\langle \mathbf{x}, \mathbf{x} \rangle = 0$, δηλαδή το $\mathbf{x} = (1, 2, 3)$ είναι κάθετο στον εαυτό του!

3. Έστω $S = \{ (1, 1, \dots, 1) \} \subseteq \mathbb{Z}_p^n$. Τότε το ορθογώνιο συμπλήρωμα του S είναι ίσο με $S^\perp = \{ (a_1, a_2, \dots, a_n) \in \mathbb{Z}_p^n \mid \sum_{i=1}^n a_i = 0 \}$.

   Στην ειδική περίπτωση, όπου $p = 2$, το ορθογώνιο συμπλήρωμα του S αποτελείται από όλες τις λέξεις αρτίου βάρους (γιατί;)

Παρατήρηση. Στο Παράδειγμα 2 παραπάνω, είδαμε ότι υπάρχουν μη μηδενικά διανύσματα τα οποία είναι κάθετα στον εαυτό τους, κάτι που δεν συμβαίνει αν βρισκόμαστε στον χώρο $\mathbb{R}^n$ με τη συνήθη γεωμετρική έννοια της καθετότητας.

Πρόταση 2.2.6. *Το ορθογώνιο συμπλήρωμα $S^\perp$ ενός υποσυνόλου S του διανυσματικού χώρου $\mathbb{F}^n$ είναι διανυσματικός υπόχωρος. Ισχύει δε $S^\perp = (\langle S \rangle)^\perp$, όπου $\langle S \rangle$ παριστά τον υπόχωρο τον παραγόμενο από το υποσύνολο S.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια της Πρότασης 2.2.3 και αφίεται ως άσκηση. ό.έ.δ.

Ορισμός 2.2.7. *Έστω $\mathcal{C} \subseteq \mathbb{F}^n$ ένας κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$. Το οθογώνιο συμπλήρωμα $\mathcal{C}^\perp$ ονομάζεται **δυϊκός** κώδικας του κώδικα $\mathcal{C}$.*

Προφανώς, από την προηγούμενη πρόταση, ο δυϊκός κώδικας ενός κώδικα είναι γραμμικός κώδικας.

Πρόταση 2.2.8. *Έστω $\mathcal{C}_1, \mathcal{C}_2$ δύο κώδικες με $\mathcal{C}_1 \subseteq \mathcal{C}_2$. Τότε ισχύει $\mathcal{C}_2^\perp \subseteq \mathcal{C}_1^\perp$.*

Απόδειξη. Έστω $\mathbf{c} \in \mathcal{C}_2^\perp$. Η (κωδικο)λέξη $\mathbf{c}$ είναι κάθετη προς κάθε στοιχείο του κώδικα $\mathcal{C}_2$, άρα κάθε στοιχείο του $\mathcal{C}_1$ είναι κάθετο προς τη $\mathbf{c}$, αφού $\mathcal{C}_1, \subseteq \mathcal{C}_2$. Δηλαδή η $\mathbf{c} \in \mathcal{C}_1^\perp$. ό.έ.δ.

Έστω $\mathcal{C} = \{\mathbf{c_1}, \mathbf{c_2}, \dots, \mathbf{c_m}\} \subseteq \mathbb{F}^n$ ένας κώδικας. Μπορούμε να περιγράψουμε τα στοιχεία του δυϊκού κώδικα $\mathcal{C}^\perp$ ως εξής: Για $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathcal{C}^\perp$, έχουμε $\langle \mathbf{x}, \mathbf{c_i} \rangle = 0$ για $i = 1, 2, \dots, m$. Επομένως, αν $\mathbf{c_i} = (c_{i1}, c_{i2}, \dots, c_{in})$, $i = 1, 2, \dots, m$, οι προηγούμενες σχέσεις γίνονται:

$$\begin{aligned}
c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n &= 0 \\
c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n &= 0 \\
&\vdots \\
c_{i1}x_1 + c_{i2}x_2 + \cdots + c_{in}x_n &= 0 \\
&\vdots \\
c_{m1}x_1 + c_{m2}x_2 + \cdots + c_{mn}x_n &= 0.
\end{aligned}$$

Δηλαδή τα στοιχεία του δυϊκού κώδικα αποτελούν τη λύση ενός ομογενούς γραμμικού συστήματος.

Έστω ο πίνακας:

$$\mathrm{P} = \begin{pmatrix}
c_{11} & c_{12} & \cdots & c_{1n} \\
c_{21} & c_{22} & \cdots & c_{2n} \\
\vdots & \vdots & \vdots & \vdots \\
c_{i1} & c_{i2} & \cdots & c_{in} \\
\vdots & \vdots & \vdots & \vdots \\
c_{m1} & c_{m2} & \cdots & c_{mn}
\end{pmatrix}.$$

Δηλαδή οι γραμμές του πίνακα P είναι οι (κωδικο)λέξεις του κώδικα $\mathcal{C}$.

Το προηγούμενο σύστημα θα μπορούσε να γραφεί υπό τη μορφή:

$$(x_1, x_2, \cdots, x_n)\mathrm{P}^t = \mathbf{0}.$$

Οι προηγούμενες εξισώσεις ονομάζονται **εξισώσεις ελέγχου ισοτιμίας** και ο πίνακας P ονομάζεται **πίνακας ελέγχου ισοτιμίας** για τον δυϊκό κώδικα $\mathcal{C}^\perp$.

Όπως είναι γνωστόν ο χώρος των λύσεων του προηγουμένου συστήματος έχει διάσταση ίση με $n - r$, όπου r είναι η τάξη $r(\mathrm{P})$ του πίνακα P. Δηλαδή ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι ένας γραμμικός κώδικας διάστασης $n - r$.

Παραδείγματα 2.2.9. 1. Έστω $\mathcal{C}$ ο 5−δικός κώδικας $\{\, 3013,\ 2004,\ 1012 \,\}$.

Ο δυϊκός κώδικας είναι ο $\mathcal{C}^\perp = \{\, \mathbf{x} = x_1x_2x_3x_4 \in \mathbb{Z}_5^4 \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$, όπου

P είναι ο πίνακας ελέγχου ισοτιμίας και έχει ως γραμμές τα στοιχεία του κώδικα $\mathcal{C}$. Δηλαδή τα στοιχεία του $\mathcal{C}^{\perp}$ είναι η λύση του συστήματος:

$$\begin{aligned} c3x_1 + 0x_2 + x_3 + 3x_4 &= 0 \\ 2x_1 + 0x_2 + 0x_3 + 4x_4 &= 0 \\ x_1 + 0x_2 + x_3 + 2x_4 &= 0. \end{aligned}$$

Ο πίνακας ελέγχου ισοτιμίας έχει τάξη ίση με 3 (γιατί;). Επομένως, η διάσταση του δυϊκού κώδικα $\mathcal{C}^{\perp}$ είναι ίση με $4 - 3 = 1$, άρα ο $\mathcal{C}^{\perp}$ αποτελείται από 5^1 στοιχεία. (Θα μπορούσατε να τα υπολογίσετε; Θα μπορούσατε να υπολογίσετε μια βάση του;).

2. Έστω $\mathcal{C}$ ο 2−δικός κώδικας $\{\, 1011,\, 0001,\, 1010 \,\}$. Ο δυϊκός κώδικας είναι ο $\mathcal{C}^{\perp} = \{\, \mathbf{x} =, x_1x_2x_3x_4 \in \mathbb{Z}_2^4 \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$, όπου P είναι ο πίνακας ελέγχου ισοτιμίας και έχει ως γραμμές τα στοιχεία του κώδικα $\mathcal{C}$. Δηλαδή τα στοιχεία του $\mathcal{C}^{\perp}$ είναι η λύση του συστήματος:

$$\begin{aligned} x_1 + 0x_2 + x_3 + x_4 &= 0 \\ 0x_1 + 0x_2 + 0x_3 + x_4 &= 0 \\ x_1 + 0x_2 + x_3 + 0x_4 &= 0. \end{aligned}$$

Ο πίνακας ελέγχου ισοτιμίας έχει τάξη ίση με δύο (γιατί;). Επομένως, η διάσταση του δυϊκού κώδικα $\mathcal{C}^{\perp}$ είναι ίση με $4 - 2 = 2$, άρα ο $\mathcal{C}^{\perp}$ αποτελείται από 2^2 στοιχεία. (Θα μπορούσατε να τα υπολογίσετε; Θα μπορούσατε να υπολογίσετε μια βάση του;).

Στο αμέσως προηγούμενο παράδειγμα οι γραμμές του πίνακα δεν είναι γραμμικώς ανεξάρτητες. Συγκεκριμένα, η δεύτερη γραμμή είναι το άθροισμα της πρώτης και τρίτης γραμμής. Επομένως, για τον υπολογισμό των στοιχείων του δυϊκού κώδικα $\mathcal{C}^{\perp}$ θα μπορούσαμε να απαλείψουμε την δεύτερη γραμμή του αντίστοιχου ομογενούς συστήματος. Δηλαδή ο κώδικας $\mathcal{C}^{\perp}$ έχει και έναν *άλλο* πίνακα ελέγχου ισοτιμίας, τον:

$$\overline{\mathrm{P}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Η έννοια του πίνακα ελέγχου ισοτιμίας (και των εξισώσεων ελέγχου ισοτιμίας) έχει ορισθεί, προς το παρόν, για τον δυϊκό κώδικα $\mathcal{C}^{\perp}$ ενός (τυχαίου) κώδικα $\mathcal{C}$. Στα επόμενα, θα δούμε ότι για **κάθε** γραμμικό κώδικα μπορεί να ορισθεί ένας πίνακας ελέγχου ισοτιμίας και θα διευκρινίσουμε τι σημαίνει ένας κώδικας να έχει πολλούς πίνακες ελέγχου ισοτιμίας.

Ορισμός 2.2.10. *Έστω $\mathcal{C}$ ένας κώδικας μήκους n με στοιχεία από το σώμα $\mathbb{F}$. Αν υπάρχει $s \times n$ πίνακας P με την ιδιότητα $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{F}^n \mid \mathbf{c}\mathrm{P}^t = \mathbf{0} \,\}$, τότε ο πίνακας P θα λέγεται πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.*

Παρατήρηση 2.2.11. Αν υπάρχει πίνακας ισοτιμίας, έστω P, για τον κώδικα $\mathcal{C}$, τότε ο κώδικας είναι γραμμικός. Πράγματι, έστω $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$, τότε $(\mathbf{c}_1 + \mathbf{c}_2)\mathrm{P}^t = \mathbf{c}_1\mathrm{P}^t + \mathbf{c}_2\mathrm{P}^t = \mathbf{0} + \mathbf{0} = \mathbf{0}$. Δηλαδή $\mathbf{c}_1 + \mathbf{c}_2 \in \mathcal{C}$. Επίσης, για $\lambda \in \mathbb{F}$ και $\mathbf{c} \in \mathcal{C}$ έχουμε $(\lambda\mathbf{c})\mathrm{P}^t = \lambda(\mathbf{c}\mathrm{P}^t) = \lambda\mathbf{0} = \mathbf{0}$, επομένως $\lambda\mathbf{c} \in \mathcal{C}$. Άρα, ο κώδικας $\mathcal{C}$ είναι γραμμικός.

Σημείωση: Θα μπορούσαμε να επιχειρηματολογίσουμε και ως εξής: Από τον τρόπο ορισμού του πίνακα ελέγχου ισοτιμίας προκύπτει ότι ο κώδικας είναι ο πυρήνας της γραμμικής απεικόνισης με πεδίο ορισμού τον διανυσματικό χώρο $\mathbb{F}^n$, η οποία ορίζεται από τον πίνακα P^t. Άρα, ο κώδικας $\mathcal{C}$ είναι γραμμικός.

Πρόταση 2.2.12. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και G ένας γεννήτορας πίνακας. Ένας $s \times n$ πίνακας P με στοιχεία από το σώμα $\mathbb{F}$ του κώδικα και τάξη $r(\mathrm{P})$ ίση με $n-k$ είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$, αν και μόνο αν $\mathrm{GP}^t = \mathbf{0}$.*

Απόδειξη. Ως γνωστόν ο κώδικας $\mathcal{C}$ είναι της μορφής:

$$\mathcal{C} = \{\, (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G},\ (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k \,\}.$$

Επομένως, για κάθε $\mathbf{c} \in \mathcal{C}$ υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}$, έτσι ώστε $\mathbf{c} = (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G}$. Υποθέτουμε ότι $G\mathrm{P}^t = \mathbf{0}$, τότε για κάθε $\mathbf{c} \in \mathcal{C}$ έχουμε $\mathbf{c}\mathrm{P}^t = ((\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot \mathrm{G}) \cdot \mathrm{P}^t = (\lambda_1, \lambda_2, \ldots, \lambda_k) \cdot (\mathrm{G} \cdot \mathrm{P}^t) = \mathbf{0}$. Δηλαδή $\mathcal{C} \subseteq \{\, \mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$. Αλλά σύμφωνα με την προηγούμενη παρατήρηση το σύνολο $\{\, \mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$ είναι ο πυρήνας της γραμμικής απεικόνισης με

πεδίο ορισμού τον διανυσματικό χώρο $\mathbb{F}^n$, η οποία ορίζεται από τον πίνακα P^t, επομένως έχει διάσταση ίση με $n - r(\mathrm{P}^t) = n - r(\mathrm{P}) = n - (n-k) = k$. Οπότε από τη σχέση $\mathcal{C} \subseteq \{\, \mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$ έχουμε ότι $\mathcal{C} = \{\, \mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0} \,\}$. Επομένως, σύμφωνα με τον ορισμό του πίνακα ελέγχου ισοτιμίας, ο πίνακας P είναι πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

Αντίστροφα, υποθέτουμε ότι ο πίνακας P είναι πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$. Τότε από τις σχέσεις:

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}^n \mid \mathbf{x}\mathrm{P}^t = \mathbf{0}\} \quad \text{και} \quad \mathcal{C} = \{(\lambda_1, \lambda_2, \dots, \lambda_k) \cdot \mathrm{G}, (\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{F}^k\}$$

έπεται ότι $\mathrm{GP}^t = \mathbf{0}$. ό.έ.δ.

Θεώρημα 2.2.13. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και* G *ένας γεννήτορας πίνακας.*

1. *Ο πίνακας* G *είναι πίνακας ελέγχου ισοτιμίας του δυϊκού γραμμικού κώδικα $\mathcal{C}^\perp$.*
2. *Ο δυϊκός κώδικας $\mathcal{C}^\perp$ έχει διάσταση ίση με $n - k$.*
3. *$\mathcal{C} = (\mathcal{C}^\perp)^\perp$.*
4. *Αν* H *ένας γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{C}^\perp$, τότε ο* H *είναι πίνακας ελέγχου ισοτιμίας του γραμμικού κώδικα $\mathcal{C}$.*

Απόδειξη. 1. Έστω $\mathbf{u} \in \mathcal{C}^\perp$. Τότε για κάθε $\mathbf{c} \in \mathcal{C}$ έχουμε $\langle \mathbf{c}, \mathbf{u} \rangle = \mathbf{c}\mathbf{u}^t = 0$. Από τον ορισμό του γεννήτορα πίνακα έχουμε ότι:

$$\mathcal{C} = \{\, (\lambda_1, \lambda_2, \dots, \lambda_k) \cdot \mathrm{G} \mid (\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{F}^k \,\}.$$

Οπότε από την προηγούμενη σχέση έχουμε $((\lambda_1, \lambda_2, \dots, \lambda_k) \cdot \mathrm{G})\mathbf{u}^t = 0$, για κάθε $(\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{F}^k$, δηλαδή $(\lambda_1, \lambda_2, \dots, \lambda_k) \cdot (\mathrm{G}\mathbf{u}^t) = 0$, για κάθε $(\lambda_1, \lambda_2, \dots, \lambda_k) \in \mathbb{F}^k$. Αυτό σημαίνει ότι $\mathrm{G}\mathbf{u}^t = 0$, δηλαδή $\mathbf{u}\mathrm{G}^t = 0$, το οποίο αποδεικνύει ότι ο πίνακας G είναι πίνακας ελέγχου ισοτιμίας του δυϊκού κώδικα $\mathcal{C}^\perp$.

2. Έχουμε επισημάνει ότι ο δυϊκός κώδικας $\mathcal{C}^\perp$ έχει διάσταση ίση με $n - r$, όπου r είναι η τάξη $r(\mathrm{G})$ του πίνακα ελέγχου ισοτιμίας G. Αλλά

ο πίνακας G, ως γεννήτορας πίνακας του κώδικα $\mathcal{C}$, έχει τάξη ίση με τη διάσταση του $\mathcal{C}$, άρα $r(\mathrm{G}) = k$. Δηλαδή ο δυϊκός κώδικας $\mathcal{C}^\perp$ έχει διάσταση ίση με $n-k$.

3. Από τον ορισμό του δυϊκού κώδικα έχουμε ότι $\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$. Από το 2. έχουμε ότι $\dim(\mathcal{C}^\perp)^\perp = n - \dim \mathcal{C}^\perp = n - (n-k) = k = \dim \mathcal{C}$. Οπότε $\mathcal{C} = (\mathcal{C}^\perp)^\perp$.

4. Από το (1.) έχουμε ότι ο γεννήτορας πίνακας H του δυϊκού κώδικα $\mathcal{C}^\perp$ είναι πίνακας ελέγχου ισοτιμίας του κώδικα $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

ό.έ.δ.

Πόρισμα 2.2.14. *1. Κάθε $s \times n$ πίνακας P με στοιχεία από ένα πεπερασμένο σώμα $\mathbb{F}$ είναι πίνακας ελέγχου ισοτιμίας ενός (μοναδικού) γραμμικού κώδικα $\mathcal{C} \subseteq \mathbb{F}^n$.*

2. Κάθε $k \times n$ πίνακας A με στοιχεία από ένα πεπερασμένο σώμα $\mathbb{F}$ με τις γραμμές του γραμμικά ανεξάρτητες είναι γεννήτορας πίνακας ενός γραμμικού κώδικα $\mathcal{C} \subseteq \mathbb{F}^n$ και πίνακας ελέγχου ισοτιμίας του δυϊκού γραμμικού κώδικα $\mathcal{C}^\perp \subseteq \mathbb{F}^n$.

3. Κάθε γραμμικός κώδικας έχει (τουλάχιστον) ένα πίνακα ελέγχου ισοτιμίας.

Απόδειξη. 1. Έστω $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{F}^n \mid \mathbf{c}\mathrm{P}^t = \mathbf{0} \,\}$ το σύνολο λύσεων του ομογενούς συστήματος $(x_1, x_2, \cdots, x_n)\mathrm{P}^t = \mathbf{0}$. Το σύνολο αυτό αποτελεί διανυσματικό υπόχωρο του $\mathbb{F}^n$, άρα ο $\mathcal{C}$ είναι γραμμικός.

2. Άμεσο από τα προηγούμενα.

3. Άμεσο από το (4.) του προηγουμένου θεωρήματος.

ό.έ.δ.

Παρατηρήσεις 2.2.15. 1. Στο (1.) του προηγουμένου πορίσματος ο κώδικας που ορίζεται είναι μοναδικός, ως ο χώρος των λύσεων ένος ομογενούς συστήματος. Επίσης, δεν αναφέρεται τίποτε για την τάξη $r(\mathrm{P})$ του πίνακα. Απλώς να έχουμε υπ'οψη ότι η διάσταση του κώδικα $\mathcal{C}$ είναι

ίση με $n-r(\mathrm{P})$, (άρα στην ακραία περίπτωση, όπου $r(\mathrm{P}) = n$, ο πίνακας P είναι πίνακας ελέγχου ισοτιμίας του μηδενικού κώδικα).

2. Στο (3.) του προηγουμένου πορίσματος αναφέρουμε ότι ένας κώδικας έχει τουλάχιστον ένα πίνακα ελέγχου ισοτιμίας. Επίσης, στο τελευταίο παράδειγμα πριν τον ορισμο 2.2.10 είχαμε επισημάνει ότι ένας κώδικας μπορεί να έχει περισσότερους του ενός πίνακες ελέγχου ισοτιμίας. Πράγματι, για έναν γραμμικό κώδικα μήκους n (δηλαδή έναν διανυσματικό υπόχωρο του $\mathbb{F}^n$) μπορούμε να κατασκευάσουμε πολλά ομογενή γραμμικά συστήματα τα οποία να έχουν ως χώρο λύσεων τον δοθέντα κώδικα (γιατί;).

3. Προσοχή! Ένας γεννήτορας πίνακας είναι πάντα ένας πίνακας ισοτιμίας ενός (του δυϊκού) κώδικα. Ένας πίνακας ελέγχου ισοτιμίας δεν είναι κατ' ανάγκην ένας γεννήτορας πίνακας ενός κώδικα[3].

Παραδείγματα 2.2.16. 1. Θεωρούμε τον πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

με στοιχεία στο $\mathbb{Z}_2$. Ο G είναι γεννήτορας πίνακας του γραμμικού κώδικα $\mathcal{C} = \{00000, 11100, 00011, 11111\}$ (γιατί;) και πίνακας ελέγχου ισοτιμίας για τον δυϊκό κώδικα:

$$\begin{aligned} \mathcal{C}^{\perp} &= \{\mathbf{x} = x_1x_2x_3x_4x_5 \in \mathbb{Z}_2^5 \mid \mathbf{x}\mathrm{G}^t = \mathbf{0}\} \\ &= \{00000, 00011, 11000, 11011, 01100, 01111, 10100, 10111\}. \end{aligned}$$

Ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

είναι γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{C}^{\perp}$ (γιατί;) και πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

[3] Για τον λόγο αυτόν, πολλοί συγγραφείς, εξ ορισμού, για έναν $[n, k, d]$ γραμμικό κώδικα $\mathcal{C}$ απαιτούν ένας πίνακας ελέγχου ισοτιμίας να έχει $n-k$ το πλήθος γραμμές (όση είναι η τάξη του).

2. Έστω:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

ο πίνακας του προηγουμένου παραδείγματος, αλλά τώρα τα στοιχεία του να θεωρούνται ως στοιχεία του $\mathbb{Z}_3$. Ο G είναι γεννήτορας πίνακας του γραμμικού κώδικα:

$$\mathcal{C} = \{\, 00000,\ 11100,\ 00011,\ 11111,\ 22200,\ 00022,\ 11122,\ 22211,\ 22222 \,\}$$

(γιατί;) και πίνακας ελέγχου ισοτιμίας για το δυϊκό κώδικα:

$$\mathcal{C}^{\perp} = \{\, \mathbf{x} = x_1x_2x_3x_4x_5 \in \mathbb{Z}_3^5 \mid \mathbf{x}\mathrm{G}^t = \mathbf{0} \,\}.$$

Ο δυϊκός κώδικας έχει 27 το πλήθος στοιχεία (μπορείτε να τα υπολογίσετε;).

Ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 0 \end{pmatrix}$$

είναι γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{C}^{\perp}$ (γιατί;) και πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

Στα προηγούμενα παραδείγματα για να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας ενός γραμμικού κώδικα υπολογίζαμε έναν γεννήτορα πίνακα του αντίστοιχου δυϊκού κώδικα. Θα κλείσουμε την παράγραφο με μια αναφορά σε γραμμικούς κώδικες, οι οποίοι έχουν γεννήτορα πίνακα σε ανηγμένη κλιμακωτή μορφή και θα εξετάσουμε τους αντίστοιχους πίνακες ελέγχου ισοτιμίας.

Θεώρημα 2.2.17. *Ένας γραμμικός κώδικας $\mathcal{C}$ μήκους n έχει ως γεννήτορα πίνακα έναν πίνακα της μορφής $\mathrm{G} = [\mathrm{I}_k \,\mathrm{B}]$, αν και μόνο αν ο πίνακας $\mathrm{P} = [-\mathrm{B}^t\mathrm{I}_{n-k}]$ είναι ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.*

Απόδειξη. Ας υπολογίσουμε το γινόμενο της $i-$γραμμής του πίνακα G με την $j-$στήλη του πίνακα P^t (θεωρούμενες ως πίνακες).

$$(0\cdots 1\cdots 0\, b_{i1}\cdots b_{i,n-k})\cdot\begin{pmatrix} -b_{1j}\\ \vdots\\ -b_{kj}\\ 0\\ \vdots\\ 1\\ \vdots\\ 0\end{pmatrix} = -b_{ij}+b_{ij}=0.$$

Επομένως έχουμε ότι $\mathrm{G}\cdot\mathrm{P}^t = \mathbf{0}$. Οπότε από την πρόταση 2.2.12 έπεται το αποτέλεσμα, καθότι η τάξη του πίνακα $\mathrm{P} = [-\mathrm{B}^t\,\mathrm{I}_{n-k}]$ είναι ίση με $n-k$. ό.έ.δ.

Έχουμε δει (Πόρισμα 2.1.12) ότι κάθε γραμμικός κώδικας $\mathcal{C}$ είναι ισοδύναμος με έναν γραμμικό κώδικα $\mathcal{D}$, ο οποίος έχει έναν γεννήτορα πίνακα της μορφής $\mathrm{G} = [\mathrm{I}_k\,\mathrm{B}]$. Στην περίπτωση αυτή, ο υπολογισμός του πίνακα ελέγχου ισοτιμίας $\mathrm{P} = [-\mathrm{B}^t\,\mathrm{I}_{n-k}]$ είναι πλέον άμεσος.

Παράδειγμα 2.2.18. Έστω ο $3-$δικός γραμμικός κώδικας:

$$\mathcal{C} = \{\,00000,\ 10022,\ 01022,\ 11011,\ 21000,\ 12000,\ 20011,\ 02011,\ 22022\,\}$$

(γιατί είναι γραμμικός;). Ένας γεννήτορας πίνακας είναι ο πίνακας:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 2 & 2\\ 0 & 1 & 0 & 2 & 2\end{pmatrix}$$

(γιατί ο G είναι γεννήτορας πίνακας;). Οπότε ο πίνακας:

$$\mathrm{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0\\ 1 & 1 & 0 & 1 & 0\\ 1 & 1 & 0 & 0 & 1\end{pmatrix}$$

είναι πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$.

2.2.1 Αυτοδυϊκοί κώδικες

Όπως είναι γνωστό από τη Γραμμική Άλγεβρα, όταν έχουμε έναν διανυσματικό χώρο επί του σώματος των πραγματικών αριθμών, τότε δεν υπάρχουν μη μηδενικά διανύσματα τα οποία να είναι κάθετα (ως προς το γνωστό εσωτερικό γινόμενο) προς τον εαυτό τους.

Στην περίπτωση όμως που έχουμε διανυσματικούς χώρους με συντελεστές από ένα πεπερασμένο σώμα τα πράγματα είναι διαφορετικά. Στο Παράδειγμα 2.2.18 παρατηρούμε ότι η (κωδικο)λέξη 10022 είναι κάθετη στον εαυτό της, όπως είχαμε επισημάνει κάτι ανάλογο και στο Παράδειγμα 2.2.5(2).

Εδώ θα ασχοληθούμε με γραμμικούς κώδικες στους οποίους κάθε στοιχείο είναι κάθετο προς όλα τα στοιχεία του κώδικα και, επιπλέον, αν μια λέξη είναι κάθετη σε κάθε (κωδικο)λέξη, τότε αυτή η λέξη είναι αναγκαστικά στοιχείο του κώδικα.

Ορισμός 2.2.19. *Ένας γραμμικός κώδικας $\mathcal{C}$ λέγεται αυτοδυϊκός αν ισχύει $\mathcal{C} = \mathcal{C}^{\perp}$.*

Παράδειγμα 2.2.20. Προφανώς (γιατί;) ο δυαδικός γραμμικός κώδικας:

$$\mathcal{C} = \{\, 0000,\, 1100,\, 0011,\, 1111 \,\}$$

είναι αυτοδυϊκός.

Οι κυριώτερες ιδιότητες ενός αυτοδυϊκού κώδικα συνοψίζονται στο επόμενο θεώρημα.

Θεώρημα 2.2.21. *1. Έστω $\mathcal{C}$ ένας αυτοδυϊκός γραμμικός κώδικας. Τότε για κάθε δύο γεννήτορες πίνακες G και D του $\mathcal{C}$ ισχύει $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$.*

2. Ένας αυτοδυϊκός κώδικας $\mathcal{C}$ έχει άρτιο μήκος $n = 2k$ και διάσταση ίση με k.

Απόδειξη. 1. Ως γνωστόν, οι γραμμές ενός γεννήτορα πίνακα ένος κώδικα αποτελούνται από τα διανύσματα μιας βάσης του κώδικα. Έστω $\mathrm{B} = \{\, \mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}, \,\}$ και $\Delta = \{\, \mathbf{d_1}, \mathbf{d_2}, \ldots, \mathbf{d_k}, \,\}$ δύο βάσεις του κώδικα

$\mathcal{C}$, έτσι ώστε οι αντίστοιχοι γεννήτορες πίνακες να είναι:

$$\mathrm{G} = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \\ \vdots \\ \mathbf{b_k} \end{pmatrix} \quad \text{και} \quad \mathrm{D} = \begin{pmatrix} \mathbf{d_1} \\ \mathbf{d_2} \\ \vdots \\ \mathbf{d_k} \end{pmatrix}.$$

Έχουμε υποθέσει ότι ο κώδικας είναι αυτοδυϊκός. Επομένως για:

$$\mathbf{b_i} = (b_{i1}, b_{i2}, \dots, b_{in}) \in \mathrm{B} \quad \text{και} \quad \mathbf{d_j} = (d_{j1}, d_{j2}, \dots, d_{jn}) \in \Delta$$

έχουμε $\langle \mathbf{b_i}, \mathbf{d_j} \rangle = b_{i1}d_{j1} + b_{i2}d_{j2} + \cdots + b_{in}d_{jn} = 0$. Αυτό ισχύει για όλα τα $i, j = 1, 2, \dots, n$. Δηλαδή $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$.

2. Ως γνωστόν, για τον δυϊκό κώδικα έχουμε $\dim(\mathcal{C}^\perp) = n - \dim(\mathcal{C})$, όπου n είναι το μήκος του κώδικα. Οπότε το αποτέλεσμα είναι άμεσο.

ό.έ.δ.

Παρατήρηση 2.2.22. Το αντίστροφο του (1.) του προηγουμένου θεωρήματος δεν ισχύει. Για παράδειγμα, ο δυαδικός κώδικας $\mathcal{C} = \{0000, 1100\}$ είναι γραμμικός, έχει διάσταση 1 και ο (μοναδικός) γεννήτορας πίνακας είναι ο πίνακας γραμμή $\mathrm{G} = (1\,1\,0\,0)$. Προφανώς ισχύει $\mathrm{G}\mathrm{G}^\perp = 0$, αλλά ο κώδικας δεν είναι αυτοδυϊκός, αφού $\langle 1100, 0011 \rangle = 0$ και $0011 \notin \mathcal{C}$.

Αν, επιπλέον, υποθέσουμε ότι ο κώδικας $\mathcal{C}$ έχει άρτιο μήκος $n = 2k$ και διάσταση ίση με k, τότε ισχύει το αντίστροφο.
Πράγματι, υποθέτουμε ότι $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$. Έστω $\mathbf{c}, \mathbf{d} \in \mathcal{C}$, εκφράζουμε το $\mathbf{c}$ ως γραμμικό συνδυασμό των στοιχείων της βάσης B και το $\mathbf{d}$ ως γραμμικό συνδυασμό των στοιχείων της βάσης Δ, δηλαδή υπάρχουν $\lambda_1, \lambda_2, \dots, \lambda_k \in \mathbb{F}$, έτσι ώστε $\mathbf{c} = \lambda_1\mathbf{b_1} + \lambda_2\mathbf{b_2} + \cdots + \lambda_k\mathbf{b_k}$ και $\mu_1, \mu_2, \dots, \mu_k \in \mathbb{F}$, έτσι ώστε $\mathbf{d} = \mu_1\mathbf{d_1} + \mu_2\mathbf{d_2} + \cdots + \mu_k\mathbf{d_k}$. Τότε από τις ιδιότητες που αναφέρονται στην Πρόταση 2.2.3 και από την υπόθεση ότι $\mathrm{G} \cdot \mathrm{D}^t = \mathbf{0}$ εύκολα έπεται ότι $\langle \mathbf{c}, \mathbf{d} \rangle = 0$. Δηλαδή $\mathcal{C} \subseteq \mathcal{C}^\perp$, επειδή όμως $\dim(\mathcal{C}) = k = n - k = \dim(\mathcal{C}^\perp)$, το αποτέλεσμα έπεται.

Η επόμενη πρόταση μας δίνει μια ικανή συνθήκη για την ύπαρξη αυτοδυϊκών κωδίκων.

Πρόταση 2.2.23. *Έστω p πρώτος αριθμός της μορφής $p = 4r+1$. Τότε για κάθε άρτιο θετικό ακέραιο $n = 2k$ υπάρχει αυτοδυϊκός κώδικας επί του $\mathbb{Z}_p$ με μήκος n.*

Απόδειξη. Επειδή ο p είναι της μορφής $p = 4r+1$, υπάρχουν θετικοί ακέραιοι a και b, έτσι ώστε $p = a^2 + b^2$. Κατασκευάζουμε τις λέξεις μήκους n $\mathbf{e}_1 = ab\cdots o$, $\mathbf{e}_2 = 00ab\cdots o$, ... , $\mathbf{e}_k = 00\cdots ab$. Είναι εύκολο να ελέγξουμε ότι τα $\mathbf{e}_i$ είναι γραμμικώς ανεξάρτητα και ότι ο κώδικας που παράγουν είναι αυτοδυϊκός. ό.έ.δ.

Παρατηρήσεις 2.2.24.

1. Στην προηγούμενη πρόταση ισχυριστήκαμε ότι για τον $p = 4r + 1$ υπάρχουν θετικοί ακέραιοι a και b, έτσι ώστε $p = a^2 + b^2$. Υπάρχει το εξής θεώρημα στη Θεωρία Αριθμών.

   Ένας περιττός πρώτος p μπορεί να γραφεί ως άθροισμα δύο τετραγώνων ($p = a^2 + b^2$), αν και μόνο αν είναι της μορφής $p = 4r + 1$. Μάλιστα δε τα a και b είναι μοναδικά.

2. Υπάρχει και ένα άλλο θεώρημα στη Θεωρία Αριθμών.

   Ένας περιττός πρώτος p μπορεί να γραφεί ως άθροισμα τεσσάρων τετραγώνων[4].

   Οπότε μπορούμε να αποδείξουμε ότι αν p είναι ένας πρώτος της μορφής $p = 4r + 3$ και ο n είναι ένας θετικός ακέραιος της μορφής $n = 4m$, τότε υπάρχει αυτοδυϊκός κώδικας επί του $\mathbb{Z}_p$ με μήκος ίσον με n.

2.2.2 Υπολογισμός της ελάχιστης απόστασης σε έναν γραμμικό κώδικα

Πρόταση 2.2.25. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας με πίνακα ελέγχου ισοτιμίας* P*. Η ελάχιστη απόσταση d είναι ίση με τον μικρότερο αριθμό γραμμικών εξαρτημένων στηλών του* P*, (δηλαδή υπάρχουν d το πλήθος γραμμικά εξαρτημένες στήλες του* P *και κάθε $d-1$ το πλήθος στήλες του είναι γραμμικά ανεξάτητες).*

[4] Ανατρέξτε σε ένα εγχειρίδιο Θεωρίας Αριθμών για αποδείξεις αυτών των θεωρημάτων, για παράδειγμα στο Niven, I. and Zuckerman, H.S. and Montgomery, H.L. [1991].

Απόδειξη. Έστω $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_n}$ οι στήλες του πίνακα P. Υποθέτουμε ότι από αυτές w το πλήθος είναι γραμμικά εξαρτημένες με το w το ελάχιστο δυνατόν. Τότε υπάρχουν συντελεστές $c_1, c_2, \dots, c_n$ από το αλφάβητο $\mathbb{F}$ εκ των οποίων οι w το πλήθος είναι διάφοροι του μηδενός και οι υπόλοιποι είναι μηδέν, έτσι ώστε $\mathbf{c_1 p_1} + c_2\mathbf{p_2} + \cdots + c_n\mathbf{p_n} = \mathbf{0}$.

Πράγματι, αν υποθέσουμε (άνευ βλάβης) ότι οι πρώτες $\mathbf{p_1}, \mathbf{p_2}, \dots, \mathbf{p_w}$ στήλες είναι γραμμικά εξαρτημένες και δεν υπάρχει γνήσιο υποσύνολό τους που να είναι γραμμικά εξαρτημένο, τότε σε κάθε γραμμικό συνδυασμό τους $\lambda_1\mathbf{p_1} + \lambda_2\mathbf{p_2} + \cdots + \lambda_w\mathbf{p_w} = \mathbf{0}$ όλοι οι συντελεστές πρέπει να είναι διάφοροι του μηδενός. Διαφορετικά, αν ένας ήταν μηδέν, τότε θα υπήρχαν λιγότερα από w το πλήθος γραμμικά εξαρτημενες στήλες (γιατί;).

Επομένως, βλέπουμε ότι $(c_1, c_2, \dots, c_n)\cdot \mathrm{P}^t = \mathbf{0}$. Η τελευταία σχέση ισοδυναμεί με το ότι η λέξη $\mathbf{c} = c_1\, c_2 \dots c_n$ ανήκει στον κώδικα $\mathcal{C}$. Δηλαδή έχουμε μια λέξη βάρους w, η οποία ανήκει στον κώδικα, οπότε από το Θεώρημα 2.1.3 έχουμε ότι $d \leq w$. Επίσης, αν $\mathbf{c}$ είναι μια (κωδικο)λέξη με βάρος ίσο με την ελάχιστη απόσταση του κώδικα, τότε για τον πίνακα P έχουμε $\mathbf{c}\mathrm{P}^t = \mathbf{0}$. Άρα d το πλήθος στήλες του πίνακα, που αντιστοιχούν στα μη μηδενικά στοιχειά της $\mathbf{c}$, είναι γραμμικά εξαρτημένες. Οπότε $w \leq d$ και το αποτέλεσμα έπεται. ό.έ.δ.

Παράδειγμα 2.2.26. Θεωρούμε τον γραμμικό κώδικα $\mathcal{D}$ επί του $\mathbb{Z}_{11}$ με πίνακα ελέγχου ισοτιμίας τον:

$$\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

Ο κώδικας αυτός είναι ένας $[10, 8]$ κώδικας και θέλουμε να υπολογίσουμε την ελάχιστη απόστασή του. Επειδή σε κάθε στήλη του πίνακα το πρώτο στοιχείο είναι 1, προφανώς ανά δύο οι στήλες είναι γραμμικά ανεξάρτητες (γιατί;). Αλλά οι τρεις πρώτες στήλες είναι γραμμικά εξαρτημένες, καθότι έχουμε $\binom{1}{3} = 10\binom{1}{1} + 2\binom{1}{2}$ (οι πράξεις γίνονται στο $\mathbb{Z}_{11}$). Επομένως, από την προηγούμενη πρόταση έχουμε ότι η ελάχιστη απόσταση του κώδικα $\mathcal{D}$ είναι ίση με τρία.

Παρατήρηση 2.2.27. Στη σελίδα 48 είχαμε ασχοληθεί με τον κώδικα $\mathcal{C} = \{\mathbf{c} = x_1x_2\cdots x_{10} \in \mathbb{Z}_{11}^{10} \mid x_{10} = x_1 + 2x_2 + 3x_3 + \cdots + 9x_9\}$ και είχαμε επισημάνει ότι ο $\mathcal{C}$ είναι ένας διανυσματικός χώρος επί του σώματος $\mathbb{Z}_{11}$ με διάσταση 9 και ελάχιστη απόσταση ίση με 2. Δεν είναι δύσκολο να δούμε ότι ο κώδικας αυτός έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα $\mathrm{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$ και ότι ο προηγούμενος κώδικας $\mathcal{D}$ προέρχεται από σμίκρυνση του κώδικα $\mathcal{C}$, αφού ο πίνακας ελέγχου ισοτιμίας του $\mathcal{D}$ προέρχεται από τον πίνακα ελέγχου ισοτιμίας του $\mathcal{C}$ με την επισύναψη μιας επιπλέον γραμμής, η οποία δεν είναι πολλαπλάσιο της ήδη υπάρχουσας γραμμής.

Επίσης, είχαμε δει ότι ο κώδικας **ISBN** προέρχεται από σμίκρυνση του κώδικα $\mathcal{C}$. Εδώ είναι ευκαιρία να επισημάνουμε πάλι ότι ο κώδικας **ISBN δεν** είναι γραμμικός. Πράγματι, το διανύσμα $\mathbf{a} = 5\,5\,5\,5\,1\,1\,1\,1\,1\,8$ είναι μια (κωδικο)λέξη του κώδικα **ISBN**, αλλά το $\mathbf{a} + \mathbf{a} = X\,X\,X\,X\,2\,2\,2\,2\,2\,5$ δεν ανήκει στον κώδικα **ISBN**.

Στην παράγραφο 1.5.2 είχαμε ασχοληθεί με το κάτω φράγμα Gilbert-Varshamov. Εδώ θα δούμε ότι το φράγμα αυτό μπορεί να βελτιωθεί αν θεωρήσουμε γραμμικούς κώδικες.

Πρόταση 2.2.28. ***(Κάτω φράγμα των Gilbert-Varshamov για γραμμικούς κώδικες).***

Υπάρχει ένας $[n, k]$ γραμμικός κώδικας με ελάχιστη απόσταση τουλάχιστον d, επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία, αρκεί να ισχύει:

$$q^k < q^n \Big/ \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i \,.$$

Επομένως, αν k είναι ο μεγαλύτερος ακέραιος που ικανοποιεί την παραπάνω ανισότητα, τότε $A_q(n, d) \geq q^k$.

Απόδειξη. Αν μπορέσουμε να κατασκευάσουμε έναν $(n-k) \times n$ πίνακα H με στοιχεία από το σώμα $\mathbb{F}$, έτσι ώστε κάθε σύνολο με $d-1$ το πλήθος από τις στήλες του να είναι γραμμικά ανεξάρτητο, τότε υπάρχει γραμμικός κώδικας με πίνακα ελέγχου ισοτιμίας τον πίνακα αυτό (Πόρισμα 2.2.14). Σύμφωνα με

την προηγούμενη πρόταση η ελάχιστη απόσταση αυτού του κώδικα θα είναι τουλάχιστον ίση με d και θα έχουμε τελειώσει.

Ως πρώτη στήλη μπορούμε να επιλέξουμε οποιαδήποτε μη μηδενική $(n-k)-$άδα. Ως δεύτερη στήλη επιλέγουμε οποιαδήποτε $(n-k)-$άδα αρκεί να μην είναι πολλαπλάσιο της πρώτης στήλης. Ως τρίτη στήλη επιλέγουμε οποιαδήποτε $(n-k)-$άδα αρκεί να μην είναι γραμμικός συνδυασμός των δύο προηγουμένων. Γενικά, σκοπός μας είναι να επιλέξουμε την i στήλη, έτσι ώστε να μην είναι γραμμικός συνδυασμός οποιωνδήποτε $d-2$ (ή λιγότερων) το πλήθος στηλών από τις $i-1$ το πλήθος στήλες που έχουν ήδη επιλεγεί. Δηλαδή αν έχουμε επιλέξει $i-1$ το πλήθος στήλες και πάρουμε τους γραμμικούς υπόχωρους του $\mathbb{F}^{n-k}$ διάστασης μικρότερης ή ίσης $d-2$ που παράγονται από στήλες που έχουν ήδη επιλεγεί, η $i-$οστή στήλη δεν πρέπει να βρίσκεται σε κανέναν από αυτούς τους υπόχωρους.

Έστω j $(j \leq d-2)$ το πλήθος στήλες από τις $i-1$ το πλήθος που έχουμε επιλέξει. Ας υπολογίσουμε το πλήθος των γραμμικών συνδυασμών (με μη μηδενικούς συντελεστές) που μπορούμε να σχηματίσουμε με αυτές τις στήλες. Υπάρχουν $(q-1)^j$ επιλογές μη μηδενικών συντελεστών, για κάθε μια από αυτές τις επιλογές έχουμε και έναν γραμμικό συνδυασμό. Τώρα τις j το πλήθος στήλες μπορούμε να τις επιλέξουμε με $\binom{i-1}{j}$ το πλήθος τρόπους. Άρα, τελικά, έχουμε $\binom{i-1}{j}(q-1)^j$ το πλήθος γραμμικούς συνδυασμούς των j το πλήθος στηλών. Αθροίζοντας ως προς j έχουμε ότι το πλήθος των γραμμικών συνδυασμών από $d-2$ ή λιγότερες το πλήθος στήλες είναι ίσο με $N_i = \sum_{j=1}^{d-2} \binom{i-1}{j}(q-1)^j$.

Επομένως, η i στήλη μπορεί να επιλεγεί από τα υπόλοιπα (μη μηδενικά) στοιχεία του διανυσματικού χώρου $\mathbb{F}^{n-k}$. Τα μη μηδενικά στοιχεία του $\mathbb{F}^{n-k}$ είναι $q^{n-k}-1$. Επομένως, για να μπορούμε να επιλέξουμε την i στήλη πρέπει να ισχύει $N_i < q^{n-k}-1$. Τελικά, για να μπορούμε να επιλέξουμε και την $n-$οστή στήλη πρέπει και αρκεί να ισχύει $N_n < q^{n-k}-1$, δηλαδή πρέπει και αρκεί να ισχύει $\sum_{j=1}^{d-2} \binom{n-1}{j}(q-1)^j < q^{n-k}-1$ ή ισοδύναμα $\sum_{j=0}^{d-2} \binom{n-1}{j}(q-1)^j < q^{n-k}$. Η τελευταία σχέση όμως ισχύει από την υπόθεση, επομένως έχουμε αποδείξει το ζητούμενο. ό.έ.δ.

Παρατήρηση 2.2.29. Αν θελήσουμε να συγκρίνουμε το κάτω φράγμα Gilbert-Varshamov στη γενική του μορφή (Θεώρημα 1.5.17) με το κάτω φράγμα

Gilbert-Varshamov για γραμμικούς κώδικες που επιτυγχάνεται στην προηγούμενη πρόταση, από το επόμενο παράδειγμα θα δούμε ότι το φράγμα Gilbert-Varshamov για γραμμικούς κώδικες είναι πολύ καλύτερο. Θα πρέπει όμως να σημειωθεί ότι το πρώτο φράγμα αναφέρεται γενικά σε όλους τους κώδικες, ενώ το δεύτερο αναφέρεται σε γραμμικούς κώδικες.

Παράδειγμα. Από το Θεώρημα 1.5.17 έχουμε ότι $A_2(5,\,3) \geq \dfrac{2^5}{1+\binom{5}{1}+\binom{5}{2}} = 2$.

Από την Πρόταση 2.2.28 έπεται ότι υπάρχει ένας δυαδικός $[5,\,k,\,3]$ γραμμικός κώδικας αρκεί να ισχύει $2^k < \dfrac{2^5}{1+\binom{4}{1}} = \dfrac{32}{5}$. Οπότε για $k = 2$ έχουμε ότι υπάρχει ένας δυαδικός $[5,\,2,\,3]$ γραμμικός κώδικας, επομένως $A_2(5,\,3) \geq 4$.

Αν ανατρέξουμε στον πίνακα, 1.2 θα δούμε ότι $A_2(5,\,3) = 4$, δηλαδή το $A_2(5,\,3)$ λαμβάνει την κατώτερη (επιτρεπόμενη) τιμή.

2.2.3 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Έστω $A,\ B$ δύο υποσύνολα του $\mathbb{Z}_p^n$, με την ιδιότητα κάθε στοιχείο του A να είναι κάθετο σε κάθε στοιχείο του B, δηλαδή $< \mathbf{a},\,\mathbf{b} > = 0$ για κάθε $\mathbf{a} \in A,\ \mathbf{b} \in B$. Υποθέτουμε ότι $\mid A \mid = p^k$ και $\mid B \mid \geq p^{n-k-1} + 1$. Δείξτε ότι το A είναι ένας γραμμικός κώδικας. Υπολογίστε τον δυϊκό του.

3. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας μήκους n. Επιλέγουμε και σταθεροποιούμε ένα $\mathbf{a} \in \mathbb{Z}_2^n$, το οποίο δεν ανήκει στον δυϊκό κώδικα $\mathcal{C}^\perp$.

   Δείξτε ότι το πλήθος των στοιχείων $\mathbf{c} \in \mathcal{C}$, για τα οποία ισχύει $\langle\, \mathbf{c},\, \mathbf{a} \,\rangle = 0$, ισούται με το πλήθος των στοιχείων $\mathbf{d} \in \mathcal{C}$, για τα οποία ισχύει $\langle\, \mathbf{d},\, \mathbf{a} \,\rangle = 1$.

4. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας για τον n-επαναληπτικό κώδικα $\mathcal{R}_q(n)$. Κατόπιν, να περιγράψετε τον δυϊκό κώδικα $(\mathcal{R}_q(n))^\perp$ και να υπολογίσετε τις παραμέτρους του.

5. Δίνεται ο δυαδικός κώδικας $\mathcal{C}$ με πίνακα ελέγχου ισοτιμίας:

$$\mathrm{P} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

και ο τριαδικός κώδικας $\mathcal{D}$ με γεννήτορα πίνακα τον ίδιο πίνακα P. Να υπολογίσετε την ελάχιστη απόσταση του $\mathcal{C}$ και του $\mathcal{D}$.

6. Δείξτε ότι σε έναν αυτοδυϊκό $[n, k, d]$ κώδικα $\mathcal{C}$ για την ελάχιστη απόστασή του ισχύει $d = k + 1$.

7. Δείξτε ότι σε έναν δυαδικό αυτοδυϊκό κώδικα $\mathcal{C}$ όλες οι (κωδικο)λέξεις έχουν άρτιο βάρος. Επιπλέον, δείξτε ότι η λέξη $11\cdots 1 \in \mathcal{C}$. Ισχύει το αντίστροφο;

8. Δείξτε ότι για κάθε άρτιο θετικό ακέραιο n υπάρχει ένας δυαδικός αυτοδυϊκός κώδικας μήκους n.

9. Να κατασκευάσετε έναν δυαδικό αυτοδυϊκό κώδικα μήκους 8. Να υπολογίσετε την ελάχιστη απόστασή του.

10. Δείξτε ότι το βάρος κάθε (κωδικο)λέξης σε έναν τριαδικό αυτοδυϊκό κώδικα είναι πολλαπλάσιο του τρία.

11. Δείξτε ότι οι λέξεις 1201 και 1012 παράγουν έναν τριαδικό αυτοδυϊκό κώδικα. Βρείτε όλα τα στοιχεία του.

12. Υπάρχει αυτοδυϊκός κώδικας μήκους 6 επί του σώματος $\mathbb{Z}_7$;

13. Ένας γραμμικός κώδικας $\mathcal{C}$ λέγεται **αυτο-ορθογώνιος**, αν ισχύει $\mathcal{C} \subseteq \mathcal{C}^{\perp}$.

    Δώστε ένα παράδειγμα ενός αυτο-ορθογώνιου κώδικα που δεν είναι αυτοδυϊκός.

    Έστω G ο γεννήτορας πίνακας ενός $p-$αδικού κώδικα $\mathcal{C}$ με $p = 2$ ή 3. Δείξτε ότι ο $\mathcal{C}$ είναι αυτο-ορθογώνιος, αν και μόνο αν ανά δύο οι γραμμές του G είναι κάθετες και το βάρος κάθε γραμμής είναι πολλαπλάσιο του p.

Στην περίπτωση ενός δυαδικού αυτο-ορθογώνιου κώδικα να δείξετε ότι κάθε (κωδικο)λέξη είναι αρτίου βάρους και ότι η λέξη $1\,1\cdots 1$ ανήκει στον δυϊκό κώδικα.

14. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας.

    i) Αν ο $\mathcal{C}$ είναι αυτο-ορθογώνιος και έχει έναν γεννήτορα πίνακα, όπου κάθε γραμμή του έχει βάρος πολλαπλάσιο του τέσσερα, τότε κάθε (κωδικο)λέξη έχει βάρος πολλαπλάσιο του τέσσερα.

    ii) Αν κάθε (κωδικο)λέξη έχει βάρος πολλαπλάσιο του τέσσερα, τότε ο κώδικας είναι αυτο-ορθογώνιος.

15. Έστω $\mathcal{C}_1$, $\mathcal{C}_2$ δύο (μη μηδενικοί) γραμμικοί κώδικες επί του σώματος $\mathbb{F}$ με q το πλήθος στοιχεία με αντίστοιχα μήκη n_1 και n_2. Έστω:

$$\mathcal{C}_1 \mid \mathcal{C}_2 = \{\, \mathbf{c}_1 \mid \mathbf{c}_2 \,:\, \mathbf{c}_1 \in \mathcal{C}_1 \text{ και } \mathbf{c}_2 \in \mathcal{C}_2 \,\}$$

    ο κώδικας, ο οποίος προκύπτει από την παράθεση των δύο κωδίκων (ιδέ Άσκηση 2.1.2$_{14}$).

    Αν οι πίνακες $\mathrm{H}_1, \mathrm{H}_2$ είναι πίνακες ελέγχου ισοτιμίας των $\mathcal{C}_1$ και $\mathcal{C}_2$ αντίστοιχα. Δείξτε ότι ο πίνακας:

$$\begin{pmatrix} \mathrm{H}_1 & \mathbf{0} \\ \mathbf{0} & \mathrm{H}_2 \end{pmatrix}$$

    είναι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}_1 \mid \mathcal{C}_2$.

16. Έστω $\mathcal{C}$, $\mathcal{D}$ γραμμικοί κώδικες του ιδίου μήκους με πίνακες ελέγχου ισοτιμίας P και Q αντίστοιχα. Δείξτε ότι ο κώδικας που προκύπτει από μια $(\mathbf{u},\, \mathbf{u}+\mathbf{v})$-κατασκευή έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα:

$$\begin{pmatrix} \mathrm{P} & \mathbf{0} \\ -\mathrm{Q} & \mathrm{Q} \end{pmatrix}$$ (ιδέ και Άσκηση 2.1.2$_{15}$).

17. Να υπολογίσετε το κάτω φράγμα Gilbert-Varshamov στις ακόλουθες περιπτώσεις: $A_2(6,\,3)$, $A_2(7,\,3)$, $A_2(8,\,5)$. Συγκρίνετε τα αποτελέσματα με τις τιμές του πίνακα στη σελίδα 63.

2.3 Κώδικες που προέρχονται από άλλους κώδικες (Η περίπτωση των γραμμικών κωδίκων)

Στην παράγραφο 1.4.1 είχαμε μελετήσει διαδικασίες για το πώς ένας κώδικας μπορεί να προέλθει από έναν άλλο κώδικα. Εδώ θα δούμε πώς μερικές από αυτές τις διαδικασίες εφαρμόζονται στηn περίπτωση των γραμμικών κωδίκων.

Έστω $\mathcal{C}$ ένας γραμμικός $[n,\, k,\, d]$ κώδικας με γεννήτορα πίνακα G. Αν επεκτείνουμε τον κώδικα $\mathcal{C}$ επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας, τότε ο κώδικας $\widehat{\mathcal{C}}$ που προκύπτει είναι και αυτός γραμμικός (γιατί;). Ένας γεννήτορας πίνακας του $\widehat{\mathcal{C}}$ μπορεί να προέλθει από τον γεννήτορα πίνακα G του κώδικα $\mathcal{C}$ επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας στις (κωδικο)λέξεις που αποτελούν τις γραμμές του G. Πράγματι, ο πίνακας, έστω $\widehat{\mathrm{G}}$, που προκύπτει έχει k το πλήθος γραμμές, οι οποίες είναι γραμμικά ανεξάρτητες, αφού οι αντίστοιχες k το πλήθος γραμμές του πίνακα G είναι γραμμικά ανεξάρτητες. Επίσης, αν $c_1 \cdots c_n\, c_{n+1}$ είναι ένα στοιχείο του κώδικα $\widehat{\mathcal{C}}$, τότε το $c_1 \cdots c_n$ είναι ένα στοιχείο του κώδικα $\mathcal{C}$, άρα γραμμικός συνδυασμός των γραμμών του πίνακα G. Επιπλέον δε, ισχύει $-c_{n+1} = c_1 + \cdots + c_n$. Οπότε εύκολα διαπιστώνουμε (από τον τρόπο κατασκευής των γραμμών του πίνακα $\widehat{\mathrm{G}}$) ότι το στοιχείο $c_1 \cdots c_n\, c_{n+1}$ είναι γραμμικός συνδυασμός των γραμμών του $\widehat{\mathrm{G}}$. Άρα, ο κώδικας $\widehat{\mathcal{C}}$ είναι ένας γραμμικός $[n+1,\, k,\, \hat{d}]$ κώδικας με ελάχιστη απόσταση $\hat{d}$ ίση με d ή $d+1$. Υπενθυμίζουμε δε ότι στην περίπτωση όπου ο κώδικας είναι δυαδικός, τότε η ελάχιστη απόσταση $\hat{d}$ είναι πάντα άρτια (ιδέ Πρόταση 1.4.9).

Έστω P ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$. Από την Πρόταση 2.2.12 έχουμε ότι $\mathrm{G}\cdot\mathrm{P}^{\mathrm{t}} = \mathbf{0}$. Επειδή για ένα στοιχείο $c_1 \cdots c_n\, c_{n+1}$ του κώδικα $\widehat{\mathcal{C}}$ ισχύει $c_1 + \cdots + c_n = -c_{n+1}$, έπεται ότι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\widehat{\mathcal{C}}$ είναι ο $(n-k+1) \times (n+1)$ πίνακας:

$$\widehat{\mathrm{P}} = \begin{pmatrix} \mathbf{1} & 1 \\ \mathrm{P} & \mathbf{0} \end{pmatrix}.$$

Έστω $\mathcal{C}$ ένας $[n,\, k,\, d]$ γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$. Για $i = 1, 2, \ldots, n$ ορίζουμε τον συνεπτυγμένο κώδικα $\mathcal{C}_i$ κατά την

συντεταγμένη i, δηλαδή:

$$\mathcal{C}_i = \{\, \mathbf{c}_i = a_1 a_2 \cdots a_{i-1} a_{i+1} \cdots a_n \mid \mathbf{c} = a_1 a_2 \cdots a_{i-1} a_i a_{i+1} \cdots a_n \in \mathcal{C} \,\}$$

(ιδέ σελίδα 46).

Είναι εύκολο να δούμε ότι κάθε κώδικας $\mathcal{C}_i$ είναι ένας $[n-1,\, k_i,\, d_i]$ γραμμικός κώδικας επί του $\mathbb{F}$. (Για τις τιμές των k_i και d_i ιδέ την Άσκηση 2 στο τέλος της παραγράφου.)

Μπορούμε να γενικεύσουμε την παραπάνω σύμπτυξη ως εξής:

Έστω $\mathcal{C}$ ένας $[n,\, k,\, d]$ γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ και I ένα υποσύνολο του συνόλου $\{\, 1,\, 2,\, \ldots,\, n \,\}$.

Κατασκευάζουμε έναν $q^k \times n$ πίνακα $\mathcal{M}$ του οποίου οι γραμμές είναι τα στοιχεία του κώδικα $\mathcal{C}$. Από τον πίνακα αυτό διαγράφουμε όλες τις στήλες των οποίων οι δείκτες είναι στοιχεία του συνόλου I. Οπότε προκύπτει ένας πίνακας $\mathcal{M}(I)$ με q^k το πλήθος γραμμές και $n-$ | I | το πλήθος στήλες. Ενδέχεται να υπάρχουν γραμμές στον πίνακα, οι οποίες επαναλαμβάνονται, οι διαφορετικές γραμμές του πίνακα $\mathcal{M}(I)$ αποτελούν έναν συνεπτυγμένο κώδικα $\mathcal{C}_I$ (ως προς τις συντεταγμένες που καθορίζονται από το σύνολο I). Είναι εύκολο να δούμε ότι ο κώδικας $\mathcal{C}_I$ είναι γραμμικός (ιδέ την Άσκηση 3 στο τέλος της παραγράφου).

Έστω τώρα $\mathcal{C}$ ένας γραμμικός $[n,\, k,\, d]$ κώδικας με γεννήτορα πίνακα G και πίνακα ελέγχου ισοτιμίας P. Υποθέτουμε ότι θέλουμε να τον σμικρύνουμε διαγράφοντας ορισμένες (κωδικο)λέξεις, αλλά ο κώδικας που θα προκύψει να παραμείνει γραμμικός. Η διαδικασία είναι απλή. Επειδή ο νέος κώδικας είναι υπόχωρος του αρχικού, αρκεί από μια βάση του κώδικα $\mathcal{C}$ να εξαιρέσουμε μερικά στοιχεία και να πάρουμε τον (υπό)χωρο τον παραγόμενο από τα εναπομείναντα στοιχεία. Αυτό επιτυγχάνεται ως εξής: Οι γραμμές του γεννήτορα πίνακα αποτελούν μια βάση του $\mathcal{C}$, οπότε διαγράφοντας μερικές γραμμές προκύπτει ένας πίνακας G_1, ο οποίος είναι γεννήτορας ενός υποκώδικα $\mathcal{C}_1$ του κώδικα $\mathcal{C}$.

Θα μπορούσαμε να έχουμε το ίδιο αποτέλεσμα, αν αντί να διαγράψουμε μερικές γραμμές από τον γεννήτορα πίνακα, προσθέσουμε μερικές γραμμές στον πίνακα ελέγχου ισοτιμίας, **αλλά** αν θέλουμε ο κώδικας που θα προκύ-

ψει να είναι γνήσια μικρότερος από τον αρχικό, πρέπει οι γραμμές που θα προσθέσουμε να είναι γραμμικά ανεξάρτητες από τις γραμμές του πίνακα ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$ (ιδέ Πόρισμα 2.2.14).

Παράδειγμα 2.3.1. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας, ο οποίος περιέχει **και** λέξεις περιττού βάρους (λέξεις αρτίου βάρους περιέχει πάντα ένας γραμμικός κώδικας). Τότε μπορούμε να βρούμε μια βάση του, η οποία να περιέχει μόνο μια λέξη περιττού βάρους. Πράγματι, αρκεί να παρατηρήσουμε ότι το άθροισμα λέξεων περιττού βάρους είναι λέξη αρτίου βάρους. Οπότε αν $\{\mathbf{c_1}, \mathbf{c_2}, \dots, \mathbf{c_i}, \dots, \mathbf{c_k}\}$ είναι μια βάση του $\mathcal{C}$ με περισσότερα του ενός στοιχεία περιττού βάρους, τότε επιλέγοντας ένα από αυτά και προσθέτοντάς το σε όλα τα υπόλοιπα περιττού βάρους προκύπτει μια βάση με ένα μόνο στοιχείο περιττού βάρους.

Από τα προηγούμενα έπεται ότι υπάρχει ένας γεννήτορας πίνακας G του οποίου μια γραμμή να είναι περιττού βάρους, ενώ όλες οι υπόλοιπες να είναι αρτίου βάρους. Αν διαγράψουμε τη γραμμή περιττού βάρους προκύπτει ένας πίνακας G_1, ο οποίος είναι γεννήτορας ενός υποκώδικα $\mathcal{C}_1$, ο οποίος έχει διάσταση κατά ένα λιγότερο από τον αρχικό κώδικα $\mathcal{C}$ και ο οποίος περιέχει όλες τις (κωδικο)λέξεις αρτίου βάρους. (Σύγκρινε με την Άσκηση $2.1.2_4$).

Αν τώρα P είναι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$, τότε προσθέτοντας μια γραμμή της οποίας όλα τα στοιχεία είναι 1, προκύπτει ένας πίνακας P_1 ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}_1$.

Με την αντίστροφη διαδικασία μπορούμε να αυξήσουμε έναν γραμμικό κώδικα. Πράγματι, αν $\mathcal{C}$ είναι ένας γραμμικός κώδικας με γεννήτορα πίνακα G, τότε προσθέτοντας γραμμές στον γεννήτορα πίνακα, οι οποίες είναι γραμμικά ανεξάρτητες από τις υπόλοιπες, παίρνουμε έναν πίνακα, ο οποίος αποτελεί γεννήτορα πίνακα ενός γραμμικού κώδικα, έστω $\bar{\mathcal{C}}$, ο οποίος περιέχει τον $\mathcal{C}$.

Παρατήρηση 2.3.2. Αυξάνοντας/σμικρύνοντας έναν γραμμικό κώδικα, τότε ο δυϊκός κώδικας σμικρύνεται/αυξάνεται ανάλογα (ιδέ Θεώρημα 2.2.13).

2.3.1 Ισοδύναμοι γραμμικοί κώδικες - Αυτομορφισμοί κωδίκων

Στην παράγραφο 1.4.1, όταν ορίσαμε τους ισοδύναμους κώδικες είχαμε ορίσει δύο στάδια μετασχηματισμού ενός κώδικα σε έναν ισοδύναμό του. Συγκεκριμένα είχαμε ορίσει τα εξής στάδια.

1. Για μια δεδομένη μετάθεση σ στα σύμβολα $\{1, 2, \dots, n\}$ αντικαθιστούμε κάθε (κωδικο)λέξη $\mathbf{c} = c_1 c_2 \cdots c_n$ με την λέξη $c_{\sigma(1)} c_{\sigma(2)} \cdots c_{\sigma(n)}$, οπότε προκύπτει ένας νέος κώδικας, έστω $\mathcal{D}$.

2. Σε κάθε θέση i των χαρακτήρων (κάθε) μιας (κωδικο)λέξης εφαρμόζουμε μια μετάθεση π_i στους χαρακτήρες του αλφάβητου $\mathbb{A}$, οπότε μια (κωδικο)λέξη, έστω $\mathbf{d} = d_1 d_2 \cdots d_n$ την αντικαθιστούμε με την λέξη:

$$\pi_1(d_1)\,\pi_2(d_2) \cdots \pi_n(d_n).$$

Συνεπώς, προκύπτει ένας νέος κώδικας, έστω $\mathcal{F}$.

Μάλιστα δε είχαμε παρατηρήσει (ιδέ Πρόταση 1.4.6) ότι για το πρώτο στάδιο μπορούμε για δεδομένη μετάθεση σ να πάρουμε τον αντίστοιχο πίνακα μετάθεση P_σ και θεωρώντας κάθε (κωδικο)λέξη:

$$\mathbf{c} = c_1 c_2 \cdots c_n$$

ως πίνακα γραμμή να κάνουμε τον πολλαπλασιασμό $\mathbf{c}\mathrm{P}_\sigma$.

Στην περίπτωση των γραμμικών κωδίκων, όπου το αλφάβητο είναι ένα σώμα και ένας κώδικας προσδιορίζεται πλήρως από έναν γεννήτορα πίνακα, είχαμε αποδείξει την εξής πρόταση (Πρόταση 2.1.9).

Πρόταση 2.3.3. *Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ και G ένας γεννήτορας πίνακάς του. Αν $\sigma \in S_n$ και P_σ είναι ο αντίστοιχος πίνακας μετάθεση, τότε ο μεταθετικά ισοδύναμος κώδικας $\mathcal{C}_\sigma$ έχει ως γεννήτορα πίνακα τον πίνακα GP_σ.*

Δηλαδή σε έναν γραμμικό κώδικα $\mathcal{C}$ πρέπει και αρκεί να εφαρμόσουμε μια μετάθεση σ στους χαρακτήρες των (κωδικο)λέξεων που αποτελούν μια βάση του και να λάβουμε μια βάση του μεταθετικά ισοδυνάμου κώδικα $\mathcal{C}_\sigma$.

Μάλιστα δε, είχαμε δει ως εφαρμογή ότι κάθε γραμμικός κώδικας είναι μεταθετικά ισοδύναμος με έναν συστηματικό κώδικα.

Παρατήρηση 2.3.4. Αν έχουμε δύο γραμμικούς κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$, οι οποίοι είναι μεταθετικά ισοδύναμοι, τότε και οι αντίστοιχοι κώδικες $\widehat{\mathcal{C}}_1$ και $\widehat{\mathcal{C}}_2$, που προκύπτουν επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας είναι μεταθετικά ισοδύναμοι (ιδέ Άσκηση 2.3.3$_4$).

Αν όμως συμπτύξουμε δύο μεταθετικά ισοδύναμους κώδικες κατά μία συντεταγμένη, τότε οι κώδικες που προκύπτουν δεν είναι κατ' ανάγκη μεταθετικά ισοδύναμοι, όπως μπορούμε να δούμε στο επόμενο παράδειγμα.

Παράδειγμα 2.3.5. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ οι δυαδικοί γραμμικοί κώδικες με αντίστοιχους γεννήτορες:

$$\mathrm{G}_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \text{ και } \mathrm{G}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Ο δεύτερος πίνακας προκύπτει από τον πρώτο αντιμεταθέτοντας την δεύτερη και έκτη στήλη, άρα οι δύο κώδικες είναι μεταθετικά ισοδύναμοι.

Αν τώρα συμπτύξουμε τους δύο κώδικες διαγράφοντας την δεύτερη στήλη και στους δύο πίνακες, εύκολα βλέπουμε ότι, από τους πίνακες που προκύπτουν, παράγονται κώδικες, οι οποίοι δεν είναι μεταθετικά ισοδύναμοι (γιατί;).

Από όλες τις μεταθέσεις που μπορούν να ορισθούν σε n σύμβολα, μια *ειδικού τύπου* μετάθεση παρουσιάζει ενδιαφέρον για την κατασκευή μεταθετικά ισοδυνάμων γραμμικών κωδίκων.

Έστω n ένας φυσικός αριθμός και a ένας ακέραιος σχετικά πρώτος προς τον n. Η απεικόνιση:

$$\varrho_a : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$$

με $\varrho_a(i) = ia \mod n$ προφανώς (γιατί;) ορίζει μια μετάθεση στα n σύμβολα[5], η οποία θα ονομάζεται **πολλαπλασιαστής**.

[5]Παρατηρήστε ότι $\varrho_a(n) = n$, επομένως στην πραγματικότητα είναι μια μετάθεση σε $n-1$ το πλήθος σύμβολα

Δεν είναι δύσκολο να αποδείξουμε ότι για δύο ακεραίους a και b ισχύει ότι $\varrho_a = \varrho_b$, αν και μόνο αν $a \equiv b, \mod n$. Οπότε έχουμε (μόνο) $\varphi(n)$ το πλήθος πολλαπλασιαστές, όπου φ είναι η συνάρτηση του Euler.

Επίσης, είναι προφανές να δούμε ότι $\varrho_a \circ \varrho_b = \varrho_{ab}$ και, επομένως, το σύνολο:

$$K = \{\, \varrho_a \mid \text{μκδ}(a, n) = 1 \,\}$$

αποτελεί υποομάδα της ομάδας μεταθέσεων S_n.

Παράδειγμα 2.3.6. Έστω $\mathcal{C}$ ο γραμμικός κώδικας μήκους 6 με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Για $a = 5$ έχουμε την μετάθεση (πολλαπλασιαστή) ϱ_5 με αντίστοιχο πίνακα μετάθεση:

$$\mathrm{P}_{\varrho_5} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

οπότε ο μεταθετικά ισοδύναμος κώδικας $\mathcal{C}_{\varrho_5}$ έχει ως γεννήτορα πίνακα τον:

$$\mathrm{GP}_{\varrho_5} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Περισσότερα για τους πολλαπλασιαστές θα δούμε στο επόμενο κεφάλαιο, όπου θα δούμε χρήσιμες εφαρμογές στους κυκλικούς κώδικες.

Για το δεύτερο στάδιο μετασχηματισμού, όπου σε κάθε θέση i των χαρακτήρων (κάθε)μιας (κωδικο)λέξης εφαρμόζουμε μια μετάθεση π_i στους χαρακτήρες του αλφάβητου, στην περίπτωση των γραμμικών κωδίκων, μπορούμε να εφαρμόσουμε *ειδικού τύπου* μεταθέσεις, οι οποίες αποτελούν και τις πλέον ενδιαφέρουσες περιπτώσεις.

Όπως είναι προφανές (γιατί;), ο πολλαπλασιασμός των στοιχείων ενός σώματος με ένα μη μηδενικό στοιχείο του επάγει μια μετάθεση στα στοιχεία του.

Επομένως, αν $\mathcal{C}$ είναι ένας γραμμικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ και $d_1, d_2, \ldots, d_n$ είναι μη μηδενικά στοιχεία του σώματος $\mathbb{F}$, τότε μπορούμε να κατασκευάσουμε έναν άλλο κώδικα $\mathcal{C}_{\mathrm{D}}$, ως εξής: Για κάθε (κωδικο)λέξη $\mathbf{c} = c_1 c_2 \cdots c_n$ του κώδικα $\mathcal{C}$ κατασκευάζουμε μια αντίστοιχη (κωδικο)λέξη για τον κώδικα $\mathcal{C}_{\mathrm{D}}$, την:

$$(c_1 d_1)(c_2 d_2) \cdots (c_n d_n).$$

Δηλαδή σε κάθε θέση i των χαρακτήρων (κάθε)μιας (κωδικο)λέξης εφαρμόζουμε μια μετάθεση π_i, η οποία επάγεται από τον πολλαπλασιασμό κάθε στοιχείου του σώματος με το στοιχείο d_i.

Πρόταση 2.3.7. *Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ και* G *ένας γεννήτορας πίνακας του. Έστω ο διαγώνιος $n \times n$ πίνακας* D*, όπου στην κυρία διαγώνιό του βρίσκονται τα μη μηδενικά στοιχεία του σώματος $d_1, d_2, \ldots, d_n$. Τότε ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}_{\mathrm{D}}$ είναι ο πίνακας* GD*.*

Απόδειξη. Η απόδειξη είναι άμεση από τα προηγούμενα. ό.έ.δ.

Θα μπορούσαμε να συνδυάσουμε τα δύο στάδια μετασχηματισμού ενός κώδικα σε έναν ισοδύναμό του ως εξής.

Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ και G ένας γεννήτορας πίνακάς του. Έστω D ο διαγώνιος $n \times n$ πίνακας, όπου στην κυρία διαγώνιό του βρίσκονται τα μη μηδενικά στοιχεία του σώματος $d_1, d_2, \ldots, d_n$, $\sigma \in S_n$ και P_σ ο αντίστοιχος πίνακας μετάθεση. Τότε αν πάρουμε τον πίνακα GM, όπου $\mathrm{M} = \mathrm{DP}_\sigma$, ο πίνακας αυτός ορίζει έναν κώδικα $\mathcal{C}_{\mathrm{M}}$, ο οποίος είναι ισοδύναμος προς τον αρχικό κώδικα $\mathcal{C}$.

Παρατηρήσεις 2.3.8. 1. Ο πίνακας:

$$\mathrm{M} = \mathrm{DP}_\sigma$$

είναι ένας τετραγωνικός πίνακας, ο οποίος σε κάθε γραμμή και κάθε στήλη έχει μόνο ένα μη μηδενικό στοιχείο.

Όμοια ο πίνακας:

$$\mathrm{N} = \mathrm{P}_\sigma \mathrm{D}$$

είναι ένας τετραγωνικός πίνακας, ο οποίος σε κάθε γραμμή και κάθε στήλη έχει μόνο ένα μη μηδενικό στοιχείο.

Προφανώς, ο πίνακας M είναι ο πίνακας που προκύπτει από τον πίνακα P_σ, αν αντικαταστήσουμε το 1 της i-γραμμής με το d_i για όλα τα $i = 1, 2, \ldots, n$. Ενώ ο πίνακας N προκύπτει από τον πίνακα P_σ, αν αντικαταστήσουμε το 1 της i-στήλης με το d_i για όλα τα $i = 1, 2, \ldots, n$.

Προφανώς, εν γένει $\mathrm{M} \neq \mathrm{N}$.

2. Γενικά ένας τετραγωνικός πίνακας ο οποίος σε κάθε γραμμή και κάθε στήλη έχει μόνο ένα μη μηδενικό στοιχείο ονομάζεται **μονωνυμικός πίνακας**.

   Από τα προηγούμενα προκύπτει (ιδέ Άσκηση 2.3.3$_7$) ότι κάθε μονωνυμικός πίνακας M γράφεται ως γινόμενο $\mathrm{M} = \mathrm{D}_1\mathrm{P}$, ή ως γινόμενο $\mathrm{M} = \mathrm{P}\mathrm{D}_2$ όπου P είναι ένας πίνακας μετάθεση και $\mathrm{D}_1, \mathrm{D}_2$ διαγώνιοι πίνακες.

3. Προφανώς, στην περίπτωση όπου το σώμα είναι το $\mathbb{Z}_2$, οι μόνοι μονωνυμικοί πίνακες είναι οι πίνακες μετάθεση.

Οι γραμμικοί κώδικες $\mathcal{C}$ και $\mathcal{C}_\mathrm{M}$, οι οποίοι έχουν ως γεννήτορες πίνακες τους G και GM, αντίστοιχα, όπου M είναι ένας μονωνυμικός πίνακας, θα ονομάζονται **μονωνυμικά ισοδύναμοι**.

Παράδειγμα 2.3.9. Έστω $\mathbb{F} = \{0, 1, c, c+1\}$ το σώμα με τέσσερα στοιχεία. Θεωρούμε τον γραμμικό κώδικα $\mathcal{C}$ επί του $\mathbb{F}$ με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & c & c \\ 0 & 1 & 0 & c & 1 & c \\ 0 & 0 & 1 & c & c & 1 \end{pmatrix}.$$

Έστω M ο μονωνυμικός πίνακας:

$$\begin{pmatrix} c & 0 & 0 & 0 & 0 & 0 \\ 0 & c+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & c+1 & 0 & 0 \\ 0 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & o & 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & c+1 & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c+1 & 0 \\ 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix}.$$

Ο πίνακας:

$$\Gamma = \mathrm{G} \cdot \mathrm{M} = \begin{pmatrix} 1 & 0 & 0 & 1 & c & c \\ 0 & 1 & 0 & c & 1 & c \\ 0 & 0 & 1 & c & c & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & c+1 & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c+1 & 0 \\ 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix}$$

$$= \begin{pmatrix} 0 & c & 0 & c+1 & c+1 & c+1 \\ 0 & 0 & c+1 & c & c+1 & c+1 \\ c & 0 & 0 & c+1 & 1 & c \end{pmatrix}$$

είναι ο γεννήτορας πίνακας ενός κώδικα $\mathcal{C}_{\mathrm{M}}$, ο οποίος είναι μονωνυμικά ισοδύναμος με τον αρχικό κώδικα $\mathcal{C}$.

Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί του σώματος $\mathbb{F}$.

Όπως είχαμε δει στο πρώτο κεφάλαιο (σελίδα 44), το σύνολο $\mu Aut(\mathcal{C}) = \{\, \sigma \in S_n$ με την ιδιότητα $\mathcal{C}_\sigma = \mathcal{C} \,\}$ αποτελεί την ομάδα μεταθετικών αυτομορφισμών του κώδικα $\mathcal{C}$.

Πρόταση 2.3.10. *Το σύνολο* $mAut(\mathcal{C}) = \{\, \mathrm{M}$, *όπου* M *μονωνυμικός πίνακας με την ιδιότητα* $\mathcal{C}_{\mathrm{M}} = \mathcal{C}\,\}$ *είναι ομάδα με πράξη τον πολλαπλασιασμό πινάκων.*

Απόδειξη. Έστω $\mathrm{M}_1, \mathrm{M}_2$ δύο μονωνυμικοί πίνακες. Έχουμε παρατηρήσει ότι υπάρχουν διαγώνιοι πίνακες $\mathrm{D}_1, \mathrm{D}_2$ και πίνακες μεταθέσεις $\mathrm{P}_1, \mathrm{P}_2$, ώστε $\mathrm{M}_1 = \mathrm{D}_1\mathrm{P}_1$ και $\mathrm{M}_2 = \mathrm{D}_2\mathrm{P}_2$, το γινόμενο $\mathrm{M}_1\mathrm{M}_2 = (\mathrm{D}_1\mathrm{P}_1)(\mathrm{D}_2\mathrm{P}_2)$ είναι ένας μονωνυμικός πίνακας, αφού $\mathrm{P}_1\mathrm{D}_2 = \overline{\mathrm{D}}_2\mathrm{P}_1$ (ιδέ Άσκηση 2.3.3$_7$). Άρα, πράγματι, το σύνολο $mAut(\mathcal{C})$ είναι ομάδα, δεδομένου ότι είναι πεπερασμένο. ό.έ.δ.

Η ομάδα $mAut(\mathcal{C})$ θα ονομάζεται ομάδα των **μονωνυμικών αυτομορφισμών**.

Πόρισμα 2.3.11. *Η ομάδα* $\mu Aut(\mathcal{C})$ *των μεταθετικών αυτομορφισμών ενός γραμμικού κώδικα* $\mathcal{C}$ *είναι υποομάδα (μέσω ισομορφισμού) της ομάδας* $mAut(\mathcal{C})$ *των μονωνυμικών αυτομορφισμών.*

Απόδειξη. Ταυτίζουμε κάθε μετάθεση $\sigma \in S_n$ με τον αντίστοιχο πίνακα μετάθεση P_σ. ό.έ.δ.

Πρόταση 2.3.12. *Έστω* $\mathcal{C}$ *ένας γραμμικός κώδικας. Τότε ισχύει* $\mu Aut(\mathcal{C}) = \mu Aut(\mathcal{C}^\perp)$.

Απόδειξη. Έστω P_σ ένας πίνακας μετάθεση, τότε ισχύει $(\mathcal{C}^\perp)_\sigma = (\mathcal{C}_\sigma)^\perp$ (ιδέ Άσκηση 2.3.3 $_6$). Επομένως, για κάθε στοιχείο $\mathrm{P} \in \mu Aut(\mathcal{C})$ έχουμε $\mathcal{C}^\perp = (\mathrm{P}(\mathcal{C}))^\perp = \mathrm{P}(\mathcal{C}^\perp)$, δηλαδή $\mathrm{P} \in \mu Aut(\mathcal{C}^\perp)$, οπότε έπεται το συμπέρασμα. ό.έ.δ.

Παρατηρήσεις 2.3.13. 1. Κάτι αντίστοιχο δεν ισχύει αν έχουμε έναν μονωνυμικό πίνακα. Πράγματι, έστω $\mathcal{C}$ ο γραμμικός κώδικας μήκους 2 επί του σώματος $\mathbb{F} = \{\, 0, 1, c, c+1 \,\}$ και γεννήτορα πίνακα $\mathrm{G} = (1\ c)$, τότε είναι εύκολο να δούμε ότι ο μονωνυμικός πίνακας:

$$\mathrm{M} = \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix}$$

αποτελεί έναν αυτομορφισμό του κώδικα, ενώ για τον δυϊκό κώδικα $\mathcal{C}^{\perp}$, ο οποίος έχει ως γεννήτορα πίνακα τον πίνακα $\Gamma = (1\ c+1)$, έχουμε:

$$(1\ c+1)\cdot\begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix} = (1\ 1)\ \notin \mathcal{C}^{\perp}.$$

2. Όταν ο κώδικας $\mathcal{C}$ δεν είναι γραμμικός, τότε δεν είναι αναγκαίο να ισχύει $\mu Aut(\mathcal{C}) = \mu Aut(\mathcal{C}^{\perp})$. Πράγματι, για τον δυαδικό κώδικα $\mathcal{C} = \{\,000,\ 100,\ 010,\ 001,\ 110,\ 111\,\}$ είναι εύκολο να δούμε ότι:

$$\mu Aut(\mathcal{C}) = \left\{ \mathrm{I}_3, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\} \quad \text{(να κάνετε τον έλεγχο).}$$

Ο δυϊκός όμως κώδικας είναι ο $\mathcal{C}^{\perp} = \{\,000\,\}$, οπότε κάθε 3×3 πίνακας μετάθεση είναι αυτομορφισμός του.

3. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ οι γραμμικοί κώδικες μήκους 2 επί του σώματος $\mathbb{F} = \{\,0,\ 1,\ c,\ c+1\,\}$ με αντίστοιχους γεννήτορες πίνακες $\mathrm{G}_1 = (1\ 1)$ και $\mathrm{G}_2 = (1\ c)$. Τότε οι δυϊκοί κώδικες $\mathcal{C}_1^{\perp}$ και $\mathcal{C}_2^{\perp}$ έχουν ως γεννήτορες πίνακες τους πίνακες $\Gamma_1 = (1\ 1)$ και $\Gamma_2 = (1\ c+1)$ αντίστοιχα. Οπότε βλέπουμε εύκολα ότι:

$$\mathrm{G}_1\cdot\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} = (1\ c).$$

Δηλαδή οι δύο κώδικες είναι μεταθετικά ισοδύναμοι. Αλλά οι αντίστοιχοι δυϊκοί κώδικες $\mathcal{C}_1^{\perp}$ και $\mathcal{C}_2^{\perp}$ δεν είναι μεταθετικά ισοδύναμοι (γιατί;).

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα. Εκτός από την μετάθεση που επάγει στα στοιχεία του ο πολλαπλασιασμός των στοιχείων του με ένα μη μηδενικό στοιχείο, κάθε αυτομορφισμός του επάγει μια μετάθεση στα στοιχεία του.

Επομένως, αν $\mathcal{C}$ είναι ένας γραμμικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ και α ένας αυτομορφισμός του, τότε μπορούμε να ορίσουμε τον ισοδύναμο κώδικα $\mathcal{C}_{\alpha} = \{\,\alpha(c_1)\,\alpha(c_2)\cdots\alpha(c_n)$ για όλα τα $c_1\,c_2\cdots c_n \in \mathcal{C}\,\}$.

Οι κώδικες $\mathcal{C}$ και $\mathcal{C}_{\alpha}$ θα ονομάζονται **αυτομορφικά ισοδύναμοι**.

Προφανώς (γιατί;), αν $\mathrm{G} = (a_{ij})$ είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}$, τότε ο πίνακας $\mathrm{G}_\alpha = (\alpha(a_{ij}))$ είναι γεννήτορας πίνακας του κώδικα $\mathcal{C}_\alpha$.

Τώρα είμαστε σε θέση να ορίσουμε μια πλέον γενική σχέση ισοδυναμίας μεταξύ κωδίκων.

Ορισμός 2.3.14. *Δύο γραμμικοί κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ επί του σώματος $\mathbb{F}$ θα ονομάζονται ισοδύναμοι, αν υπάρχει ένας μονωνυμικός πίνακας M και ένας αυτομορφισμός α του σώματος $\mathbb{F}$, έτσι ώστε $\mathcal{C}_2 = ((\mathcal{C}_1)_\mathrm{M})_\alpha$.*

Είναι εύκολο να αποδείξουμε ότι στο σύνολο των γραμμικών κωδίκων μήκους n, επί ενός σώματος $\mathbb{F}$, η ισοδυναμία κωδίκων αποτελεί σχέση ισοδυναμίας.

Παρατηρήσεις 2.3.15.

1. Πρέπει να παρατηρήσουμε ότι ο προηγούμενος ορισμός αναφέρεται μόνο σε γραμμικούς κώδικες και είναι *στενώτερος* από τον γενικό Ορισμό 1.4.1, καθότι εδώ αναφερόμαστε σε *ειδικού τύπου* (αλλά τις πλέον ενδιαφέρουσες) μεταθέσεις στα στοιχεία του σώματος /αλφαβήτου (πολλαπλασιασμός με ένα στοιχείο του σώματος ή εφαρμογή ενός αυτομορφισμού του σώματος).

   Στα επόμενα, όταν αναφερόμαστε σε ισοδύναμους γραμμικούς κώδικες, θα εννοούμε ως προς τον τελευταίο ορισμό.

2. Από τον προηγούμενο ορισμό έπεται ότι, όταν έχουμε έναν μονωνυμικό πίνακα M και έναν αυτομορφισμό α του σώματος $\mathbb{F}$, μπορούμε να ορίσουμε μια *σύνθεση*[6] $\mathrm{M} \circ \alpha$, η οποία εφαρμόζεται στα στοιχεία ενός γραμμικού κώδικα μήκους n και έτσι έχουμε μια απεικόνιση που απεικονίζει τον κώδικα $\mathcal{C}$ στον κώδικα $(\mathcal{C}_\mathrm{M})_\alpha$.

   Συγκεκριμμένα, έστω $\mathrm{M} = \mathrm{DP}_\sigma$, όπου D είναι ένας διαγώνιος πίνακας και P_σ ο πίνακας μετάθεση ως προς την μετάθεση σ. Σε κάθε i συντεταγμένη μιας (κωδικο)λέξης πολλαπλασιάζουμε το αντίστοιχο στοιχείο

[6] Εδώ ο όρος σύνθεση χρησιμοποιείται υπό την ευρεία έννοια ως δύο διαδοχικές *δράσεις* επί των στοιχείων ενός κώδικα.

με το στοιχείο του διαγωνίου πίνακα που βρίσκεται στην $(i\,i)$ θέση, κατόπιν μεταθέτουμε το στοιχείο αυτό στην $\sigma(i)$ θέση που υπαγορεύεται από την μετάθεση σ και τέλος, στο στοιχείο αυτό εφαρμόζουμε τον αυτομορφισμό α.

Στα επόμενα, θα χρησιμοποιούμε πλέον τον συμβολισμό $\mathcal{C}_{\mathrm{M}\circ\alpha}$ αντί του $(\mathcal{C}_{\mathrm{M}})_{\alpha}$

Παράδειγμα 2.3.16. Θα συνεχίσουμε το Παράδειγμα 2.3.9.

Είχαμε τον γραμμικό κώδικα $\mathcal{C}$ με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & c & c \\ 0 & 1 & 0 & c & 1 & c \\ 0 & 0 & 1 & c & c & 1 \end{pmatrix}$$

επί του σώματος $\mathbb{F} = \{\,0,\,1,\,c,\,c+1\,\}$ και τον μονωνυμικό πίνακα:

$$\begin{pmatrix} 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & c+1 & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & c+1 & 0 \\ 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & c \end{pmatrix},$$

οπότε κατασκευάσαμε τον κώδικα $\mathcal{C}_{\mathrm{M}}$ με γεννήτορα πίνακα:

$$\Gamma = \mathrm{G}\cdot\mathrm{M} = \begin{pmatrix} 0 & c & 0 & c+1 & c+1 & c+1 \\ 0 & 0 & c+1 & c & c+1 & c+1 \\ c & 0 & 0 & c+1 & 1 & c \end{pmatrix}.$$

Αν τώρα πάρουμε τον αυτομορφισμό α του σώματος $\mathbb{F}$, ο οποίος απεικονίζει κάθε στοιχείο x στο x^2, τότε ο ισοδύναμος κώδικας $\mathcal{C}_{\mathrm{M}\circ\alpha}$ θα έχει ως γεννήτορα πίνακα τον πίνακα:

$$\Gamma_{\alpha} = \begin{pmatrix} 0 & c+1 & 0 & c & c & c \\ 0 & 0 & c & c+1 & c & c \\ c+1 & 0 & 0 & c & 1 & c+1 \end{pmatrix}.$$

Ένα ερώτημα που προκύπτει είναι, αν έχουμε να μετασχηματίσουμε έναν γραμμικό κώδικα $\mathcal{C}$ σε έναν ισοδύναμό του, κατά πόσο έχει σημασία η σειρά των επιμέρους μετασχηματισμών που πραγματοποιούμε [μετάθεση των χαρακτήρων σε κάθε (κωδικο)λέξη, μετάθεση των στοιχείων του σώματος]. Στην Πρόταση 2.3.10 είχαμε δει ότι αν έχουμε έναν πίνακα μετάθεση P και έναν διαγώνιο πίνακα D, τότε υπάρχει ένας άλλος διαγώνιος πίνακας $\overline{\mathrm{D}}$, έτσι ώστε $\mathrm{DP} = \mathrm{P}\overline{\mathrm{D}}$, δηλαδή δεν έχει σημασία αν πρώτα πραγματοποιήσουμε μια μετάθεση των χαρακτήρων στις (κωδικο)λέξεις και μετά μετάθεση των στοιχείων του σώματος με πολλαπλασιασμό με ένα στοιχείο ή αντίστροφα.

Αν τώρα έχουμε έναν αυτομορφισμό α του σώματος, τότε είναι εύκολο να δούμε ότι δεν έχει σημασία αν πρώτα πραγματοποιήσουμε μια μετάθεση των χαρακτήρων στις (κωδικο)λέξεις και μετά μετάθεση των στοιχείων του σώματος με εφαρμογή του αυτομορφισμού α ή αντίστροφα.

Αυτό θα το συμβολίζουμε ως $\mathrm{P} \circ \alpha = \alpha \circ \mathrm{P}$, όπου P είναι ένας πίνακας μετάθεση.

Επίσης, αν $c_1\, c_2 \cdots c_n$ είναι μια (κωδικο)λέξη, $d_1, d_2 \ldots, d_n$ στοιχεία του σώματος $\mathbb{F}$ και α ένας αυτομορφισμός του $\mathbb{F}$, τότε επειδή $\alpha(c_i d_i) = \alpha(c_i)\,\alpha(d_i)$, δεν έχει σημασία αν πρώτα πολλαπλασιάσουμε κάθε χαρακτήρα μιας (κωδικο)λέξης με ένα στοιχείο και μετά εφαρμόσουμε τον αυτομορφισμό α ή αντίστροφα.

Αυτό θα το συμβολίζουμε με $\alpha \circ \mathrm{D} = \mathrm{D}_\alpha \circ \alpha$, όπου $\mathrm{D} = (\, d_i\,)$ είναι ένας διαγώνιος πίνακας και D_α ο αντίστοιχος διαγώνιος $(\, \alpha(d_i)\,)$.

Πρόταση 2.3.17. *Έστω $\mathcal{C}$ ένας γραμμικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$. Το σύνολο $Aut(\mathcal{C})$ των απεικονίσεων $\mathrm{M} \circ \alpha$, όπου M είναι μονωνυμικός πίνακας και α αυτομορφισμός του $\mathbb{F}$, με την ιδιότητα $\mathcal{C} = \mathcal{C}_{\mathrm{M}\circ\alpha}$ αποτελεί ομάδα.*

Απόδειξη. Η απόδειξη στην πραγματικότητα έχει προηγηθεί, με τις λεπτομέρειες να αφίονται ως άσκηση. ό.έ.δ.

Η ομάδα $Aut(\mathcal{C})$ θα ονομάζεται **ομάδα αυτομορφισμών** του γραμμικού κώδικα $\mathcal{C}$.

Πόρισμα 2.3.18. *Για έναν γραμμικό κώδικα $\mathcal{C}$ επί του πεπερασμένου σώματος $\mathbb{F}$ ισχύει $\mu Aut(\mathcal{C}) \leq mAut(\mathcal{C}) \leq Aut(\mathcal{C})$ (ιδέ και Πορισμα 2.3.11).*

Στην Πρόταση 2.3.12 είχαμε δει ότι, για έναν γραμμικό κώδικα $\mathcal{C}$, ισχύει $\mu Aut(\mathcal{C}) = \mu Aut(\mathcal{C}^{\perp})$. Ενώ είχαμε επισημάνει (Παρατήρηση $2.3.13_1$) ότι κάτι αντίστοιχο δεν συμβαίνει για την ομάδα των μονωνυμικών αυτομορφισμών.

Πρόταση 2.3.19. *Έστω $\mathcal{C}$ ένας γραμμικός κώδικας. Τότε ισχύει:*

i) $mAut(\mathcal{C}^{\perp}) = \{\, \mathrm{D}^{-1}\mathrm{P} \mid \mathrm{DP} \in mAut(\mathcal{C}) \,\}$.

ii) $Aut(\mathcal{C}^{\perp}) = \{\, (\mathrm{D}^{-1}\mathrm{P}) \circ \alpha \mid (\mathrm{DP}) \circ \alpha \in Aut(\mathcal{C}) \,\}$.

Απόδειξη. Έστω $\mathbf{c} = c_1\, c_2 \cdots c_n$ ένα στοιχείο του κώδικα $\mathcal{C}$ και $\mathbf{b} = b_1\, b_2 \cdots b_n$ ένα στοιχείο του $\mathcal{C}^{\perp}$. Αν $\mathrm{DP} \in mAut(\mathcal{C})$, όπου $\mathrm{D} = (\, d_i \,)_{n\times n}$ είναι διαγώνιος πίνακας με μη μηδενικά στοιχεία στην κυρία διαγώνιο και P ένας πίνακας που επάγεται από την μετάθεση σ, τότε, επειδή $\mathrm{DP} \in mAut(\mathcal{C})$, υπάρχει $\mathbf{a} = a_1\, a_2 \cdots a_n \in \mathcal{C}$ έτσι ώστε $\mathbf{c} = \mathbf{a}\mathrm{DP}$. Οπότε για το εσωτερικό γινόμενο $\langle\, \mathbf{c},\, \mathbf{b}\mathrm{D}^{-1}\mathrm{P} \,\rangle$ έχουμε:

$$\begin{aligned} \langle\, \mathbf{c},\, \mathbf{b}\mathrm{D}^{-1}\mathrm{P} \,\rangle = \langle\, \mathbf{a}\mathrm{DP},\, \mathbf{b}\mathrm{D}^{-1}\mathrm{P} \,\rangle &= \sum_{i=1}^{n} (a_{\sigma(i)} d_{\sigma(i)})(b_{\sigma(i)} d_{\sigma(i)}^{-1}) \\ &= \sum_{i=1}^{n} a_i b_i \;=\; 0. \end{aligned}$$

Δηλαδή $\mathbf{b}\mathrm{D}^{-1}\mathrm{P} \in \mathcal{C}^{\perp}$. Οπότε εύκολα αποδεικνύονται και οι δύο ισχυρισμοί της πρότασης. ό.έ.δ.

Θα κλείσουμε την παράγραφο διατυπώνοντας ένα ενδιαφέρον *αντίστροφο* πρόβλημα.

Έστω G_1 και G_2 δύο τυχαίοι $k \times n$ πίνακες με στοιχεία από ένα πεπερασμένο σώμα $\mathbb{F}$. Μπορούμε να αποφανθούμε αν οι αντίστοιχοι γραμμικοί κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ που ορίζουν οι δύο πίνακες είναι ισοδύναμοι;

Η πολυπλοκότητα αυτού του προβλήματος είναι μεγάλη και δεν θα ασχοληθούμε εδώ.

2.3.2 (Υπο)κώδικες ως προς υποσώματα

Μια αξιόλογη περίπτωση σμίκρυνσης ενός γραμμικού κώδικα είναι η εξής:

Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί ενός πεπερασμένου σώματος $\mathbb{K}$ και έστω $\mathbb{F}$ ένα υπόσωμα του $\mathbb{K}$. Θεωρούμε όλες τις (κωδικο)λέξεις του κώδικα $\mathcal{C}$ των οποίων οι χαρακτήρες προέρχονται από το υπόσωμα $\mathbb{F}$, δηλαδή το σύνολο $\mathcal{C}_{\mathbb{F}} = \mathcal{C} \cap \mathbb{F}^n$. Το σύνολο αυτό, επειδή ο κώδικας $\mathcal{C}$ είναι γραμμικός, είναι διανυσματικός χώρος επί του σώματος $\mathbb{F}$.

Έστω $\mathrm{H} = (h_{ij})_{\nu\times n}$ ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$. Θα κατασκευάσουμε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}_{\mathbb{F}}$, ο οποίος 'προέρχεται' από τον πίνακα H.

Επιλέγουμε και σταθεροποιούμε μια διατεταγμένη βάση $B = \{ e_1, e_2, \dots , e_s \}$ του $\mathbb{K}$ επί του $\mathbb{F}$, όπου $s = [\mathbb{K} : \mathbb{F}]$ ο βαθμός επέκτασης του σώματος $\mathbb{K}$ επί του υποσώματος $\mathbb{F}$. Για κάθε στοιχείο h_{ij} του πίνακα H, ως στοιχείο του σώματος $\mathbb{K}$, έστω $[r_i^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση του ως γραμμικός συνδυασμός στοιχείων της βάσης B με συντελεστές από το σώμα $\mathbb{F}$. Κατασκευάζουμε τον πίνακα:

$$\mathrm{P} = \begin{pmatrix} [r_1^1] & [r_1^2] & \cdots & [r_1^n] \\ [r_2^1] & [r_2^2] & \cdots & [r_2^n] \\ \vdots & \vdots & \vdots & \vdots \\ [r_\nu^1] & [r_\nu^2] & \cdots & [r_\nu^n] \end{pmatrix}.$$

Δηλαδή αντικαθιστούμε κάθε στοιχείο του πίνακα H με το αντίστοιχο διάνυσμα στήλη των συντελεστών του. Αν τώρα αναπτύξουμε κάθε διάνυσμα στήλη προκύπτει ένας $\nu s \times n$ πίνακας $\overline{\mathrm{H}}$ με στοιχεία από το (υπό)σωμα $\mathbb{F}$.

Το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα, αν και μόνο αν:

$$(c_1, c_2, \dots , c_n) \cdot \mathrm{H}^t = \mathbf{0}.$$

Οπότε, σε συνδυασμό με την προηγούμενη σχέση, έχουμε ότι το $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα, αν και μόνο αν $c_1[r_i^1] + c_2[r_i^2] + \cdot c_n[r_i^n] = \mathbf{0}$ για κάθε $i = 1, 2, \dots , \nu$. Δηλαδή το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα $\mathcal{C}_{\mathbb{F}}$, αν και μόνο αν $(c_1, c_2, \dots , c_n) \cdot \overline{\mathrm{H}}^t = \mathbf{0}$.

Συνεπώς, με την διαδικασία αυτή κατασκευάσαμε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}_{\mathbb{F}}$.

Παράδειγμα 2.3.20. Έστω $\mathbb{K}$ ένα σώμα με τέσσερα στοιχεία. Έστω $B = \{1, c\}$ μια βάση του επί του $\mathbb{Z}_2$, Όπότε $\mathbb{K} = \{0, 1, c, c+1\}$.

Θεωρούμε τον κώδικα $\mathcal{C}$ επί του $\mathbb{K}$ με γεννήτορα πίνακα:

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & c & c \\ 0 & 1 & 0 & c & 1 & c \\ 0 & 0 & 1 & c & c & 1 \end{pmatrix}.$$

Προφανώς (Θεώρημα 2.2.17), ένας πίνακας ελέγχου ισοτιμίας του κώδικα είναι ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 1 & c & c & 1 & 0 & 0 \\ c & 1 & c & 0 & 1 & 0 \\ c & c & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Από τον πίνακα $\mathrm{P} = ([r_j^i])_{3\times 6}$ προκύπτει ο πίνακας:

$$\begin{pmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{pmatrix}.$$

Οπότε ο 6×6 πίνακας:

$$\overline{\mathrm{H}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

είναι ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}_{\mathbb{Z}_2}$.

Μάλιστα δε, θα μπορούσαμε να παραλείψουμε την τελευταία γραμμή του πίνακα, καθότι είναι γραμμικός συνδυασμός των υπολοίπων και τελικά να πάρουμε έναν 5×6 πίνακα ελέγχου ισοτιμίας.

Παρατήρηση 2.3.21. Η ανωτέρω κατασκευή έχει ενδιαφέρουσες εφαρμογές στην περίπτωση όπου η επέκταση $\mathbb{K}$, επί της οποίας ορίζεται ο αρχικός κώδικας, δεν είναι τυχαία, αλλά το σώμα ριζών ενός πολυωνύμου $\varphi(x)$ με συντελεστές από το (υπό)σωμα $\mathbb{F}$.

Περισσότερα επ' αυτού θα δούμε, όταν ασχοληθούμε με κυκλικούς κώδικες και γενικευμένους Reed-Solomon κώδικες. (Ιδέ παραγράφους *Κυκλικοί κώδικες και ρίζες της μονάδας*, σελίδα 189 και *Εναλλασσόμενοι κώδικες*, σελίδα 333).

2.3.3 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$. Για $i = 1, 2, \ldots, n$ έστω $\mathcal{C}_i$ ο συνεπτυγμένος κώδικας κατά τη συντεταγμένη i.

   Να αποδείξετε ότι:

   i) Αν έχουμε έναν γεννήτορα πίνακα G του αρχικού κώδικα $\mathcal{C}$, τότε διαγράφοντας την i συντεταγμένη από τις γραμμές του G προκύπτει ένα σύνολο που παράγει τον κώδικα $\mathcal{C}_i$ (δηλαδή ο κώδικας $\mathcal{C}_i$ είναι γραμμικός).

   ii) $k \geq k_i \geq k-1$ και $d \geq d_i \geq d-1$.

   Στην περίπτωση όπου $d > 1$, να αποδείξετε ότι $k = k_i$. Μπορείτε να αποφανθείτε πότε έχουμε $d = d_i$ και πότε $d_i = d-1$;

   Αν $d = 1$, ενδέχεται να έχουμε $d_i \geq d$. Μπορείτε να δώσετε ένα παράδειγμα;

   iii) Υπάρχουν τουλάχιστον $n-k$ το πλήθος δείκτες i για τους οποίους ισχύει ότι $k_i = k$.

3. Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ και $\mathcal{C}_I$ ο συνεπτυγμένος κώδικας ως προς τις συντεταγμένες που υπαγορεύονται από ένα υποσύνολο I του συνόλου $\{1, 2, \ldots, n\}$.

Δείξτε ότι απεικόνιση η $f : \mathcal{C} \longrightarrow \mathcal{C}_I$ με $f(\mathbf{c}) = \mathbf{c}_I$, όπου $\mathbf{c}_I$ είναι η λέξη που προκύπτει από την $\mathbf{c}$ με διαγραφή των χαρακτήρων που βρίσκονται στις θέσεις που υπαγορεύονται από τα στοιχεία του I είναι γραμμική. Να υπολογίσετε τον πυρήνα της.

4. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ δύο γραμμικοί κώδικες, οι οποίοι είναι μεταθετικά ισοδύναμοι. Αν $\widehat{\mathcal{C}}_1$ και $\widehat{\mathcal{C}}_2$ είναι οι αντίστοιχοι κώδικες που προκύπτουν επισυνάπτοντας ένα ψηφίο ελέγχου ισοτιμίας, δείξετε ότι και οι κώδικες αυτοί είναι μεταθετικά ισοδύναμοι.

5. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ δύο γραμμικοί κώδικες επί του ιδίου σώματος. Αν $\mathcal{C} = \mathcal{C}_1 \mid \mathcal{C}_2$ (ιδέ Άσκηση 2.1.2$_{14}$), δείξτε ότι $\mu Aut(\mathcal{C}_1) \times \mu Aut(\mathcal{C}_2) \leq \mu Aut(\mathcal{C})$.

   Μπορείτε να δώσετε ένα παράδειγμα, όπου στην προηγουμένη σχέση έχουμε ισότητα και ένα παράδειγμα, όπου έχουμε γνήσια ανισότητα;

6. Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n. Αν σ είναι μια μετάθεση σε n σύμβολα, P_σ ο πίνακας μετάθεση και $\mathcal{C}_\sigma$ ο μεταθετικά ισοδύναμος κώδικας, τότε δείξτε ότι $(\mathcal{C}^\perp)_\sigma = (\mathcal{C}_\sigma)^\perp$.

   Επιπλέον, δείξτε ότι αν ο κώδικας $\mathcal{C}$ είναι αυτοδυϊκός, τότε και ο κώδικας $\mathcal{C}_\sigma$ είναι αυτοδυϊκός.

7. Έστω M ένας $n \times n$ μονωνυμικός πίνακας. Δείξτε ότι υπάρχει ένας πίνακας μετάθεση P και διαγώνιοι πίνακες $\mathrm{D}_1, \mathrm{D}_2$ έτσι ώστε:

$$\mathrm{M} = \mathrm{D}_1\mathrm{P} = \mathrm{D}_2\mathrm{P}.$$

8. Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί του σώματος $\mathbb{F}$. Έστω σ μια μετάθεση σε n σύμβολα και P_σ ο αντίστοιχος πίνακας μετάθεση, M ένας $n \times n$ μονωνυμικός πίνακας και α ένας αυτομορφισμός του σώματος.

   Αν $\mathcal{C}_1 = \mathcal{C}_\sigma$ είναι ο μεταθετικά ισοδύναμος κώδικας, $\mathcal{C}_2 = \mathcal{C}_\mathrm{M}$ είναι ο μονωνυμικά ισοδύναμος κώδικας και $\mathcal{C}_3 = \mathcal{C}_{\mathrm{M}\circ\alpha}$ είναι ο ισοδύναμος κώδικας, δείξτε ότι:

   i) $\mu Aut(\mathcal{C}_1) = \mathrm{P}_\sigma^{-1} \mu Aut(\mathcal{C}) \mathrm{P}_\sigma$.

ii) $mAut(\mathcal{C}_2) = \mathrm{M}^{-1} mAut(\mathcal{C})\mathrm{M}$.

iii) $Aut(\mathcal{C}_3) = (\mathrm{M} \circ \alpha)^{-1} Aut(\mathcal{C})(\mathrm{M} \circ \alpha)$.

9. Έστω $\mathcal{C}$ ένας γραμμικός κώδικας μήκους n επί του σώματος $\mathbb{F}$. Υποθέτουμε ότι το πλήθος των στοιχείων του σώματος είναι πρώτος αριθμός.

   Δείξτε ότι: $mAut(\mathcal{C}) = Aut(\mathcal{C})$.

10. Έστω $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ με βαθμό επέκτασης s και $\mathcal{C}$ ένας γραμμικός κώδικας επί του $\mathbb{K}$ με παραμέτρους $[n,\, k,\, d]$. Αν η διάσταση του κώδικα $\mathcal{C}_{\mathbb{F}}$ είναι k_0, δείξτε ότι:

$$k \geq k_0 \geq n - s(n-k).$$

    Στην περίπτωση όπου ο αρχικός κώδικας $\mathcal{C}$ έχει μια βάση, η οποία αποτελείται από στοιχεία του $\mathbb{F}^n$, δείξτε ότι η βάση αυτή είναι και βάση του (υπο)κώδικα $\mathcal{C}_{\mathbb{F}}$.

    Προσοχή! Οι δύο κώδικες $\mathcal{C}$ και $\mathcal{C}_{\mathbb{F}}$ δεν είναι ίσοι.

11. Έστω $\mathbb{F}$ το σώμα με οκτώ στοιχεία που προκύπτει από το $\mathbb{Z}_2$ αν επισυνάψουμε ένα στοιχείο c που ικανοποιεί τη σχέση $c^3 = c + 1$. Θεωρούμε τους γραμμικούς κώδικες $\mathcal{C},\ \mathcal{D},\ \mathcal{F}$ μήκους 7 επί του $\mathbb{F}$ με πίνακες ελέγχου ισοτιμίας:

$$\mathrm{H}_1 = (1,\, c\, c^2\, c^3\, c^4\, c^5\, c^6), \quad \mathrm{H}_2 = \begin{pmatrix} 1 & c & c^2 & c^3 & c^4 & c^5 & c^6 \\ 1 & c^2 & c^4 & c^6 & c & c^3 & c^5 \end{pmatrix},$$

$$\mathrm{H}_3 = \begin{pmatrix} 1 & c & c^2 & c^3 & c^4 & c^5 & c^6 \\ 1 & c^3 & c^6 & c^2 & c^5 & c & c^4 \end{pmatrix}$$

    αντίστοιχα.

    Επιλέγοντας το σύνολο $\{\, 1,\, c,\, c^2 \,\}$ ως βάση του $\mathbb{F}$ επί του $\mathbb{Z}_2$ να υπολογίσετε τους αντίστοιχους πίνακες ελέγχου ισοτιμίας για τους κώδικες:

$$\mathcal{C}_{\mathbb{Z}_2},\ \mathcal{D}_{\mathbb{Z}_2},\ \mathcal{F}_{\mathbb{Z}_2}.$$

Δείξτε ότι $\mathcal{C}_{\mathbb{Z}_2} = \mathcal{D}_{\mathbb{Z}_2}$ και ότι ο κώδικας $\mathcal{F}_{\mathbb{Z}_2}$ είναι ο επαναληπτικός δυαδικός κώδικας μήκους 7.

12. Έστω $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ με βαθμό επέκτασης s και $\mathcal{C}$ ένας γραμμικός κώδικας επί του $\mathbb{K}$ με παραμέτρους $[n, k, d]$. Υποθέτουμε ότι M είναι ένας μονωνυμικός πίνακας με στοιχεία από το σώμα $\mathbb{F}$. Δείξτε ότι, αν $\mathrm{M} \in mAut(\mathcal{C})$, τότε $\mathrm{M} \in mAut(\mathcal{C}_{\mathbb{F}})$.

2.4 Κωδικοποίηση και αποκωδικοποίηση με γραμμικούς κώδικες

Στη σελίδα 5 είχαμε αναφερθεί στη διαδικασία κωδικοποίησης - αποκωδικοποίησης. Συγκεκριμένα, είχαμε ορίσει ως συνάρτηση κωδικοποίησης μια συνάρτηση $f : S \longrightarrow \mathcal{C}$ από το σύνολο πηγή S σε έναν κώδικα $\mathcal{C}$, η οποία είναι $1-1$ και επί.

Στην περίπτωση των γραμμικών κωδίκων η διαδικασία της κωδικοποίησης γίνεται ευκολότερη χρησιμοποιώντας τον γεννήτορα πίνακα του κώδικα.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας, επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία, του οποίου ο γεννήτορας πίνακας είναι ο $k \times n$ πίνακας G. Αν ως σύνολο πηγή επιλέξουμε τον διανυσματικό χώρο $\mathbb{F}^k$, τότε η συνάρτηση $f : \mathbb{F}^k \longrightarrow \mathcal{C}$ με $f(\mathbf{u}) = \mathbf{u}\mathrm{G}$ είναι μια συνάρτηση κωδικοποίησης αφού είναι 1-1 και επί (γιατί;). Επιπλέον, η συνάρτηση f είναι γραμμική, επομένως μπορούμε να *εκμεταλλευθούμε* όλες τις ιδιότητες των γραμμικών συναρτήσεων.

Στην περίπτωση, όπου ο γεννήτορας πίνακας είναι σε ανηγμένη κλιμακωτή μορφή $\mathrm{G} = [\mathrm{I}_k \, \mathrm{A}]$, έχουμε ότι η προς κωδικοποίηση λέξη $\mathbf{u} \in \mathbb{F}^k$ κωδικοποιείται ως $\mathbf{u}[\mathrm{I}_k \, \mathrm{A}] = \mathbf{u}\,\mathbf{v}$, όπου $\mathbf{v} = \mathbf{u}\mathrm{A}$, δηλαδή η κωδικοποιημένη λέξη αποτελείται από δύο τμήματα, το πρώτο είναι η προς κωδικοποίηση λέξη (το τμήμα πληροφορίας) και το δεύτερο *πλεονάζον* τμήμα είναι το τμήμα που επισυνάπτεται για την προστασία από τους θορύβους κατά τη μετάδοση. (Μια ανάλογη συζήτηση έχει προηγηθεί στη σελίδα 80).

Σ' αυτή την περίπτωση, ένας πίνακας ελέγχου ισοτιμίας είναι ο $\mathrm{P} = [-\mathrm{A}^t \, \mathrm{I}_{n-k}]$ (Θεώρημα 2.2.17), οπότε μπορούμε να κωδικοποιήσουμε μια λέξη

$\mathbf{u} = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{F}^k$ και με τον εξής τρόπο: Αν η κωδικοποιημένη λέξη είναι η $\mathbf{c} = (c_1, c_2, \ldots, c_k, c_{k+1}, \ldots, c_n)$, τότε $c_i = \lambda_i$ για $i = 1, \ldots, k$ και απομένει να υπολογισθούν τα υπόλοιπα c_j για $j = k+1, \ldots, n$. Όμως από την σχέση $\mathbf{c}\mathrm{P}^t = \mathbf{0}$ έχουμε ότι $\mathbf{u}\mathrm{A} = (c_{k+1}, \ldots, c_n)$.

Από τα παραπάνω είναι φανερό ότι ένας δίαυλος επικοινωνίας για να αποστείλει k το πλήθος σύμβολα πληροφορίας πρέπει να μεταδόσει n το πλήθος σύμβολα στο κωδικοποιημένο μήνυμα. Επομένως, αποκτά σημασία ο λόγος $\frac{k}{n}$, ο οποίος *μετρά* το μέγεθος της μεταδιδόμενης πληροφορίας συγκριτικά με το μέγεθος της μεταδιδόμενης (κωδικο)λέξης, η οποία *εμπεριέχει* την πληροφορία.

Ο λόγος $\frac{k}{n}$ κυμαίνεται μεταξύ 0 και 1. Για την ακραία τιμή $\frac{k}{n} = 0$ έχουμε τον τετριμμένο κώδικα και δεν έχουμε μετάδοση πληροφορίας. Για την ακραία τιμή $\frac{k}{n} = 1$ έχουμε $k = n$, όπου το πηγαίο μήνυμα μεταδίδεται ως έχει χωρίς καμία προστασία από θορύβους.

Στην περίπτωση ενός επαναληπτικού κώδικα, όπου έχουμε $k = 1$, ο λόγος $\frac{k}{n}$ ισούται με $1/n$. Συνεπώς, όταν το n αυξάνει, η προστασία είναι μεγάλη, αλλά συγκριτικά το μέγεθος της μεταδιδόμενης πληροφορίας είναι πολύ μικρό (ιδέ τη σχετική παρατήρηση στη σελίδα 50).

Τα παραπάνω αφορούν γραμμικούς κώδικες, όπου το μέγεθός τους είναι ίσον με q^k, οπότε $k = \log_q q^k$. Στην γενική περίπτωση ενός (όχι κατ' ανάγκη γραμμικού) κώδικα μεγέθους M μπορούμε να γενικεύσουμε και ως αντίστοιχο λόγο να θεωρήσουμε τον λόγο $\frac{\log_q M}{n}$.

2.4.1 Διόρθωση λαθών με έναν γραμμικό κώδικα

Η συνάρτηση αποκωδικοποίησης (ιδέ σελίδα 18) $\varphi : \mathbb{F}_p^n \longrightarrow \mathcal{C}$ ορίζεται από τον διανυσματικό χώρο $\mathbb{F}_p^n$ στον διανυσματικό υπόχωρο $\mathcal{C}$. Αυτό μας επιτρέπει να βρούμε *αποτελεσματικούς* τρόπους ανίχνευσης και διόρθωσης λαθών.

Πριν δούμε πώς διορθώνουμε λάθη με έναν γραμμικό κώδικα εκμεταλλευόμενοι το γεγονός ότι έχει τη δομή διανυσματικού χώρου, θα παραθέσουμε μερικά αποτελέσματα απο τη Γραμμική Άλγεβρα.

Ορισμός 2.4.1. *Έστω V ένας διανυσματικός χώρος με συντελεστές από ένα (όχι κατ' ανάγκη πεπερασμένο) σώμα $\mathbb{F}$ και U ένας διανυσματικός υπόχωρος του V. Για κάθε $v \in V$ ορίζουμε το σύνολο $v + U = \{ v + u \mid u \in U \}$. Το σύνολο αυτό ονομάζεται* ***σύμπλοκο*** *του υπόχωρου U και το v* ***αντιπρόσωπος*** *του συμπλόκου.*

Θεώρημα 2.4.2. *Έστω V ένας διανυσματικός χώρος με συντελεστές από ένα σώμα $\mathbb{F}$, $a, b \in V$ και U ένας διανυσματικός υπόχωρος του V. Οι ακόλουθες προτάσεις είναι ισοδύναμες.*

1. $a + U = b + U$.
2. $a - b \in U$.
3. $b \in a + U$.

Απόδειξη. Έστω $x \in a + U = b + U$. Τότε υπάρχουν $u_1, u_2 \in U$, έτσι ώστε $x = a + u_1 = b + u_2$, δηλαδή $a - b = u_2 - u_1$. Αλλά ο U είναι διανυσματικός υπόχωρος, επομένως $a - b = u_2 - u_1 \in U$. Δηλαδή $b = a + (u_1 - u_2) \in U$, οπότε για κάθε $u \in U$ έχουμε $b + u = a + (u_1 - u_2) + u \in U$. Άρα $b + U \subseteq a + U$. Όμοια αποδεικνύεται ότι $a + U \subseteq b + U$. ό.έ.δ.

Πόρισμα 2.4.3. *Με τις υποθέσεις του προηγουμένου θεωρήματος*

1. $a + U = U$, *αν και μόνο αν* $a \in U$.
2. *Δύο σύμπλοκα είτε συμπίπτουν είτε είναι ξένα μεταξύ τους. Δηλαδή αν* $(a + U) \cap (b + U) \neq \emptyset$, *τότε* $(a + U) = (b + U)$.
3. *Ένα στοιχείο του διανυσματικού χώρου V ανήκει σε (ακριβώς) ένα σύμπλοκο ως προς τον υπόχωρο U.*

Απόδειξη. 1. Προφανώς $a + U = U = 0 + U$, αν και μόνο αν $a - 0 = a \in U$.

2. Έστω $v \in (a + U) \cap (b + U)$, τότε $a + U = v + U = b + U$.

3. Κάθε $v \in V$ ανήκει σε ένα (ακριβώς) σύμπλοκο, το $v + U$.

ό.έ.δ.

Έστω τώρα $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί του αλφαβήτου $\mathbb{F}$ με q το πλήθος στοιχεία. Το μέγεθος του $\mathcal{C}$ είναι ίσο με $M = q^k$ και για κάθε $\mathbf{x} \in \mathbb{F}^n$ το αντίστοιχο σύμπλοκο $\mathbf{x} + \mathcal{C}$ έχει τόσα στοιχεία όσα και ο κώδικας $\mathcal{C}$ (γιατί;). Επομένως, υπάρχουν q^{n-k} το πλήθος διαφορετικά σύμπλοκα ως προς τον κώδικα (υπόχωρο) $\mathcal{C}$.

Έστω $\mathcal{C} = \{\, \mathbf{c}_1 = \mathbf{0}, \mathbf{c}_2, \mathbf{c}_3, \ldots, \mathbf{c}_M \}$. Επιλέγουμε έναν αντιπρόσωπο $\mathbf{a}_2 \in \mathbb{F}^n$, έτσι ώστε να μην ανήκει στον κώδικα $\mathcal{C}$ και να έχει μικρότερο βάρος από όλα τα στοιχεία του $\mathcal{C}$.

Το σύμπλοκο $\mathbf{a}_2 + \mathcal{C} = \{\mathbf{a}_2 + \mathbf{0}, \mathbf{a}_2 + \mathbf{c}_2, \mathbf{a}_2 + \mathbf{c}_3, \ldots, \mathbf{a}_2 + \mathbf{c}_M\}$ είναι ξένο προς τον κώδικα. Κατόπιν, επιλέγουμε έναν αντιπρόσωπο $\mathbf{a}_3 \in \mathbb{F}^n$, έτσι ώστε να μην ανήκει στην ένωση $\mathcal{C} \cup (\mathbf{a}_2 + \mathcal{C})$ και να έχει μικρότερο βάρος από όλα τα στοιχεία του $\mathcal{C} \cup (\mathbf{a}_2 + \mathcal{C})$. Συνεχίζοντας την ίδια διακασία επιλέγουμε έναν αντιπρόσωπο $\mathbf{a}_{i+1} \in \mathbb{F}^n$, έτσι ώστε να μην ανήκει στην ένωση $\mathcal{C} \cup (\mathbf{a}_2 + \mathcal{C}) \cup (\mathbf{a}_3 + \mathcal{C}) \cup \cdots \cup (\mathbf{a}_i + \mathcal{C})$ και να έχει μικρότερο βάρος από όλα τα στοιχεια του $\mathcal{C} \cup (\mathbf{a}_2 + \mathcal{C}) \cup (\mathbf{a}_3 + \mathcal{C}) \cup \cdots \cup (\mathbf{a}_i + \mathcal{C})$. Τελικά, επιλέγουμε με την ίδια διαδικασία και τον τελευταίο αντιπρόσωπο $\mathbf{a}_r$, όπου $r = q^{n-k}$, οπότε το $\mathbb{F}^n$ γράφεται ως (διακεκριμένη) ένωση αυτών των συμπλόκων, δηλαδή $\mathbb{F}^n = \mathcal{C} \cup (\mathbf{a}_2 + \mathcal{C}) \cup (\mathbf{a}_3 + \mathcal{C}) \cup \cdots \cup (\mathbf{a}_r + \mathcal{C})$.

Σύμφωνα με την προηγούμενη διαδικασία τα στοιχεία του $\mathbb{F}^n$ θα μπορούσαν να *διευθετηθούν* σε έναν πίνακα:

$\mathbf{0}$	$\mathbf{c}_2$	$\mathbf{c}_3$	$\cdots$	$\mathbf{c}_M$
$\mathbf{a}_2 + \mathbf{0}$	$\mathbf{a}_2 + \mathbf{c}_2$	$\mathbf{a}_2 + \mathbf{c}_3$	$\cdots$	$\mathbf{a}_2 + \mathbf{c}_M$
$\mathbf{a}_3 + \mathbf{0}$	$\mathbf{a}_3 + \mathbf{c}_2$	$\mathbf{a}_3 + \mathbf{c}_3$	$\cdots$	$\mathbf{a}_3 + \mathbf{c}_M$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{a}_r + \mathbf{0}$	$\mathbf{a}_r + \mathbf{c}_2$	$\mathbf{a}_r + \mathbf{c}_3$	$\cdots$	$\mathbf{a}_r + \mathbf{c}_M$

Ο πίνακας αυτός θα ονομάζεται **αντιπροσωπευτική διάταξη** των στοιχείων του $\mathbb{F}^n$ ως προς τους αντιπροσώπους $\mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$.

Παρατηρήσεις 2.4.4. 1. Όπως βλέπουμε στον πίνακα, τα στοιχεία κάθε γραμμής (εκτός της πρώτης) είναι αθροίσματα των στοιχείων της πρώτης γραμμής με τον αντίστοιχο αντιπρόσωπο που βρίσκεται στην πρώτη

στήλη. Δηλαδή, όταν μια (κωδικο)λέξη $\mathbf{c}$ διατρέχει τα στοιχεία του κώδικα $\mathcal{C}$, τότε το στοιχείο $\mathbf{a}_i + \mathbf{c}$ διατρέχει τα στοιχεία της i γραμμής.

2. Μια αντιπροσωπευτική διάταξη **δεν** είναι μοναδική και εξαρτάται από την επιλογή των αντιπροσώπων. Η επιλογή αυτή έχει μεγάλη σημασία, όπως θα δούμε στα επόμενα, στη διόρθωση λαθών.

Παράδειγμα 2.4.5. Έστω $\mathcal{C}$ ο δυαδικός κώδικας $\{\,0000,\ 1011,\ 0110,\ 1101\,\}$. Μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{Z}_2^4$ είναι η εξής:

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Αν αντί του αντιπροσώπου 0100 επιλέξουμε τον αντιπρόσωπο 0010, τότε έχουμε την ακόλουθη αντιπροσωπευτική διάταξη:

0000	1011	0110	1101
1000	0011	1110	0101
0010	1001	0100	1111
0001	1010	0111	1100

Θεωρούμε τώρα ένα στοιχείο $\mathbf{x} \in \mathbb{F}^n$, το οποίο καταλαμβάνει μια θέση, έστω $i\,j$, στον παραπάνω πίνακα, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$. Ας υπολογίσουμε την ελάχιστη απόσταση του $\mathbf{x}$ από τα στοιχεία του κώδικα $\mathcal{C}$. Ως γνωστόν, ισχύει ότι $d(\mathbf{x},\, \mathbf{c}) = w(\mathbf{x} - \mathbf{c})$, επομένως:

$$\begin{aligned}\min\{d(\mathbf{x}, \mathbf{c}),\mathbf{c} \in \mathcal{C}\} &= \min\{w(\mathbf{x} - \mathbf{c}), \mathbf{c} \in \mathcal{C}\} \\ &= \min\{w((\mathbf{a}_i + \mathbf{c}_j) - \mathbf{c}), \mathbf{c} \in \mathcal{C}\} = \min\{w(\mathbf{a}_i + (\mathbf{c}_j - \mathbf{c})), \mathbf{c} \in \mathcal{C}\}.\end{aligned}$$

Αλλά ο κώδικας $\mathcal{C}$ είναι διανυσματικός υπόχωρος. Άρα, όταν η (κωδικο)λέξη $\mathbf{c}$ διατρέχει τα στοιχεία του $\mathcal{C}$, τότε και η (κωδικο)λέξη $\mathbf{c}_j - \mathbf{c}$ διατρέχει όλα τα στοιχεία του $\mathcal{C}$. Επομένως, συνεχίζοντας την προηγούμενη σχέση έχουμε:

$$\begin{aligned}\min\{w(\mathbf{a}_i + (\mathbf{c}_j - \mathbf{c})), \mathbf{c} \in \mathcal{C}\} &= \min\{w(\mathbf{a}_i + \mathbf{c}), \mathbf{c} \in \mathcal{C}\} = w(\mathbf{a}_i) \\ &= w(\mathbf{x} - \mathbf{c}_j) = d(\mathbf{x}, \mathbf{c}_j).\end{aligned}$$

Επομένως, έχουμε ότι:

$$\min\{\, d(\mathbf{x},\, \mathbf{c}),\ \mathbf{c} \in \mathcal{C}\,\} \;=\; d(\mathbf{x},\, \mathbf{c}_j).$$

Δηλαδή βλέπουμε ότι η λέξη $\mathbf{x}$ που βρίσκεται στην j στήλη του πίνακα απέχει την μικρότερη απόσταση από την (κωδικο)λέξη που βρίσκεται στην κορυφή της αντίστοιχης στήλης. Όλα τα παραπάνω συνοψίζονται στο ακόλουθο Θεώρημα

Θεώρημα 2.4.6. *Έστω $\mathcal{C}$ ένας $[n,\, k,\, d]$ κώδικας. Μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}^n$ μπορεί να χρησιμεύσει για την αποκωδικοποίηση σύμφωνα με την αρχή της πλησιέστερης λέξης.*

Απόδειξη. Έστω ότι έχει επιλεγεί μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}^n$ και έχει ληφθεί η λέξη $\mathbf{x} \in \mathbb{F}^n$. Υποθέτουμε ότι αυτή η λέξη καταλαμβάνει την $i\,j$ θέση στον πίνακα, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$, ορίζουμε την συνάρτηση αποκωδικοποίησης ως εξής $\varphi : \mathbb{F}^n \longrightarrow \mathcal{C}$ με $\varphi(\mathbf{x}) = \mathbf{c}_j$. ό.έ.δ.

Παρατήρηση 2.4.7. Ο τρόπος κατασκευής μιας αντιπροσωπευτικής διάταξης, που περιγράψαμε προηγουμένως, μας εξασφαλίζει ότι η αποκωδικοποίηση που επιτυγχάνεται μέσω αυτής είναι πάντα πλήρης (ιδέ Παρατήρηση 1.3.7). Αυτό **δεν** σημαίνει ότι πάντα η αποκωδικοποίηση είναι σωστή.

Ενδέχεται να έχει σταλεί η (κωδικο)λέξη $\mathbf{c}_m$ και να έχει ληφθεί η λέξη $\mathbf{x}$, η οποία βρίσκεται στην $i\,j$ θέση στον πίνακα με $j \neq m$, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$. Σ' αυτή την περίπτωση, η ληφθείσα λέξη θα αποκωδικοποιηθεί (λανθασμένα) ως $\mathbf{c}_j$ και **όχι** ως $\mathbf{c}_m$. Συγκεκριμένα μια λέξη $\mathbf{x}$ αποκωδικοποιείται σωστά αν και μόνο αν το διάνυσμα λάθους που (πιθανόν) παρεισέφρησε είναι ένας από τους αντιπροσώπους που χρησιμοποίηθηκαν στη δημιουργία της αντιπροσωπευτικής διάταξης. Δηλαδή αν $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$, τότε η αποκωδικοποίηση είναι σωστή, αν και μόνο αν ο *θόρυβος* που υπεισήλθε είναι το διανύσμα $\mathbf{a}_i$.

Παράδειγμα 2.4.8. Έστω ο κώδικας $\mathcal{C} = \{\, 0000,\, 1011,\, 0110,\, 1101\,\}$ του προηγουμένου παραδείγματος. Υποθέτουμε ότι αποστέλλεται η λέξη 0110 και λαμβάνουμε τη λέξη 0100. Η λέξη αυτή ισαπέχει από τις λέξεις του κώδικα 0000 και 0110 απόσταση ίση με ένα. Αν αρκεσθούμε γενικά στην αποκωδικοποίηση

σύμφωνα με την αρχή της πλησιέστερης λέξης, τότε είμαστε αναγκασμένοι να δηλώσουμε *αμηχανία*. Αν χρησιμοποιήσουμε την αντιπροσωπευτική διάταξη που παριστάνεται στον πρώτο πίνακα, τότε αποκωδικοποιούμε λανθασμένα ως 0000. Αν όμως χρησιμοποιήσουμε την αντιπροσωπευτική διάταξη που παριστάνεται στον δεύτερο πίνακα, τότε αποκωδικοποιούμε σωστά ως 0110.

Παρατήρηση 2.4.9. Μπορείτε να αποδείξετε ότι η μόνη περίπτωση, όπου η αποκωδικοποίηση με τη βοήθεια μιας αντιπροσωπευτικής διάταξης ενδέχεται να είναι λανθασμένη, είναι όταν γενικά στην αποκωδικοποίηση σύμφωνα με την αρχή της πλησιέστερης λέξης είμαστε αναγκασμένοι να δηλώσουμε *αμηχανία*. Δηλαδή όταν σε μια γραμμή του πίνακα μιας αντιπροσωπευτικής διάταξης υπάρχουν δύο (τουλάχιστον) λέξεις με το ίδιο βάρος.

Δεδομένου ότι ένας κώδικας με ελάχιστη απόσταση ίση με d διορθώνει μέχρι $\lambda \leq [(d-1)/2]$ το πλήθος λάθη, σε έναν $[n,\, k,\, d]$ γραμμικό κώδικα όταν λαμβάνουμε μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}^n$, πρέπει (να φροντίζουμε) όλες οι λέξεις με βάρος το πολύ $w = [(d-1)/2]$ να λαμβάνονται ως αντιπρόσωποι. Αυτό βεβαίως δεν σημαίνει ότι δεν υπάρχουν και άλλοι αντιπρόσωποι. Στην περίπτωση όμως ενός τέλειου γραμμικού κώδικα, όλοι οι αντιπρόσωποι είναι ακριβώς όλες οι λέξεις με βάρος μικρότερο ή ίσον με $[(d-1)/2]$ (γιατί;).

2.4.2 Η πιθανότητα σωστής αποκωδικοποίησης με έναν γραμμικό κώδικα

Έστω $\mathcal{C}$ ένας $[n,\, k,\, d]$ γραμμικός κώδικας. Στην παράγραφο 1.3.1 είδαμε ότι η (δεσμευμένη) πιθανότητα $p(\mathbf{c} \mid \mathbf{c}) =$ *η πιθανότητα σωστής αποκωδικοποίησης, δεδομένου ότι εστάλη η λέξη* $\mathbf{c}$, είναι ίση με το άθροισμα όλων των πιθανοτήτων $p($ *ελήφθη η λέξη* $\mathbf{x} \mid$ *εστάλη η λέξη* $\mathbf{c})$, όπου το $\mathbf{x}$ διατρέχει όλες τις λέξεις στο $\mathbb{F}^n$ που ικανοποιούν τη σχέση $\varphi(\mathbf{x}) = c$. Δηλαδή:

$$p(\mathbf{c} \mid \mathbf{c}) = \sum_{x \in \varphi^{-1}(\mathbf{c})} p(\textit{ ελήφθη η λέξη } \mathbf{x} \mid \textit{ εστάλη η λέξη } \mathbf{c}).$$

Έστω ότι για την αποκωδικοποίηση έχουμε επιλέξει μια αντιπροσωπευτική διάταξη με αντιπροσώπους $\mathbf{a}_1 = \mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$. Όπως είδαμε η συνάρτηση

αποκωδικοποίησης ορίζεται για $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$ ως $\varphi(\mathbf{a}_i + \mathbf{c}_j) = \mathbf{c}_j$. Επομένως, έχουμε $p(\mathbf{c} \mid \mathbf{c}) = \sum_{i=1}^{r} p(\textit{παρεισέφρησε το } \mathbf{a}_i \textit{ ως λάθος})$. Άρα, το πρόβλημα ανάγεται στον υπολογισμό της πιθανότητας ένας από τους αντιπροσώπους που επιλέξαμε να παρεισφρήσει ως διάνυσμα λάθους.

Για τον υπολογισμό της πιθανότητας $p(\textit{ παρεισέφρησε το } \mathbf{a}_i \textit{ ως λάθος })$ θα περιορισθούμε στην μερική περίπτωση ενός δυαδικού κώδικα, όπου η μετάδοση των μηνυμάτων γίνεται μέσω ενός αμνήμονος συμμετρικού διαύλου επικοινωνίας και όπου η πιθανότητα λανθασμένης μετάδοσης ενός χαρακτήρα είναι ίση με p. Έστω $w(\mathbf{a}_i)$ το βάρος του $\mathbf{a}_i$. Το ότι ο $\mathbf{a}_i$ παρεισφρέει ως λάθος στην (κωδικο)λέξη $\mathbf{c}_j$ που αποστέλλεται, σημαίνει ότι λαμβάνουμε τη λέξη $\mathbf{a}_i + \mathbf{c}_j$, επομένως *αλλοιώνονται* οι χαρακτήρες στις αντίστοιχες θέσεις που η λέξη $\mathbf{a}_i$ έχει 1. Άρα, έχουμε $p(\textit{ παρεισέφρησε το } \mathbf{a}_i \textit{ ως λάθος }) = p^{w(\mathbf{a}_i)}(1-p)^{n-w(\mathbf{a}_i)}$, οπότε αντικαθιστώντας στην προηγούμενη σχέση έχουμε $p(\mathbf{c} \mid \mathbf{c}) = \sum_{i=1}^{r} p^{w(\mathbf{a}_i)}(1-p)^{n-w(\mathbf{a}_i)}$.

Θα μπορούσαμε διαφορετικά να υπολογίσουμε την πιθανότητα σωστής αποκωδικοποίησης ως εξής; Έχουμε δει (σελ. 16) ότι η πιθανότητα να *αλλοιωθούν* k το πλήθος χαρακτήρες είναι ίση με $p^k(1-p)^{n-k}$. Αν α_k παριστά το πλήθος των αντιπροσώπων με βάρος k, τότε προφανώς έχουμε:

$$p(\mathbf{c} \mid \mathbf{c}) = \sum_{k=1}^{n} \alpha_k p^k (1-p)^{n-k}.$$

Επομένως, έχουμε αποδείξει το επόμενο θεώρημα.

Θεώρημα 2.4.10. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ δυαδικός γραμμικός κώδικας. Υποθέτουμε ότι έχουμε επιλέξει μια αντιπροσωπευτική διάταξη με αντιπροσώπους $\mathbf{a}_1 = \mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$. Τότε η πιθανότητα σωστής αποκωδικοποίησης είναι ίση με:*

$$p(\mathbf{c} \mid \mathbf{c}) = \sum_{i=1}^{r} p^{w(\mathbf{a}_i)}(1-p)^{n-w(\mathbf{a}_i)} = \sum_{k=1}^{n} \alpha_k p^k (1-p)^{n-k}.$$

Παράδειγμα 2.4.11. Έστω $\mathcal{C}$ ο δυαδικός κώδικας $\{0000, 1011, 0110, 1101\}$ του Παραδείγματος 2.4.5 με την ακόλουθη αντιπροσωπευτική διάταξη των

στοιχείων του $\mathbb{Z}_2^4$.

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Παρατηρούμε ότι $\alpha_0 = 1, \alpha_1 = 3, \alpha_2 = \alpha_3 = \alpha_4 = 0$, επομένως έχουμε $p(\mathbf{c} \mid \mathbf{c}) = (1-p)^4 + 3p(1-p)^3$. Αν, για παράδειγμα, έχουμε $p = 0.01$, τότε έχουμε $p(\mathbf{c} \mid \mathbf{c}) \approx 0.9897$. Επειδή το μέγεθος του κώδικα είναι τέσσερα, θα μπορούσαμε να υποθέσουμε ότι η πηγή είναι το σύνολο $\mathbb{Z}_2^2 = \{00, 01, 10, 11\}$ και τα στοιχεία της κωδικοποιούνται μεσω μιας συνάρτησης κωδικοποίησης $f : \mathbb{Z}_2^2 \longrightarrow \mathcal{C}$.

Υποθέτουμε τώρα ότι το σύνολο $\mathbb{Z}_2^2$ (η πηγή) θεωρείται και κώδικας (στην πραγματικότητα εδώ η συνάρτηση κωδικοποίησης είναι η ταυτοτική συνάρτηση), οπότε (στην πραγματικότητα) το μήνυμα αποστέλλεται μη κωδικοποιημένο. Στην περίπτωση αυτή, η πιθανότητα σωστής αποκωδικοποίησης είναι ίση με $p(\mathbf{c} \mid \mathbf{c}) = (1-p)^2 = 0.9801$ (γιατί;), η οποία, όπως ήταν αναμενόμενο, είναι μικρότερη από την πιθανότητα σωστής αποκωδικοποίησης αν χρησιμοποιήσουμε τον κώδικα.

Εδώ θα θέλαμε να τονίσουμε, για άλλη μια φορά, το *κόστος* που επιφέρει η απαίτηση να αυξήσουμε την πιθανότητα σωστής αποκωδικοποίησης, καθότι την πρώτη φορά μεταδίδουμε λέξεις με τέσσερεις χαρακτήρες, ενώ τη δεύτερη λέξεις με δύο χαρακτήρες.

Ο προσδιορισμός, στο προηγούμενο θεώρημα, του πλήθους α_k των αντιπροσώπων βάρους k είναι πολύ δύσκολο να υπολογιστεί γενικά, μάλιστα υπάρχουν σημαντικές κατηγορίες κωδίκων, που τα αντίστοιχα α_k είναι άγνωστα. Στην περίπτωση όμως ενός τέλειου κώδικα τα α_k είναι εύκολο να υπολογισθούν. Πράγματι, στο τέλος της προηγουμένης παραγράφου είχαμε επισημάνει ότι στην περίπτωση ένος τέλειου γραμμικού κώδικα όλοι οι αντιπρόσωποι είναι ακριβώς όλες οι λέξεις με βάρος μικρότερο ή ίσον με $t = [(d-1)/2]$. Αλλά στο σύνολο $\mathbb{Z}_2^n$ υπάρχουν $\binom{n}{k}$ το πλήθος λέξεις βάρους k, επομένως έχουμε $\alpha_k = \binom{n}{k}$ για $0 \leq k \leq [(d-1)/2]$ και $\alpha_k = 0$ για $[(d-1)/2] < k \leq n$.

Συνεπώς, έχουμε:

Θεώρημα 2.4.12. *Σε έναν τέλειο* $[n, k, d]$ *δυαδικό γραμμικό κώδικα* $\mathcal{C}$ *η πιθανότητα σωστής αποκωδικοποίησης με μια αντιπροσωπευτική διάταξη είναι ίση με* $p(\mathbf{c} \mid \mathbf{c}) = \sum_{k=0}^{t} \binom{n}{k} p^k (1-p)^{n-k}$.

Παρατήρηση 2.4.13. Οι ισότητες στα δύο προηγούμενα θεωρήματα για την πιθανότητα σωστής αποκωδικοποίησης συνάδουν με τις ανισότητες στη σελίδα 53.

2.4.3 Ανίχνευση λαθών με έναν γραμμικό κώδικα

Υποθέτουμε ότι έχουμε έναν γραμμικό κώδικα $\mathcal{C}$ με παραμέτρους $[n, k, d]$, τον οποίο χρησιμοποιούμε (μόνο) για ανίχνευση λαθών.

Έστω ότι εστάλη η (κωδικο)λέξη $\mathbf{a}$, αλλά ελήφθη η λέξη $\mathbf{x}$. Αν υπεισήλθε λάθος, αυτό θα διαφύγει της προσοχής μας, αν και μόνο αν η $\mathbf{x} \in \mathcal{C}$. Ο κώδικας όμως είναι γραμμικός. Άρα, το λάθος $\mathbf{e} = \mathbf{x} - \mathbf{a}$ δεν ανιχνεύται, αν και μόνο αν $\mathbf{e} \in \mathcal{C}$.

Αν θέλουμε να υπολογίσουμε την πιθανότητα **μη** ανίχνευσης λαθών, θα πρέπει να υπολογίσουμε την πιθανότητα σε κάθε (κωδικο)λέξη να επέλθουν τόσες αλλοιώσεις, έτσι ώστε να προκύψει μια άλλη (κωδικο)λέξη και μετά να αθροίσουμε. Στη μερική περίπτωση ενός δυαδικού κώδικα, όπου η μετάδοση των μηνυμάτων γίνεται μέσω ενός αμνήμονος συμμετρικού διαύλου επικοινωνίας, όπου η πιθανότητα λανθασμένης μετάδοσης ενός χαρακτήρα είναι ίση με p, έχουμε το επόμενο θεώρημα.

Θεώρημα 2.4.14. *Έστω* $\mathcal{C}$ *ένας δυαδικός γραμμικός κώδικας με παραμέτρους* $[n, k, d]$. *Με* A_i *συμβολίζουμε το πλήθος των στοιχείων του* $\mathcal{C}$ *που έχουν βάρος ίσο με* i.

Η πιθανότητα $p($ μη ανίχνευσης λαθών $)$ *εξαρτάται μόνο από τον κώδικα και τον δίαυλο επικοινωνίας και είναι ίση με* $p($ μη ανίχνευσης λαθών $) = \sum_{i=1}^{n} A_i \cdot p^i \cdot (1-p)^{n-i}$.

Απόδειξη. Όπως γνωρίζουμε (ιδέ σελίδα 16) η πιθανότητα να *αλλοιωθούν* i το πλήθος χαρακτήρες είναι ίση με $p^i(1-p)^{n-i}$. Προηγουμένως, είδαμε

ότι ένα λάθος δεν ανιχνεύεται αν και μόνο αν είναι στοιχείο του κώδικα $\mathcal{C}$. Θεωρούμε ότι κάθε μη μηδενική (κωδικο)λέξη βάρους i προέρχεται από αλλοίωση i το πλήθος χαρακτήρων της μηδενικής λέξης. Επομένως, εύκολα έπεται το αποτέλεσμα. ό.έ.δ.

Παράδειγμα 2.4.15. Έστω $\mathcal{C}$ ο δυαδικός κώδικας $\{0000, 1011, 0110, 1101\}$ του Παραδείγματος 2.4.11. Παρατηρούμε ότι $A_1 = 0, A_2 = 1, A_3 = 2, A_4 = 0$. Επομένως, έχουμε $p(\textit{μη ανίχνευσης λαθών}) = \sum_{i=1}^{4} A_i \cdot p^i \cdot (1-p)^{n-i} = p^2(1-p)^2 + 2p^3(1-p) = p^2 - p^4$. Αν, για παράδειγμα, έχουμε $p = 0.01$, τότε έχουμε $p(\textit{μη ανίχνευσης λαθών}) = 0.00009999$.

Παρατηρήσεις 2.4.16.

1. Αν συγκρίνουμε τα αποτελέσματα στα δύο Παραδείγματα 2.4.5 και 2.4.11, βλέπουμε ότι η πιθανότητα μη σωστής αποκωδικοποίησης είναι ίση με $1 - p(\mathbf{c} \mid \mathbf{c}) \approx 1 - 0.9897 = 0,0103$, ενώ η $p(\textit{μη ανίχνευσης λαθών}) = 0.00009999$. Αυτό είναι αναμενόμενο, διότι αν εφαρμόσουμε την αρχή αποκωδικοποίησης ως προς τη πλησιέστερη λέξη, τότε ενδέχεται μια ληφθείσα λέξη να αποκωδικοποιθεί λανθασμένα.

2. Στο προηγούμενο άθροισμα $\sum_{i=1}^{n} A_i \cdot p^i \cdot (1-p)^{n-i}$ οι παράγοντες A_i είναι δύσκολο να υπολογισθούν στη γενική περίπτωση. Το πρόβλημα υπολογισμού των A_i παρουσιάζει μεγάλο θεωρητικό και πρακτικό ενδιαφέρον. Μια πρώτη προσέγγιση θα επιχειρήσουμε στην Παράγραφο 2.5 .

2.4.4 Το σύνδρομο σε έναν γραμμικό κώδικα

Η αποκωδικοποίηση με τη βοήθεια μιας αντιπροσωπευτικής διάταξης παρουσιάζει εγγενείς δυσκολίες, καθότι (ιδίως όταν το μήκος n του κώδικα είναι μεγάλο) χρειάζεται αρκετός χρόνος να εντοπιστεί η θέση μιας λέξης που λαμβάνεται, ούτως ώστε να αποκωδικοποιηθεί ως η λέξη που βρίσκεται στην κορυφή της στήλης στην οποία βρίσκεται. Όπως θα δούμε μπορούμε να συντομεύσουμε δραστικά την παραπάνω διαδικασία.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και P ένας $s \times n$ πίνακας ελέγχου ισοτιμίας του $\mathcal{C}$. Για $\mathbf{x} \in \mathbb{F}^n$ το στοιχείο $\mathbf{x}\mathrm{P}^t$ θα λέγεται το **σύνδρομο** του $\mathbf{x}$.

Ως γνωστόν, ο πίνακας P^t ορίζει μια γραμμική απεικόνιση $h : \mathbb{F}^n \longrightarrow \mathbb{F}^s$ με $h(\mathbf{x}) = \mathbf{x}\mathrm{P}^t$, δηλαδή το σύνδρομο του $\mathbf{x}$ είναι η εικόνα του μέσω της γραμμικής απεικόνισης h.

Από τον ορισμό του πίνακα ελέγχου ισοτιμίας (Ορισμός 2.2.10) για τον κώδικα $\mathcal{C}$ έχουμε $\mathcal{C} = \{\, \mathbf{c} \in \mathbb{F}^n \mid \mathbf{c}\mathrm{P}^t = \mathbf{0} \,\}$, δηλαδή ο κώδικας είναι ο πυρήνας της γραμμικής απεικόνισης h.

Πρόταση 2.4.17. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας και P ένας $s \times n$ πίνακας ελέγχου ισοτιμίας του. Δύο στοιχεία του $\mathbf{x}, \mathbf{y} \in \mathbb{F}^n$ έχουν το ίδιο σύνδρομο, αν και μόνο αν τα αντίστοιχα σύμπλοκα ως προς τον $\mathcal{C}$ είναι ίσα.*

Απόδειξη. Η απόδειξη είναι άμεση, καθότι η απεικόνιση h είναι γραμμική και ο πυρήνας της αποτελείται από τα στοιχεία του κώδικα $\mathcal{C}$.

Διαφορετικά θα μπορούσαμε να πούμε ότι $\mathbf{x} + \mathcal{C} = \mathbf{y} + \mathcal{C}$, αν και μόνο αν (από το Θεώρημα 2.4.2) $\mathbf{x} - \mathbf{y} \in \mathcal{C}$, αν και μόνο αν $(\mathbf{x} - \mathbf{y})\mathrm{P}^t = \mathbf{0}$ (από τον ορισμό του πίνακα ελεγχου ισοτιμίας), αν και μόνο αν $\mathbf{x}\mathrm{P}^t = \mathbf{y}\mathrm{P}^t$. ό.έ.δ.

Από την προηγούμενη πρόταση βλέπουμε ότι υπάρχει μια ένα προς ένα και επί αντιστοιχία μεταξύ των συμπλόκων του κώδικα και των συνδρόμων.

Έστω τώρα μια αντιπροσωπευτική διάταξη των στοιχείων του $\mathbb{F}^n$ ως προς τους αντιπροσώπους $\mathbf{0}, \mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_r$. Υποθέτουμε ότι ελήφθη η λέξη $\mathbf{x}$, η οποία καταλαμβάνει μια θέση, έστω $i\,j$, στον πίνακα της αντιπροσωπευτικής διάταξης, δηλαδή $\mathbf{x} = \mathbf{a}_i + \mathbf{c}_j$. Σύμφωνα με τα προηγούμενα, η λέξη θα αποκωδικοποιηθεί ως η (κωδικο)λέξη $\mathbf{c}_j = \mathbf{x} - \mathbf{a}_i$. Επομένως, το πρόβλημα είναι να εντοπιστεί ο αντιπρόσωπος $\mathbf{a}_i$. Από την προηγούμενη πρόταση όμως έχουμε ότι η λέξη $\mathbf{x}$ και ο αντιπρόσωπος $\mathbf{a}_i$ έχουν το ίδιο σύνδρομο. Επομένως, αν γνωρίζουμε τα σύνδρομα των αντιπροσώπων, μπορούμε εύκολα να προχωρήσουμε στην αποκωδικοποίηση σύμφωνα με τον ακόλουθο αλγόριθμο.

Επισυνάπτουμε (προσωρινά) στην αντιπροσωπευτική διάταξη μια επιπλέον στήλη υπολογίζοντας τα σύνδρομα των αντιπροσώπων. Όταν λαμβάνουμε μια λέξη, υπολογίζουμε το σύνδρομό της και το συγκρίνουμε με τα σύνδρομα των αντιπροσώπων. Με αυτό τον τρόπο εντοπίζουμε τον αντίστοιχο

αντιπρόσωπο και αποκωδικοποιούμε αφαιρώντας από τη λέξη που λάβαμε τον αντιπρόσωπο που εντοπίσαμε.

Όπως βλέπουμε για την αποκωδικοποίηση πλέον **δεν** χρειαζόμαστε όλη την αντιπροσωπευτική διάταξη, αλλά μόνο δύο στήλες, την στήλη των αντιπροσώπων και την στήλη των αντίστοιχων συνδρόμων.

Παρατήρηση 2.4.18. Όπως έχουμε επισημάνει (ιδέ Παρατηρήσεις 2.4.4, 2.4.7 και 2.4.9), η επιλογή των αντιπροσώπων των συμπλόκων σε μια αντιπροσωπευτική διάταξη έχει μεγάλη σημασία για σωστή αποκωδικοποίηση. Μάλιστα δε, η επιλογή αντιπροσώπων από κάθε σύμπλοκο ενός αντιπροσώπου με το μικρότερο δυνατόν βάρος αυξάνει την πιθανότητα σωστής αποκωδικοποίησης (ιδέ Θεώρημα 2.4.10). Επομένως, στον προηγούμενο αλγόριθμο θα πρέπει να έχουμε επιλέξει αντιπροσώπους με το μικρότερο δυνατόν βάρος. Αυτό (θεωρητικά) γίνεται ως εξής: Δεν επιλέγουμε αντιπροσώπους από την αρχή. Όταν λαμβάνουμε μια λέξη $\mathbf{x} \in \mathbb{F}^n$, υπολογίζουμε το σύνδρομό της $\mathbf{s} = \mathbf{x}\mathrm{P}^t$. Κατόπιν, *αναζητούμε* μια λέξη $\mathbf{e} \in \mathbb{F}^n$ ελαχίστου βάρους με την ιδιότητα $\mathbf{s} = \mathbf{e}\mathrm{P}^t$. Η λέξη αυτή είναι ο *πιθανότερος* αντιπρόσωπος του συμπλόκου, στο οποίο ανήκει η ληφθείσα λέξη $\mathbf{x}$. Δηλαδή το (πιθανόν) λάθος που παρεισέφρησε.

Το πρόβλημα της αναζήτησης μιας λέξης $\mathbf{e} \in \mathbb{F}^n$ με την παραπάνω ιδιότητα στην πραγματικότητα είναι ισοδύναμο με το πρόβλημα αναζήτησης του ελαχίστου πλήθους γραμμών του πίνακα P, οι οποίες, ως διανύσματα του χώρου $\mathbb{F}^n$, παράγουν έναν υπόχωρο, στον οποίον ανήκει το (γνωστό) σύνδρομο $\mathbf{s}$.

Το πρόβλημα αυτό είναι ένα υπολογιστικά δύσκολο πρόβλημα, για ένα τυχαίο $\mathbf{s} \in \mathbb{F}^n$ και έναν τυχαίο πίνακα P. Οπότε στην πράξη καταφεύγουμε σε άλλες μεθόδους ανάλογα με την δομή του κώδικα που χρησιμοποιούμε (ιδέ για παράδειγμα την αποκωδικοποίηση με κυκλικούς κώδικες στην Παράγραφο 3.2.4).

Παραδείγματα 2.4.19. 1. Έστω ο δυαδικός κώδικας:

$$\mathcal{C} = \{0000, 1011, 0110, 1101\}$$

του Παραδείγματος 2.4.5 με την αντιπροσωπευτική διάταξη των στοι-

χείων του $\mathbb{Z}_2^4$

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Ένας πίνακας ελέγχου ισοτιμίας είναι ο:

$$\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad \text{(γιατί;)}$$

Υπολογίζουμε τα σύνδρομα των αντιπροσώπων (δηλαδή τα σύνδρομα των στοιχείων της πρώτης στήλης).

$$(0\,0\,0\,0)\mathrm{P}^t = (0\,0), \qquad (1\,0\,0\,0)\mathrm{P}^t = (1\,1), \qquad (0\,1\,0\,0)\mathrm{P}^t = (1\,0),$$
$$(0\,0\,0\,1)\mathrm{P}^t = (0\,1).$$

Υποθέτουμε ότι λαμβάνουμε τη λέξη $0\,1\,1\,1$. Αν θέλαμε να χρησιμοποιήσουμε την παραπάνω αντιπροσωπευτική διάταξη, θα έπρεπε να εντοπίσουμε τη θέση της και κατά τα γνωστά να την αποκωδικοποιήσουμε. Τώρα υπολογίζουμε το σύνδρομό της $(0\,1\,1\,1)\mathrm{P}^t = (0\,1)$ και βλέπουμε ότι είναι το ίδιο με το σύνδρομο του αντιπροσώπου $0\,0\,0\,1$. Επομένως, σύμφωνα με τον προηγούμενο αλγόριθμο αποκωδικοποιούμε ως $0\,1\,1\,1 - 0\,0\,0\,1 = 0\,1\,1\,0 \in \mathcal{C}$. Δηλαδή για την αποκωδικοποίηση αντί του προηγουμένου πίνακα είναι αρκετός ο πίνακας:

0000	00
1000	11
0100	10
0001	01

ο οποίος έχει μόνο δύο στήλες.

2. Θεωρούμε τον γραμμικό κώδικα $\mathcal{D}$ επί του $\mathbb{Z}_{11}$ με πίνακα ελέγχου ισοτιμίας τον:

$$\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

Ο κώδικας αυτός είναι ένας $[10, 8]$ κώδικας και στο Παράδειγμα 2.2.26 είχαμε υπολογίσει ότι η ελάχιστη απόστασή του είναι ίση με τρία. Επομένως, διορθώνει ένα λάθος. Θα δούμε ότι ο κώδικας αυτός έχει μια επιπλέον ιδιότητα. Ταυτόχρονα με την διόρθωση ενός λάθους μπορεί να ανιχνεύει την ύπαρξη δύο λαθών, τα οποία προέρχονται από την αντιμετάθεση δύο χαρακτήρων κατά τη μετάδοση μιας (κωδικο)λέξης.

Έστω ότι εστάλη η (κωδικο)λέξη $\mathbf{a} = a_1\, a_2 \cdots a_{10}$, αλλά ελήφθη η λέξη $\mathbf{x} = x_1\, x_2 \cdots x_{10}$, στην οποία σε μια θέση υπεισήλθε ένα λάθος. Δηλαδή $\mathbf{x} = x_1\, x_2 \cdots x_{10} = a_1\, a_2 \cdots (a_j + k), \cdots a_{10}$.

Υπολογίζουμε το σύνδρομο της λέξης $\mathbf{x}$. Δηλαδή:

$$\begin{aligned}\mathbf{x} \cdot \mathrm{P}^{\perp} &= (\sum_{1}^{10} x_i, \sum_{1}^{10} i x_i) = (\sum_{1}^{10} a_i + k, \sum_{1}^{10} i a_i + jk) = \\ &= (k \mod 11, jk \mod 11).\end{aligned}$$

Οπότε μπορούμε όχι μόνο να διορθώσουμε το λάθος, αλλά επιπλέον να εντοπίσουμε τη θέση στην οποία υπεισήλθε το λάθος, καθώς και το μέγεθος του χαρακτήρα k που προκάλεσε την αλλοίωση.

Αν κατά τη μετάδοση της λέξης επήλθε αναγραμματισμός και δύο χαρακτήρες έχουν αντιμετατεθεί στις θέσεις r και j, δηλαδή $x_r = a_j$ και $x_j = a_r$, τότε έχουμε:

$$\begin{aligned}\mathbf{x} \cdot \mathrm{P}^{\perp} &= (\sum_{1}^{10} a_i, \sum_{i=1}^{10} i \cdot a_i) + (r - j)x_j + (j - r)x_r) \\ &= (0, (r - j)x_j + (j - r)x_r) = (0, (r - j)(x_j - x_r)).\end{aligned}$$

Στην τελευταία ισότητα βλέπουμε ότι η πρώτη συντεταγμένη είναι ίση με 0, η δεύτερη όμως συντεταγμένη ανιχνεύει ότι επήλθε αναγραμματισμός (ιδέ παρατηρήσεις μετά το Παράδειγμα 1.3.19).

Παρατηρήσεις 2.4.20. 1. Στο τελευταίο παράδειγμα ο κώδικας $\mathcal{D}$ είναι επί του $\mathbb{Z}_{11}$. Ενδιαφέρον παρουσιάζει ο *δεκαδικός* κώδικας $\mathcal{E}$, ο οποίος προέρχεται από σμίκρυνση του κώδικα $\mathcal{D}$ αν διαγράψουμε όλες τις (κωδικο)λέξεις στις οποίες εμφανίζεται ο χαρακτήρας '10' (κάτι ανάλογο

είχαμε κάνει για τον σχηματισμό του κώδικα ISBN). Ο κώδικας $\mathcal{E}$ ως υποκώδικας του $\mathcal{D}$ έχει ελάχιστη απόσταση (τουλάχιστον) ίση με τρία και για κάθε $\mathbf{a} \in \mathcal{E}$ ικανοποιούνται οι εξισώσεις ισοτιμίας $\mathbf{a}\cdot \mathrm{P}^{\perp} = (0,0)$, όπου φυσικά οι πράξεις εξακολουθούν να γίνονται $\bmod 11$.

Ο κώδικας $\mathcal{E}$ δεν είναι γραμμικός (γιατί;), είναι όμως αρκετά μεγάλος (ιδέ Άσκηση 1.5.3$_4$) και είχε χρησιμοποιηθεί στο παρελθόν για την κωδικοποίηση των αριθμών τηλεφώνων. Πράγματι, υποθέτουμε ότι οι δεκαψήφιοι αριθμοί τηλεφώνου σε μια χώρα αποτελούν στοιχεία του κώδικα $\mathcal{E}$. Τότε, κατά την επιλογή ενός αριθμού κλήσης, αν γίνει λάθος σε ένα μόνο ψηφίο, ο αριθμός *διορθώνεται* αυτόματα και η κλήση κατευθύνεται στον παραλήπτη που πράγματι ήθελε ο αποστολέας. Αν κατά την επιλογή γίνει ένας αναγραμματισμός (σύνηθες φαινόμενο), τότε η κλήση δεν προωθείται και ο αποστολέας ειδοποιείται (π.χ. «ο αριθμός που καλείτε δεν αντιστοιχεί σε συνδρομητή») και επαναλαμβάνει την κλήση.

2. Ας δούμε συνοπτικά τους κώδικες που αναφέρονται στα Παραδείγματα 2.2.26 και 2.4.19$_2$. Όπως βλέπουμε, έχουμε τον 11-δικό κώδικα $\mathcal{C}$ με πίνακα ελέγχου ισοτιμίας τον $\mathrm{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$. Επισυνάπτοντας μια γραμμή στον πίνακα H λαμβάνουμε τον πίνακα:

$$\mathrm{P} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}.$$

Ο P είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{D}$, ο οποίος αποτελεί μια σμίκρυνση του κώδικα $\mathcal{C}$.

Με την ίδια διαδικασία θα μπορούσαμε να συνεχίσουμε την σμίκρυνση επισυνάπτοντας μια επιπλέον γραμμή στον πίνακα P και να πάρουμε τον πίνακα:

$$\mathrm{Q} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 \end{pmatrix},$$

ο οποίος αποτελεί τον πίνακα ελέγχου ισοτιμίας ενός ακόμη *μικρότερου*

κώδικα, έστω $\mathcal{F}$. Οπότε θα μπορούσαμε να συνεχίσουμε με την ίδια διαδικασία.

Οι κώδικες που αναφέρονται στην προηγούμενη παρατήρηση ανήκουν σε μια ευρεία και πολύ σημαντική οικογένεια κωδίκων, στους BCH κώδικες. Η ονομασία προέρχεται από τα αρχικά των R.C. Bose, D.K. Ray-Chaudhuri, A. Hocquenghem που τους ανακάλυψαν στα τέλη της δεκαετίας του '50 και στις αρχές της δεκαετίας του '60. Οι κώδικες αυτοί έχουν καλές ιδιότητες και παρουσιάζουν ευκολία στην αποκωδικοποίηση και διόρθωση λαθών. Το μεγάλο τους πλεονέκτημα όμως είναι ότι μπορούν να κατασκευασθούν (υπό ορισμένες προϋποθέσεις) ώστε να έχουν μια επιθυμητή ελάχιστη απόσταση. Είναι, όπως συνηθίζεται να λέγεται, κώδικες *προσχεδιασμένης* απόστασης.

Μια συστηματική μελέτη αυτών των κωδίκων θα επιχειρήσουμε στο Κεφάλαιο 5. Εδώ θα αρκεσθούμε στη γενίκευση των προηγούμενων παραδειγμάτων.

Έστω p ένας πρώτος αριθμός και d, n θετικοί ακέραιοι με $3 \leq d \leq n \leq p-1$ και $a_1, a_2, \ldots, a_n$ διακεκριμένα μη μηδενικά στοιχεία του $\mathbb{Z}_p$ (άνευ βλάβης μπορούμε να υποθέσουμε ότι $a_1 = 1, a_2 = 2, \ldots, a_n = n$), με τα οποία σχηματίζουμε τον πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ a_1^{d-2} & a_2^{d-2} & \cdots & a_n^{d-2} \end{pmatrix}.$$

Παρατηρούμε ότι κάθε $d-1$ το πλήθος στήλες του πίνακα αυτού σχηματίζουν έναν πίνακα Vandermonde.[7] Επομένως η τάξη του πίνακα είναι ίση με $d-1$.

Έστω $\mathcal{C}$ ο κώδικας με πίνακα ελέγχου ισοτιμίας τον πίνακα H. Η ελάχιστη απόσταση του κώδικα είναι ίση με d (Πρόταση 2.2.25), δηλαδή είναι ένας $[n, n-(d-1), d]$ γραμμικός κώδικας. Το μέγεθος του κώδικα αυτού είναι ίσο με $p^{n-(d-1)}$, που ικανοποιεί το φράγμα Singleton (Θεώρημα 1.5.21). Επομένως, έχουμε αποδείξει το ακόλουθο θεώρημα.

[7] Για τους πίνακες Vandermonde και τις ιδιότητές τους παραπέμπουμε σε οποιοδήποτε, έστω και στοιχειώδες, βιβλίο Γραμμικής Άλγεβρας, για παράδειγμα στο Herstein, I. N. [1990].

Θεώρημα 2.4.21. *Έστω p πρώτος αριθμός και d, n θετικοί ακέραιοι με $3 \leq d \leq n \leq p-1$. Τότε ισχύει $A_p(n,d) = p^{n-d+1}$.*

Παρατήρηση 2.4.22. Περισσότερα για γραμμικούς κώδικας που ικανοποιούν το φράγμα Singleton θα δούμε στην Παράγραφο 2.6.

2.4.5 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Να κατασκευάσετε μια αντιπροσωπευτική διάταξη για τον δυαδικό κώδικα με γεννήτορα πίνακα:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

   Αποκωδικοποιήστε τις λέξεις 111 και 100.

   Υπολογίστε την πιθανότητα σωστής αποκωδικοποιήσης, όταν η μετάδοση γίνεται μέσω ενός συμμετρικού δυαδικού δίαυλου επικοινωνίας με πιθανότητα (λανθαμένης) μετάδοσης ίση με p.

   Δώστε ένα παράδειγμα λέξης που περιέχει ένα λάθος και αποκωδικοποιείται λανθασμένα.

3. Να κατασκευάσετε μια αντιπροσωπευτική διάταξη για τον δυαδικό κώδικα με γεννήτορα πίνακα:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

   Αποκωδικοποιήστε τις λέξεις 11111, 00000 και 10110.

   Υπολογίστε την πιθανότητα σωστής αποκωδικοποιήσης, όταν η μετάδοση γίνεται μέσω ενός συμμετρικού δυαδικού δίαυλου επικοινωνίας με πιθανότητα (λανθαμένης) μετάδοσης ίση με p.

   Δώστε ένα παράδειγμα λέξης που περιέχει δύο λάθη και αποκωδικοποιείται λανθασμένα και ένα παράδειγμα λέξης που περιέχει δύο λάθη, αλλά αποκωδικοποιείται σωστά.

4. Στις δύο προηγούμενες ασκήσεις, αντί να χρησιμοποιήσετε μια αντιπροσωπευτική διάταξη, να χρησιμοποιήσετε το σύνδρομο.

5. Έστω ένας δυαδικός κώδικας με πίνακα ελέγχου ισοτιμίας H. Δείξτε ότι το σύνδρομο μιας λέξης που λαμβάνουμε ισούται με το άθροισμα εκείνων των στηλών του πίνακα H που αντιστοιχούν στις θέσεις, όπου επήλθε αλλοίωση χαρακτήρων.

6. Δείξτε ότι σε έναν γραμμικό κώδικα η ακτίνα κάλυψης είναι ίση με το μέγιστο βάρος ενός αντιπροσώπου σε μια αντιπροσωπευτική διάταξη.

7. Έστω ένας τριαδικός κώδικας με γεννήτορα πίνακα:

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}.$$

   Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας σε κανονική μορφή.

   Να αποκωδικοποιήσετε με τη βοήθεια του συνδρόμου τις λέξεις

   2121, 1201 και 2222.

8. Έστω ο κώδικας του Παραδείγματος 2.4.19$_2$. Με τη βοήθεια του συνδρόμου να αποκωδικοποιήσετε τις λέξεις 0617960587 και 9876543210.

2.5 Διασπορά βαρών σε έναν κώδικα

Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Με A_i θα συμβολίζουμε το πλήθος των (κωδικο)λέξεων, οι οποίες έχουν βάρος ίσο με i. Το σύνολο $\{ A_0, A_1, A_2, \dots, A_n \}$ ονομάζεται **διασπορά βαρών** του κώδικα $\mathcal{C}$. Προφανώς $A_0 = 1$ και $A_i = 0$ για $1 \leq i \leq d-1$. Επίσης, από τον ορισμό των A_i, έχουμε ότι $A_0 + A_1 + \cdots + A_n = q^n$.

Το πολυώνυμο $W_{\mathcal{C}}(z) = \sum_{i=0}^{n} A_i z^i$ ονομάζεται **απαριθμητής βάρους** για τον κώδικα $\mathcal{C}$. Προφανώς ισχύει:

$$W_{\mathcal{C}}(z) = \sum_{\mathbf{a} \in \mathcal{C}} z^{w(\mathbf{a})}.$$

Το πολυώνυμο $W_{\mathcal{C}}(z)$ ορισμένες φορές συναντάται *ομογενοποιημένο* με δύο μεταβλητές. Αντικαθιστούμε την μεταβλητή z με z/x και πολλαπλασιάζουμε με x^n και έχουμε $W^h_{\mathcal{C}}(z,x) = x^n W_{\mathcal{C}}(z/x) = \sum_{i=0}^{n} A_i x^{n-i} z^i$.

Μια απλή, αλλά σημαντική, παρατήρηση είναι ότι ισοδύναμοι κώδικες έχουν την ίδια διασπορά βαρών (γιατί;).

Το αντίστροφο δεν ισχύει, όπως μπορούμε να δούμε από το εξής παράδειγμα.

Παράδειγμα 2.5.1. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ οι δυαδικοί γραμμικοί κώδικες με αντίστοιχους γεννήτορες πίνακες:

$$\mathrm{G}_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{και} \quad \mathrm{G}_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Μπορούμε να δούμε ότι οι δύο κώδικες έχουν την ίδια διασπορά βαρών, Μάλιστα δε, και στους δύο κώδικες έχουμε $A_0 = A_6 = 1$ και $A_2 = A_4 = 3$.

Ο κώδικας $\mathcal{C}_1$ είναι αυτοδυϊκός, ενώ ο $\mathcal{C}_2$ δεν είναι αυτοδυϊκός (γιατί;). Επομένως, δεν είναι μεταθετικά ισοδύναμοι (ιδέ Άσκηση 2.3.3 $_6$).

Στην Παράγραφο 2.4.3 είχαμε δει (Θεώρημα 2.4.14) ότι η διασπορά βαρών ενός γραμμικού κώδικα είναι σημαντική στην πιθανότητα σωστής ανίχνευσης λαθών. Η μελέτη του απαριθμητή βάρους αναδεικνύει τη δομή ενός κώδικα ως διανυσματικού χώρου και *αποκαλύπτει* μια βαθύτερη σχέση ενός γραμμικού κώδικα με τον αντίστοιχο δυϊκό κώδικα, κάτι που δεν είναι προφανές από τον ορισμό της καθετότητας και δεν μπορούμε να το συνάγουμε από τον απευθείας υπολογισμό των A_i διατρέχοντας μία προς μία τις (κωδικο)λέξεις του κώδικα.

Το κύριο αποτέλεσμα σ' αυτή την κατεύθυνση είναι το Θεώρημα του MacWilliams. Εδώ θα δώσουμε μια απλή απόδειξη στην ειδική περίπτωση των δυαδικών κωδίκων. Πριν διατυπώσουμε και αποδείξουμε το αντίστοιχο θεώρημα, θα παραθέσουμε μερικά αποτελέσμα υπό μορφήν Λημμάτων, τα οποία από μόνα τους παρουσιάζουν ανεξάρτητο ενδιαφέρον.

Λήμμα 2.5.2. *Έστω $\mathcal{C}$ ένας δυαδικός $[n,k,d]$ κώδικας. Επιλέγουμε και*

σταθεροποιούμε ένα $\mathbf{y} \in \mathbb{Z}_2^n$ *με* $\mathbf{y} \notin \mathcal{C}^\perp$. *Το σύνολο* $A = \{\, \mathbf{x} \in \mathcal{C} \mid \langle \mathbf{x}, \mathbf{y} \rangle = 0 \,\}$ *είναι διανυσματικός υπόχωρος του* $\mathbb{Z}_2^n$ *διάστασης ίσης με* $k-1$.

Απόδειξη. Το αποτέλεσμα έπεται άμεσα από την Πρόταση 2.2.6 και το γεγονός ότι αν δύο στοιχεία $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ δεν ανήκουν στο σύνολο A, τότε $\mathbf{u}-\mathbf{v} \in A$ (πάντα υπάρχει τουλάχιστον ένα στοιχείο του κώδικα που δεν ανήκει στο A, αφού το $\mathbf{y} \notin \mathcal{C}^\perp$). ό.έ.δ.

Από το προηγούμενο λήμμα έπεται άμεσα ότι αν $\mathbf{y} \notin \mathcal{C}^\perp$, τότε ακριβώς τα μισά στοιχεία του κώδικα είναι κάθετα ως προς το $\mathbf{y}$.

Λήμμα 2.5.3. *Έστω* $\mathcal{C}$ *ένας δυαδικός* $[n, k, d]$ *κώδικας. Επιλέγουμε και σταθεροποιούμε ένα* $\mathbf{y} \in \mathbb{Z}_2^n$. *Τότε:*

$$\sum_{\mathbf{x} \in \mathcal{C}} (-1)^{\langle \mathbf{x}, \mathbf{y} \rangle} = \begin{cases} 2^k & \text{αν } \mathbf{y} \in \mathcal{C}^\perp \\ 0 & \text{αν } \mathbf{y} \notin \mathcal{C}^\perp \end{cases}.$$

Απόδειξη. Αν $\mathbf{y} \in \mathcal{C}^\perp$, τότε $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ για κάθε $\mathbf{x} \in \mathcal{C}$, οπότε έχουμε την πρώτη περίπτωση, αφού ο κώδικας περιέχει 2^k το πλήθος στοιχεία.

Υποθέτουμε ότι $\mathbf{y} \notin \mathcal{C}^\perp$. Όπως έχουμε παρατηρήσει, για τα μισά το πλήθος στοιχεία του κώδικα ισχύει $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, επομένως για τα υπόλοιπα μισά θα ισχύει $\langle \mathbf{x}, \mathbf{y} \rangle = 1$. Άρα, έχουμε την δεύτερη περίπτωση. ό.έ.δ.

Λήμμα 2.5.4. *Επιλέγουμε και σταθεροποιούμε ένα* $\mathbf{x} = x_1\, x_2 \cdots x_n \in \mathbb{Z}_2^n$. *Τότε τα πολυώνυμα* $\sum_{\mathbf{y} \in \mathbb{Z}_2^n} z^{w(\mathbf{y})} (-1)^{\langle \mathbf{x}, \mathbf{y} \rangle}$ *και* $(1-z)^{w(\mathbf{x})} (1+z)^{n-w(\mathbf{x})}$ *είναι ίσα.*

Απόδειξη. Για το τυχαίο $\mathbf{y} = y_1\, y_2 \cdots y_n \in \mathbb{Z}_2^n$ έχουμε:

$$w(\mathbf{y}) = y_1 + y_2 + \cdots + y_n \quad \text{και} \quad \langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Οπότε έχουμε:

$$\begin{aligned} \sum_{\mathbf{y} \in \mathbb{Z}_2^n} z^{w(\mathbf{y})} (-1)^{\langle \mathbf{x}, \mathbf{y} \rangle} &= \sum_{\mathbf{y} \in \mathbb{Z}_2^n} z^{y_1 + y_2 + \cdots + y_n} (-1)^{x_1 y_1 + x_2 y_2 + \cdots + x_n y_n} \\ &= \sum_{\mathbf{y} \in \mathbb{Z}_2^n} \Big(\prod_{i=1}^{n} z^{y_i} (-1)^{x_i y_i} \Big). \end{aligned}$$

Στο τελευταίο άθροισμα έχουμε 2^n το πλήθος προσθεταίους (τόσα είναι τα στοιχεία του $\mathbb{Z}_2^n$) και κάθε προσθεταίος είναι ένα γινόμενο με n το πλήθος όρους. Επίσης, οι εκθέτες y_i λαμβάνουν τις τιμές 0 και 1. Οπότε εύκολα βλέπουμε ότι το τελευταίο άθροισμα είναι ίσον με:

$$\prod_{i=1}^{n}(\sum_{j=0}^{1} z^j(-1)^{x_i j}) = \prod_{i=1}^{n}(1+z(-1)^{x_i}).$$

Στο τελευταίο γινόμενο οι όροι $1+z(-1)^{x_i}$ είναι της μορφής $1+z$ αν $x_i = 0$ και της μορφής $1-z$ αν $x_i = 1$. Το πλήθος των x_i, τα οποία ισούνται με 1 είναι όσο και το βάρος $w(\mathbf{x})$. Επομένως, μπορούμε να συνεχίσουμε και το τελευταίο γινόμενο γίνεται:

$$\prod_{i=1}^{n}(1+z(-1)^{x_i}) = (1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})}.$$

Δηλαδή αποδείξαμε την αποδεικτέα σχέση:

$$\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{\langle \mathbf{x},\, \mathbf{y}\rangle} = (1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})}. \qquad \text{ό.έ.δ.}$$

Θεώρημα 2.5.5. ***Η ταυτότητα MacWilliams***

Έστω $\mathcal{C}$ ένας δυαδικός $[n,\, k,\, d]$ κώδικας. Τότε ισχύει:

$$W_{\mathcal{C}^\perp}(z) = (\mid \mathcal{C} \mid)^{-1}(1+z)^n W_{\mathcal{C}}\Big(\frac{1-z}{1+z}\Big).$$

Απόδειξη. Από το προηγούμενο λήμμα έχουμε:

$$\begin{aligned}\sum_{\mathbf{x}\in\mathcal{C}}\left(\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{\langle \mathbf{x},\, \mathbf{y}\rangle}\right) &= \sum_{\mathbf{x}\in\mathcal{C}}(1-z)^{w(\mathbf{x})}(1+z)^{n-w(\mathbf{x})} \\ &= (1+z)^n \sum_{\mathbf{x}\in\mathcal{C}}\left(\frac{1-z}{1+z}\right)^{w(\mathbf{x})} \\ &= (1+z)^n W_{\mathcal{C}}\left(\frac{1-z}{1+z}\right).\end{aligned}$$

Θα υπολογίσουμε το προηγούμενο (διπλό) άθροισμα αλλάζοντας τη σειρά των προσθεταίων.

$$\sum_{\mathbf{x}\in\mathcal{C}}\left(\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{\langle \mathbf{x},\, \mathbf{y}\rangle}\right) = \sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}\left(\sum_{\mathbf{x}\in\mathcal{C}}(-1)^{\langle \mathbf{x},\, \mathbf{y}\rangle}\right).$$

Από το Λήμμα 2.5.3 έχουμε ότι το άθροισμα $\sum_{\mathbf{x}\in\mathcal{C}}(-1)^{\langle \mathbf{x},\, \mathbf{y}\rangle} = 2^k$ μόνο για τα $\mathbf{y} \in \mathcal{C}^{\perp}$, οπότε συνεχίζοντας έχουμε:

$$\sum_{\mathbf{x}\in\mathcal{C}} \left(\sum_{\mathbf{y}\in\mathbb{Z}_2^n} z^{w(\mathbf{y})}(-1)^{\langle \mathbf{x},\, \mathbf{y}\rangle} \right) = \sum_{\mathbf{y}\in\mathcal{C}^{\perp}} z^{w(\mathbf{y})} 2^k = 2^k W_{\mathcal{C}^{\perp}}(z).$$

Οπότε με απλή σύγκριση έπεται το αποτέλεσμα. ό.έ.δ.

Παρατηρήσεις 2.5.6.

1. Αλλάζοντας τον ρόλο του κώδικα $\mathcal{C}$ με τον δυϊκό του $\mathcal{C}^{\perp}$, για την προηγούμενη ισότητα έχουμε την εξής έκφραση:

$$W_{\mathcal{C}}(z) = \frac{1}{2^{n-k}}(1+z)^n W_{\mathcal{C}^{\perp}}\Big(\frac{1-z}{1+z}\Big) .$$

2. Η χρήση της ταυτότητας MacWilliams δεν προσφέρεται για τον άμεσο υπολογισμό του απαριθμητή βάρους ένος κώδικα. Συνήθως, όταν η διάσταση k του κώδικα είναι μικρή, μπορούμε να προχωρήσουμε στον απευθείας υπολογισμό των A_i διατρέχοντας μία προς μία τις (κωδικο)λέξεις του κώδικα. Όταν όμως η διάσταση είναι μεγάλη, η διάσταση $n-k$ του δυϊκού κώδικα είναι μικρή, οπότε η χρήση της ταυτότητας MacWilliams είναι απαραίτητη και αποτελεσματική.

3. Στη γενική περίπτωση, όπου έχουμε έναν γραμμικό $[n,\, k,\, d]$ κώδικα $\mathcal{C}$ επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία, η ταυτότητα MacWilliams έχει τη μορφή:

$$W_{\mathcal{C}^{\perp}}(z) = (\mid \mathcal{C} \mid)^{-1}[1+(q-1)z]^n W_{\mathcal{C}}\Big(\frac{1-z}{1+(q-1)z}\Big) .$$

   Για μια απόδειξη, με την χρήση χαρακτήρων, μπορείτε να ανατρέξετε στο βιβλίο Ron M. Roth [2006] (Θεώρημα 4.6, σελίδα 100).

4. Χρησιμοποιώντας τον ομογενοποιημένο τύπο για τον απαριθμητή βάρους μπορούμε να εκφράσουμε την ταυτότητα MacWilliams ως εξής:

$$W_{\mathcal{C}^{\perp}}(z) = (\mid \mathcal{C} \mid)^{-1} W^h_{\mathcal{C}}(1+(q-1)z, 1-z) .$$

5. Έστω $A_0^\perp, A_1^\perp, A_2^\perp, \ldots, A_n^\perp$ η διασπορά βαρών για τον δυϊκό κώδικα $\mathcal{C}^\perp$. Από την ταυτότητα MacWilliams έχουμε ότι:

$$W_{\mathcal{C}^\perp}(z) = \sum_{i=0}^{n} A_i^\perp z^i = (\mid \mathcal{C} \mid)^{-1}[1+(q-1)z]^n W_{\mathcal{C}}\Big(\frac{1-z}{1+(q-1)z}\Big)$$
$$= (\mid \mathcal{C} \mid)^{-1} \sum_{i=0}^{n} A_i (1+(q-1)z)^{n-i}(1-z)^i \ (*).$$

Από το διωνυμικό ανάπτυγμα εύκολα βλέπουμε ότι:

$$(1+(q-1)z)^{n-i}(1-z)^i = \sum_{\ell=0}^{n} \mathcal{K}_\ell(i) z^\ell,$$

όπου $\mathcal{K}_\ell(i) =: \mathcal{K}_\ell(i; n, q) = \sum_{r=0}^{\ell} \binom{i}{r}\binom{n-i}{\ell-r}(-1)^r (q-1)^{\ell-r}$.

Οπότε, αντικαθιστώντας στην προηγούμενη σχέση, έχουμε:

$$\sum_{i=0}^{n} A_i^\perp z^i = (\mid \mathcal{C} \mid)^{-1} \sum_{i=0}^{n} A_i \sum_{\ell=0}^{n} \mathcal{K}_\ell(i) z^\ell .$$

Στην τελευταία ισότητα και τα δύο μέλη είναι πολυώνυμα ως προς z, οπότε λαμβάνοντας την ισότητα των αντιστοίχων ομοβάθμιων όρων έχουμε ότι:

$$A_\ell^\perp = (\mid \mathcal{C} \mid)^{-1} \sum_{i=0}^{n} \mathcal{K}_\ell(i) A_i, \ 0 \le \ell \le n .$$

Η τελευταία ισότητα αποτελεί την έκφραση της διασποράς βαρών του δυϊκού κώδικα ως γραμμικό συνδυασμό της διασποράς βαρών του κώδικα.

Σχόλιο 2.5.7. Η έκφραση $\mathcal{K}_\ell(i) = \sum_{r=0}^{\ell} \binom{i}{r}\binom{n-i}{\ell-r}(-1)^r (q-1)^{\ell-r}$ είναι τα πολυώνυμα **Krawtchouk**, όπου εδώ η *μεταβλητή* i είναι ακέραιος αριθμός.

Ο υπολογισμός των πολυωνύμων Krawtchouk δεν είναι εύκολος, οπότε η τελευταία σχέση παρουσιάζει περισσότερο θεωρητικό ενδιαφέρον. Αντ' αυτής θα μπορούσαμε να βρούμε μια άλλη (ισοδύναμη) σχέση μεταξύ των απαριθμητών βάρους του δυϊκού κώδικα και των απαριθμητών βάρους του κώδικα.

Πράγματι, πολλαπλασιάζοντας τα μέλη της $(*)$ με z^{-n} και αντικαθιστώντας το z με $1/1+\xi$ έχουμε ότι:

$$\sum_{i=0}^{n} A_i^\perp (\xi+1)^{n-i} = (\mid \mathcal{C} \mid)^{-1} \sum_{i=0}^{n} A_i (q+\xi)^{n-i} \xi^i .$$

Από τη σχέση αυτή, συγκρίνοντας τους συντελεστές των ομοβαθμίων όρων ως προς ξ, έχουμε ότι:

$$\sum_{i=0}^{n-\ell} \binom{n-i}{\ell} A_i^{\perp} = q^{n-k-\ell} \sum_{i=0}^{\ell} \binom{n-i}{\ell-i} A_i,\ 0 \leq \ell \leq n\,.$$

Αντιστρέφοντας τον ρόλο των $\mathcal{C}$ και $\mathcal{C}^{\perp}$ και λαμβάνοντας υπόψη ότι $\binom{n-i}{\ell-i} = \binom{n-i}{n-\ell}$, η τελευταία ισότητα γίνεται:

$$\sum_{i=0}^{n-\ell} \binom{n-i}{\ell} A_i = q^{k-\ell} \sum_{i=0}^{\ell} \binom{n-i}{n-\ell} A_i^{\perp},\ 0 \leq \ell \leq n\ \ (**).$$

2.5.1 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας μήκους n. Υποθέτουμε ότι η λέξη $11\cdots 1$ είναι στοιχείο του $\mathcal{C}$, δείξτε ότι $A_i = A_{n-i},\ i = 0, 1, \ldots, n$.

3. Υπολογίστε τον απαριθμητή βάρους ενός δυαδικού κώδικα με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

   με δύο τρόπους. Απευθείας και με χρήση της ταυτότητας MacWilliams.

4. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ οι δυαδικοί κώδικες με γεννήτορες πίνακες:

$$\mathrm{G}_1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{και} \quad \mathrm{G}_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

   αντίστοιχα. Δείξτε ότι οι δύο κώδικες έχουν την ίδια διασπορά βαρών.

   Υποθέτουμε ότι οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ θεωρούνται τριαδικοί με τους ίδιους γεννήτορες πίνακες. Εξετάστε αν ισχύει κάτι ανάλογο στην περίπτωση αυτή.

5. Έστω $\mathcal{C}$ ένας δυαδικός γραμμικός κώδικας και $\widehat{\mathcal{C}}$ ο κώδικας που προέρχεται με την επισύναψη ενός ψηφίου ελέγχου ισοτιμίας. Δείξτε ότι:

$$W_{\widehat{\mathcal{C}}}(z) = \frac{1}{2}\Big[(1+z)W_{\mathcal{C}}(z) + (1-z)W_{\mathcal{C}}(-z)\Big].$$

6. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ δύο γραμμικοί κώδικες επί του ιδίου σώματος και $\mathcal{C} = \mathcal{C}_1 \mid \mathcal{C}_2$ (ιδέ Άσκηση 2.1.2$_{14}$). Δείξτε ότι $W^h_{\mathcal{C}}(z,x) = W^h_{\mathcal{C}_1}(z,x) \cdot W^h_{\mathcal{C}_2}(z,x)$.

   Εφαρμογή: Έστω $\mathcal{C}$ ο δυαδικός κώδικας μήκους 6 με πίνακα ελέγχου ισοτιμίας:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

   Δείξτε ότι $\mathcal{C} = \mathcal{E} \mid \mathcal{E} \mid \mathcal{E}$, όπου $\mathcal{E}$ είναι ο επαναληπτικός δυαδικός κώδικας μήκους 2. Οπότε υπολογίστε τη διασπορά βαρών του κώδικα $\mathcal{C}$ με τη βοήθεια της διασποράς βαρών του $\mathcal{E}$.

7. Αποδείξτε την εξής έκφραση του Θεωρήματος 2.4.14.

   Έστω $\mathcal{C}$ ένας $[n, k, d]$ δυαδικός γραμμικός κώδικας. Η πιθανότητα μη ανίχνευσης λαθών είναι ίση με:

$$p(\,\textit{μη ανίχνευσης λαθών}\,) = \frac{1}{2^{n-k}} W_{\mathcal{C}^\perp}(1-2p) - (1-p)^n.$$

2.6 Κώδικες με μέγιστη απόσταση (MDS Κώδικες)

Στην Παράγραφο 1.5.2 είχαμε ασχοληθεί με το δύσκολο πρόβλημα της εύρεσης του μεγέθους βέλτιστων κωδίκων. Αν έχουμε ένα αλφάβητο $\mathbb{A}$ με r το πλήθος στοιχεία και n και d φυσικούς αριθμούς, ζητούσαμε να προσδιορίσουμε το μεγαλύτερο μέγεθος κώδικα που μπορεί να υπάρξει με μήκος ίσο με n και ελάχιστη απόσταση ίση με d. Δηλαδή αναζητούσαμε να προσδιορίσουμε τον αριθμό $A_r(n,d) = \max\{\, M \mid \text{υπάρχει } (n, M, d) \text{ κώδικας}\,\}$.

Ένα από τα άνω φράγματα για τον αριθμό $A_r(n,d)$ είναι το φράγμα Singleton (Θεώρημα 1.5.21), το οποίο στην περίπτωση των γραμμικών κωδίκων έχει τη μορφή:

Για έναν γραμμικό $[n,\, k,\, d]$ κώδικα ισχύει $k \leq n-d+1$ (Πρόταση 2.1.13).

Αντί να σταθεροποιήσουμε το μήκος n και την ελάχιστη απόσταση d και να αναζητήσουμε το μεγαλύτερο δυνατόν μέγεθος κώδικα που μπορεί να υπάρξει με τις παραμέτρους n και d, μπορούμε να σταθεροποιήσουμε τις παραμέτρους μήκος n και το μέγεθος M και να αναζητούμε κώδικες με τη μεγαλύτερη δυνατή ελάχιστη απόσταση και με τις παραμέτρους n και M.

Στην περίπτωση των γραμμικών κωδίκων, λόγω του ότι $d \leq n-k+1$, το τελευταίο πρόβλημα ανάγεται στην αναζήτηση κωδίκων με παραμέτρους $[n,\, k,\, n-k+1]$ (ή δυϊκά με παραμέτρους $[n,\, n-d+1,\, d]$).

Ένας γραμμικός κώδικας $\mathcal{C}$ με παραμέτρους $[n,\, k,\, n-k+1]$ θα ονομάζεται κώδικας **μέγιστης** (ελάχιστης) απόστασης (για συντομία MDS κώδικες, από το Maximum Distance Separable).

Παραδείγματα 2.6.1. 1. Προφανώς ο κώδικας $\mathcal{C} = \mathbb{F}^n$, δηλαδή όλος ο χώρος, έχει παραμέτρους $[n,\, n,\, 1]$ και είναι κώδικας μέγιστης απόστασης.

2. Ο επαναληπτικός $p-$αδικός κώδικας:

$$\mathcal{R}_p(n) = \{\ \underbrace{00\cdots 0}_{n-\text{φορές}}\ ,\ \underbrace{11\cdots 1}_{n-\text{φορές}}\ , \ldots , \underbrace{p-1\, p-1\cdots p-1}_{n-\text{φορές}}\}$$

είναι ένας κώδικας μέγιστης απόστασης με παραμέτρους $[n, 1, n]$.

3. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα και n ένας θετικός ακέραιος με $n \geq 2$. Για κάθε $1 \leq i \leq n-1$, έστω $\mathbf{e}_i$ η λέξη μήκους n, η οποία έχει στις θέσεις i και $i+1$ το 1 και παντού αλλού μηδέν. Δεν είναι δύσκολο να δούμε ότι τα $n-1$ το πλήθος $\mathbf{e}_i$ είναι γραμμικά ανεξάρτητα και, επομένως, ο γραμμικός κώδικας, έστω $\mathcal{C}$, που έχει αυτά ως βάση είναι ένας κώδικας με παραμέτρους $[n,\, n-1,\, 2]$, δηλαδή ένας κώδικας μέγιστης απόστασης.

   [Αν περιορισθούμε σε δυαδικούς κώδικες, τότε ο κώδικας του παραδείγματος αυτού είναι ο γνωστός κώδικας $\mathcal{A}_n$ που αποτελείται από όλες τις λέξεις αρτίου βάρους (γιατί;) (ιδέ Άσκηση $2.1.2_3$)].

4. Έστω $n \geq 3$, για κάθε $1 \leq i \leq n-2$ λαμβάνουμε τις λέξεις $\mathbf{e}_i$ μήκους n, οι οποίες έχουν στις θέσεις $i, i+1$ και $i+2$ το 1 και παντού αλλού μηδέν.

Δεν είναι δύσκολο να δούμε ότι τα $n-2$ το πλήθος $\mathbf{e}_i$ είναι γραμμικά ανεξάρτητα και, επομένως, ο γραμμικός κώδικας, έστω $\mathcal{C}$, που έχει αυτά ως βάση είναι ένας κώδικας με παραμέτρους $[n,\, n-2,\, 2]$, δηλαδή δεν είναι ένας κώδικας μέγιστης απόστασης.

5. Στη σελίδα 142 είχαμε δει πως με τη βοήθεια των πινάκων Vandermonde μπορούμε να κατασκευάσουμε κώδικες μέγιστης απόστασης, Στο Κεφάλαιο για Reed Solomon κώδικες θα δούμε κατηγορίες κωδίκων μέγιστης απόστασης.

Τα τρία πρώτα παραδείγματα αποτελούν ακραίες περιπτώσεις κωδίκων μέγιστης απόστασης, κώδικες με παραμέτρους $[n,\, n,\, 1], [n, 1,\, n]$ και $[n,\, n-1,\, 2]$ θα ονομάζονται **τετριμμένοι** MDS κώδικες. Στα επόμενα, θα ασχοληθούμε με κώδικες μέγιστης απόστασης και παραμέτρους $[n,\, k,\, n-k+1]$ με $2 \leq k \leq n-2$.

Από την Πρόταση 2.2.25 έχουμε έναν τρόπο υπολογισμού της ελάχιστης απόστασης ενός γραμμικού κώδικα με τη βοήθεια ενός πίνακα ελέγχου ισοτιμίας του κώδικα. Στην περίπτωση των κωδίκων μέγιστης απόστασης έχουμε τον ακόλουθο χαρακτηρισμό.

Πρόταση 2.6.2. *Έστω $\mathcal{C}$ ένας γραμμικός $[n,\, k,\, d]$ κώδικας με έναν πίνακα ελέγχου ισοτιμίας* P*. Ο κώδικας $\mathcal{C}$ είναι κώδικας μεγίστης απόστασης, αν και μόνο αν οποιεσδήποτε $n-k$ το πλήθος στήλες του* P *είναι γραμμικά ανεξάρτητες.*

Απόδειξη. Η απόδειξη είναι άμεση από την Πρόταση 2.2.25. ό.έ.δ.

Θεώρημα 2.6.3. *Ένας γραμμικός κώδικας $\mathcal{C}$ επί ενός σώματος $\mathbb{F}$ είναι κώδικας μέγιστης απόστασης, αν και μόνο αν ο αντίστοιχος δυϊκός κώδικας $\mathcal{C}^{\perp}$ είναι κώδικας μέγιστης απόστασης.*

Απόδειξη. Υποθέτουμε ότι ο κώδικας $\mathcal{C}$ έχει παραμέτρους $[n,\, k,\, n-k+1]$, τότε ο δυϊκός $\mathcal{C}^{\perp}$ έχει παραμέτρους $[n,\, n-k,\, d]$ με $d \leq n-(n-k)+1 = k+1$. Σκοπός μας είναι να αποδείξουμε ότι $d = k+1$.

Υποθέτουμε ότι $d \leq k$, τότε υπάρχει μια (κωδικο)λέξη $\mathbf{c} \in \mathcal{C}^{\perp}$ με βάρος ίσο με d, δηλαδή η $\mathbf{c}$ σε d το πλήθος θέσεις έχει μη μηδενικούς χαρακτήρες.

Έστω P ένας $(n-k)\times n$ πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$, τότε αυτός είναι γεννήτορας πίνακας για τον δυϊκό κώδικα $\mathcal{C}^{\perp}$, επομένως υπάρχει $\mathbf{a}\in\mathbb{F}^{n-k}$, έτσι ώστε $\mathbf{c}=\mathbf{a}\mathrm{P}$. Από τον πίνακα P διαγράφουμε k το πλήθος στήλες ως εξής, διαγράφουμε d το πλήθος στήλες στις αντίστοιχες θέσεις που στην (κωδικο)λέξη $\mathbf{c}$ εμφανίζονται μη μηδενικοί χαρακτήρες και τις υπόλοιπες $k-d$ τυχαία (έχουμε υποθέσει ότι $d\leq k$). Ο υποπίνακας $\bar{\mathrm{P}}$ που προκύπτει είναι τετραγωνικός $(n-k)\times(n-k)$ πίνακας και από την προηγούμενη πρόταση έχουμε ότι είναι αντιστρέψιμος. Από τον τρόπο διαγραφής των k στηλών του πίνακα για τη δημιουργία του $\bar{\mathrm{P}}$ και το γεγονός ότι $\mathbf{c}=\mathbf{a}\mathrm{P}$ έπεται ότι $\mathbf{a}\bar{\mathrm{P}}=\mathbf{0}$. Ο πίνακας $\bar{\mathrm{P}}$ είναι αντιστρέψιμος, άρα $\mathbf{a}=\mathbf{0}$, δηλαδή $\mathbf{c}=\mathbf{a}\mathrm{P}=\mathbf{0}$, άτοπο. Επομένως, δεν ισχύει η υπόθεση $d\leq k$. Άρα $d=k+1$. ό.έ.δ.

Από τα προηγούμενα, επειδή κάθε γεννήτορας πίνακας ενός κώδικα είναι πίνακας ελέγχου ισοτιμίας του αντίστοιχου δυϊκού και αντίστροφα, έχουμε το ακόλουθο πόρισμα.

Πόρισμα 2.6.4. *Ένας γραμμικός $[n,\,k,\,d]$ κώδικας είναι κώδικας μέγιστης απόστασης, αν και μόνο αν σε έναν γεννήτορα πίνακα κάθε k το πλήθος στήλες είναι γραμμικά ανεξάρτητες.*

Θεώρημα 2.6.5. *Ένας γραμμικός $[n,\,k,\,d]$ κώδικας $\mathcal{C}$ με γεννήτορα πίνακα $\mathrm{G}=[\mathrm{I}_k\ \ \mathrm{A}]$ είναι κώδικας μέγιστης απόστασης, αν και μόνο αν κάθε τετραγωνικός υποπίνακας του* A *είναι αντιστρέψιμος.*

Απόδειξη. Υποθέτουμε ότι κάθε τετραγωνικός υποπίνακας του πίνακα A είναι αντιστρέψιμος. Ο πίνακας A είναι ένας $k\times(n-k)$ πίνακας. Αν $k\leq n-k$, τότε κάθε k το πλήθος από τις στήλες του A είναι γραμμικά ανεξάρτητες. Αν $n-k\leq k$, τότε όλες οι στήλες του A είναι γραμμικά ανεξάρτητες. Έστω k το πλήθος στήλες του γεννήτορα πίνακα G. Αν αυτές είναι οι πρώτες στήλες, προφανώς είναι γραμμικά ανεξάρτητες. Αν όλες είναι στήλες του πίνακα A, τότε από τα προηγούμενα είναι γραμμικά ανεξάρτητες. Υποθέτουμε ότι έχουμε k το πλήθος στήλες από τον πίνακα G, οι οποίες δεν είναι γραμμικά ανεξάρτητες, τότε μερικές από αυτές θα είναι στήλες του πίνακα I_k και μερικές θα είναι στήλες του A. Άρα, μια από τις στήλες του I_k θα είναι γραμμικός

συνδυασμός κάποιων στηλών του πίνακα I_k και κάποιων στηλών του πίνακα A με τουλάχιστον μια από τις στήλες του πίνακα A να έχει μη μηδενικό συντελεστή (γιατί;). Από τις στήλες αυτές διαγράφουμε τις θέσεις στις οποίες εμφανίζεται το 1. Τότε προκύπτει ένας γραμμικός συνδυασμός της μηδενικής στήλης με τμήματα στηλών του πίνακα A δηλαδή υπάρχει τετραγωνικός υποπίνακας του A που δεν είναι αντιστρέψιμος, άτοπο. Άρα, κάθε k το πλήθος στήλες του πίνακα G είναι γραμμικά ανεξάρτητες και ο κώδικας είναι κώδικας μέγιστης απόστασης από το προηγούμενο πόρισμα.

Αντίστροφα, υποθέτουμε ότι ο κώδικας είναι κώδικας μέγιστης απόστασης. Έστω ένας B $\nu \times \nu$ υποπίνακας του πίνακα A. Μεταθέτοντας τις γραμμές και στήλες του πίνακα G, μπορούμε να πάρουμε έναν $k \times n$ πίνακα της μορφής:

$$\widehat{\mathrm{G}} = \begin{bmatrix} \mathbf{0} & \mathrm{B} & * \\ \mathrm{I}_{k-\nu} & * & * \end{bmatrix},$$

όπου τα $*$ παριστούν πίνακες καταλλήλων διαστάσεων. Ο πίνακας $\widehat{\mathrm{G}}$ είναι γεννήτορας πίνακας ενός κώδικα ισοδυνάμου με τον κώδικα $\mathcal{C}$, επομένως και ο νέος κώδικας είναι κώδικας μέγιστης απόστασης (ισοδύναμοι κώδικες έχουν την ίδια ελάχιστη απόσταση). Από το προηγούμενο πόρισμα έχουμε ότι οι πρώτες k το πλήθος στήλες του πίνακα $\widehat{\mathrm{G}}$ είναι γραμμικά ανεξάρτητες, δηλαδή ο πίνακας:

$$\begin{bmatrix} \mathbf{0} & \mathrm{B} \\ \mathrm{I}_{k-\nu} & * \end{bmatrix}$$

είναι αντιστρέψιμος. Άρα, ο πίνακας B είναι αντιστρέψιμος. ό.έ.δ.

Μια άμεση παρατήρηση είναι ότι σε έναν κώδικα μέγιστης απόστασης με γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ κανένα στοιχείο του πίνακα A δεν είναι μηδενικό.

Συνοψίζοντας όλα τα προηγούμενα, μπορούμε να δώσουμε τους εξής ισοδύναμους χαρακτηρισμούς ενός κώδικα μέγιστης απόστασης.

Θεώρημα 2.6.6. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ γραμμικός κώδικας. Τα ακόλουθα είναι ισοδύναμα.*

1. *Ο κώδικας $\mathcal{C}$ είναι μέγιστης απόστασης.*

2. *Οποιεσδήποτε k το πλήθος στήλες ενός γεννήτορα πίνακα του $\mathcal{C}$ είναι γραμμικά ανεξάρτητες.*

3. *Οποιεσδήποτε $n-k$ το πλήθος στήλες ενός πίνακα ελέγχου ισοτιμίας του $\mathcal{C}$ είναι γραμμικά ανεξάρτητες.*

4. *Ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ είναι κώδικας μέγιστης απόστασης.*

5. *Αν $\mathrm{G} = [\mathrm{I}_k \quad \mathrm{A}]$ είναι ένας γεννήτορας πίνακας του $\mathcal{C}$ σε κανονική μορφή, τότε κάθε τετραγωνικός υποπίνακας του A είναι αντιστρέψιμος.*

Παράδειγμα 2.6.7. Θεωρούμε τον πίνακα:

$$\mathrm{A} = \begin{pmatrix} 1 & 6 & 2 & 5 & 1 \\ 1 & 4 & 3 & 3 & 6 \\ 1 & 5 & 5 & 1 & 5 \end{pmatrix}$$

επί του σώματος $\mathbb{Z}_7$. Μπορούμε να ελέγξουμε ότι κάθε τετραγωνικός υποπίνακας του A είναι αντιστρέψιμος (κάντε το!), άρα μπορούμε να κατασκευάσουμε δύο κώδικες μέγιστης απόστασης επί του $\mathbb{Z}_7$, έναν $[8, 3, 6]$ κώδικα με γεννήτορα πίνακα $[\mathrm{I}_3 \quad \mathrm{A}]$ και έναν $[8, 5, 4]$ κώδικα με πίνακα ελέγχου ισοτιμίας τον πίνακα $[\mathrm{A} \quad \mathrm{I}_3]$.

Στο τελευταίο θεώρημα έχουμε ισοδύναμους χαρακτηρισμούς για έναν κώδικα μέγιστης απόστασης, αλλά δεν έχουμε συνθήκες για το αν υπάρχουν μη τετριμμένοι κώδικες μέγιστης απόστασης με δεδομένο μήκος n και δεδομένη διάσταση k. Η μόνη συνθήκη που έχουμε είναι ότι για μη τετριμμένους κώδικες μέγιστης απόστασης πρέπει να ισχύει $2 \leq k \leq n-2$. Θα δούμε ότι η απαίτηση, να είναι η ελάχιστη απόσταση του κώδικα ίση με $d = n-k+1$, περιορίζει κατά πολύ τη δυνατότητα υπάρξης κωδίκων μέγιστης απόστασης. Συγκεκριμμένα έχει σχέση με το μέγεθος του πεπερασμένου σώματος $\mathbb{F}$, επί του οποίου ορίζεται ο κώδικας.

Θεώρημα 2.6.8. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Δεν υπάρχει μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης με $2 \leq k \leq n-q$.*

Απόδειξη. Υποθέτουμε ότι επί του σώματος $\mathbb{F}$ υπάρχει ο κώδικας $\mathcal{C}$ μέγιστης απόστασης με παραμέτρους $[n, k, n-k+1]$ και ότι $2 \leq k \leq n-q$. Έστω $\mathrm{G} = [\mathrm{I}_k \; \mathrm{A}]$ ένας γεννήτορας πίνακας σε κανονική μορφή. Ο πίνακας A έχει $n-k \geq q$ το πλήθος στήλες. Όπως έχουμε παρατηρήσει, κανένα στοιχείο του A δεν είναι 0. Οπότε, πολλαπλασιάζοντας κάθε στήλη του A με το αντίστροφο του πρώτου στοιχείου της, λαμβάνουμε έναν πίνακα $\widehat{\mathrm{A}}$, του οποίου τα στοιχεία της πρώτης γραμμής είναι όλα 1. Ο κώδικας με γεννήτορα πίνακα $\widehat{\mathrm{G}} = [\mathrm{I}_k \; \widehat{\mathrm{A}}]$ είναι ισοδύναμος με τον αρχικό κώδικα, άρα είναι κώδικας μέγιστης απόστασης. Επειδή υποθέσαμε ότι $n-k \geq q$, δηλαδή το πλήθος των στηλών είναι μεγαλύτερο από το πλήθος των στοιχείων του αλφαβήτου, προφανώς στη δεύτερη γραμμή (και σε κάθε γραμμή) του πίνακα $\widehat{\mathrm{A}}$ δύο τουλάχιστον στοιχεία θα είναι ίσα. Πολλαπλασιάζουμε την πρώτη γραμμή του πίνακα $\widehat{\mathrm{G}}$ με το στοιχείο, το οποίο εμφανίζεται στη δεύτερη γραμμή (τουλάχιστον) δύο φορές και την αφαιρούμε από τη δεύτερη γραμμή. Τότε προκύπτει μία (κωδικο)λέξη η οποία στις k πρώτες θέσεις έχει $k-2$ το πλήθος μηδενικά και στις υπόλοιπες $n-k$ θέσεις τουλάχιστον δύο μηδενικά, άρα συνολικά έχει τουλάχιστον k το πλήθος μηδενικά, δηλαδή η απόστασή της από τη μηδενική (κωδικο)λέξη είναι το πολύ ίση με $n-k$. Αυτό είναι άτοπο, διότι υποθέσαμε ότι ο κώδικας είναι μέγιστης απόστασης ($d = n-k+1$). Άρα, δεν υπάρχει κώδικας μέγιστης απόστασης με $2 \leq k \leq n-q$. ό.έ.δ.

Αν στο προηγούμενο θεώρημα αντί του κώδικα $\mathcal{C}$ πάρουμε τον δυϊκό του, τότε έχουμε.

Πόρισμα 2.6.9. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Δεν υπάρχει μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης με $q \leq k \leq n$.*

Οπότε, αν υπάρχει ένας μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης, τότε αναγκαστικά $n-q+1 \leq k \leq q-1$.

Την τελευταία σχέση θα μπορούσαμε να την εκφράσουμε διαφορετικά ως εξής: Αν υπάρχει ένας μη τετριμμένος $[n, k, d]$ κώδικας μέγιστης απόστασης, τότε αναγκαστικά $2 \leq k \leq q-1$ και $2 \leq n-k \leq q-1$.

Από τις σχέσεις αυτές, λαμβάνοντας υπόψη ότι ενδιαφερόμαστε για μη τετριμμένους κώδικες μέγιστης απόστασης, έχουμε ότι $2 \leq k \leq min\{\, n-2,\, q-1 \,\}$ και $n \leq k+q-1 \leq 2q-2$.

Από τα προηγούμενα έπεται το εξής πόρισμα.

Πόρισμα 2.6.10. *Οι μόνοι δυαδικοί κώδικες μέγιστης απόστασης είναι οι τετριμμένοι.*

Έχοντας υπόψη τη σχέση $n-q+1 \leq k \leq q-1$, δηλαδή $n \leq k+q-1$, γεννάται το ερώτημα: Δοθέντων των k και q να βρεθεί η μεγαλύτερη δυνατή τιμή του n, έτσι ώστε να υπάρχει ένας κώδικας μέγιστης απόστασης με μήκος n.

Ας συμβολίσουμε με $m(k,\, q)$ τη μεγαλύτερη δυνατή τιμή του n.

Υπάρχει η εικασία ότι $m(k,\, q) = q+1$, εκτός από την περίπτωση $k=3$, όπου έχει αποδειχθεί ότι αφενός μεν $m(3,\, q) = q+1$, αν το q είναι περιττός, αφετέρου δε $m(3,\, q) = q+2$, αν το q είναι άρτιος.

Η εικασία αυτή έχει αποδειχθεί για $k \leq 5$ και όλα τα q. Για όλα τα k με $q \leq 11$ και για όλα τα περιττά $q > (4k-9)^2$. Χρησιμοποιώντας το γεγονός ότι ένας κώδικας είναι κώδικας μέγιστης απόστασης, αν και μόνο αν ο αντίστοιχος δυϊκός κώδικας είναι κώδικας μέγιστης απόστασης, η εικασία έχει αποδειχθεί και σε άλλες περιπτώσεις.

Πριν αποδείξουμε την εικασία για $k=2$ θα αναδιατυπώσουμε το πρόβλημα της εύρεσης της μέγιστης τιμής $m(k,\, q)$ του μήκους για κώδικες μέγιστης απόστασης σε ισοδύναμα προβλήματα της Γραμμικής Άλγεβρας.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και k ένας θετικός ακέραιος.

Τα επόμενα προβλήματα είναι ισοδύναμα με την εύρεση της μεγαλύτερης δυνατής τιμής του n, ώστε να υπάρχει κώδικας επί του $\mathbb{F}$ με παραμέτρους $[n,\, k,\, n-k+1]$.

1 Να βρεθεί η μεγαλύτερη τιμή του n, ώστε να υπάρχει ένας $k \times n$ πίνακας με στοιχεία από το σώμα $\mathbb{F}$ με την ιδιότητα: Κάθε υποσύνολο με k το πλήθος στήλες είναι γραμμικά ανεξάρτητο.

2 Έστω V ένας διανυσματικός χώρος επί του σώματος $\mathbb{F}$ με διάσταση ίση με k. Να βρεθεί η μεγαλύτερη τιμή n, ώστε να υπάρχει υποσύνολο του V

με n το πλήθος στοιχεία και κάθε υποσύνολό του με k το πλήθος στοιχεία να αποτελεί βάση του V.

3 Να βρεθεί η μεγαλύτερη τιμή του n, ώστε να υπάρχει ένας $k \times (n-k)$ πίνακας A με στοιχεία από το σώμα $\mathbb{F}$ με την ιδιότητα: Κάθε τετραγωνικός υποπίνακας του A είναι αντιστρέψιμος.

Με την βοήθεια του Θεωρήματος 2.6.6 ελέγξτε την ισοδυναμία των προβλημάτων αυτών με την εύρεση της μεγαλύτερης δυνατής τιμής του n, ώστε να υπάρχει κώδικας επί του $\mathbb{F}$ με παραμέτρους $[n,\, k,\, n-k+1]$.

Θεώρημα 2.6.11. *Για κάθε q θετικό ακέραιο, ο οποίος είναι δύναμη ενός πρώτου αριθμού ισχύει $m(2,\, q) = q+1$.*

Απόδειξη. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και V ένας διανυσματικός χώρος επί του σώματος $\mathbb{F}$ διάστασης 2. Ο V έχει q^2 το πλήθος στοιχεία. Οι γνήσιοι μη μηδενικοί υπόχωροι του V είναι διάστασης 1 και είναι $q+1$ το πλήθος (γιατί;).

Έστω S ένα υποσύνολο του V με το μεγαλύτερο δυνατόν πλήθος στοιχείων, έτσι ώστε κάθε δύο στοιχεία του να είναι γραμμικά ανεξάρτητα. Το σύνολο S περιέχει το πολύ ένα στοιχείο από κάθε μονοδιάστατο υπόχωρο. Επίσης, αν υπήρχε μονοδιάστατος υπόχωρος W, έτσι ώστε κάθε στοιχείο του W να μην ανήκει στο S, τότε για $w \in W$ θα είχαμε ότι στο σύνολο $S \cup \{\, w \,\}$ κάθε δύο στοιχεία του να είναι γραμμικά ανεξάρτητα, άτοπο από την επιλογή του S. Άρα, τα στοιχεία του S είναι ακριβώς όσοι και οι μονοδιάστατοι υπόχωροι του V, δηλαδή το S περιέχει $q+1$ το πλήθος στοιχεία.

Οπότε, σύμφωνα με το ισοδύναμο Πρόβλημα **2** έπεται το αποτέλεσμα. ό.έ.δ.

Εδώ δεν θα ασχοληθούμε με την απόδειξη άλλων περιπτώσεων, όπου η εικασία ισχύει. Θα αποδείξουμε όμως μερικές προτάσεις, οι οποίες, εκτός του ότι συμβάλλουν στην απόδειξη μερικών περιπτώσεων της εικασίας, από μόνες τους παρουσιάζουν ανεξάρτητο ενδιαφέρον.

Πρόταση 2.6.12. *Για δύο κώδικες μέγιστης απόστασης επί ενός σώματος με q το πλήθος στοιχεία, όπου ο ένας έχει διάσταση k και ο άλλος $k+1$, ισχύει ότι $m(k+1,\, q) \leq m(k,\, q)+1$.*

Απόδειξη. Έστω ένας κώδικας μέγιστης απόστασης μήκους $n+1 = m(k+1, q)$. Ο κώδικας αυτός έχει διάσταση ίση με $k+1$ και ελάχιστη απόσταση ίση με $n-k+1$. Επομένως, αν H είναι ένας πίνακας ελέγχου ισοτιμίας, ο H θα έχει $n-k$ το πλήθος γραμμικά ανεξάρτητες στήλες (ίδε Θεώρημα 2.6.6$_3$). Συνεπώς, αν πάρουμε τις n πρώτες στήλες του πίνακα H, έχουμε έναν πίνακα, ο οποίος είναι πίνακας ελέγχου ισοτιμίας ενός (άλλου) κώδικα, ο οποίος έχει παραμέτρους $[n, k, n-k+1]$ (γιατί;), δηλαδή είναι και αυτός ένας κώδικας μέγιστης απόστασης. Άρα $m(k+1, q) - 1 = n \leq m(k, q)$. ό.έ.δ.

Πρόταση 2.6.13. *Για $k \geq 2$ και $n \geq m(k, q)$ ισχύει ότι*
$m(n-k+1, q) \leq n$.

Απόδειξη. Υποθέτουμε ότι $m(n-k+1, q) \geq n+1$, τότε υπάρχει γραμμικός κώδικας $\mathcal{C}$ μέγιστης απόστασης με παραμέτρους $[n+1, n-k+1, k+1]$. Ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ θα είναι και αυτός μέγιστης απόστασης και θα έχει παραμέτρους $[n+1, k, (n+1)-k+1]$. Δηλαδή θα έχουμε έναν κώδικα μέγιστης απόστασης μήκους $n+1 \geq m(k, q)$, άτοπο. ό.έ.δ.

Πρόταση 2.6.14. *Υποθέτουμε ότι έχουμε ένα πεπερασμένο σώμα $\mathbb{F}$ με q το πλήθος στοιχεία. Τότε ισχύει:*

$$m(q, q) \leq q+2.$$

Στην περίπτωση όπου ο q είναι περιττός ισχύει:

$$m(q-1, q) \leq q+1.$$

Απόδειξη. Αν θέσουμε $k = 3$ και $n = q+2$, τότε προφανώς ισχύει $m(3, q) \leq q+2$. Οπότε από την προηγούμενη πρόταση έχουμε $m(q+2-3+1, q) \leq q+2$.

Στην περίπτωση όπου ο q είναι περιττός, όπως έχουμε προαναφέρει, έχει αποδειχθεί ότι $m(3, q) = q+1$. Οπότε, αν θέσουμε $k = 3$ και $n = q+1$, έπεται το αποτέλεσμα. ό.έ.δ.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathcal{C}$ ένας κώδικας μέγιστης απόστασης επί του $\mathbb{F}$ με παραμέτρους $[n, k, d]$. Θα υπολογίσουμε τον απαριθμητή βάρους του $\mathcal{C}$.

Προφανώς, $A_0 = 1$ και $A_i = 0$ για $1 \leq i \leq n-k$. Επίσης, επειδή και ο δυϊκός κώδικας είναι κώδικας μέγιστης απόστασης, έχουμε ότι $A_0^\perp = 1$ και $A_i^\perp = 0$ για $1 \leq i \leq k$.

Από τη σχέση $(**)$ στο Σχόλιο 2.5.7 έχουμε ότι:

$$\binom{n}{\ell} + \sum_{i=n-k+1}^{n-\ell} \binom{n-i}{\ell} A_i = q^{k-\ell}\binom{n}{\ell},\ 0 \leq \ell \leq k-1\,,$$

ή

$$\sum_{i=n-k+1}^{n-\ell} \binom{n-i}{\ell} A_i = (q^{k-\ell}-1)\binom{n}{\ell},\ 0 \leq \ell \leq k-1\,.$$

Πρόταση 2.6.15. *Έστω $\mathcal{C}$ ένας κώδικας μέγιστης απόστασης, όπως παραπάνω. Τότε για τη διασπορά βαρών ισχύει:*

$$\begin{aligned} A_i &= \binom{n}{i} \sum_{j=0}^{i-d} \binom{i}{j} (-1)^j (q^{i+1-d-j} - 1) \\ &= \binom{n}{i}(q-1) \sum_{j=0}^{i-d} \binom{i-1}{j} (-1)^j q^{i-d-j}, \quad d \leq i \leq n\,. \end{aligned}$$

Όπου $d = n-k+1$ είναι η ελάχιστη απόσταση του κώδικα.

Απόδειξη. Οι σχέσεις:

$$\sum_{i=n-k+1}^{n-\ell} \binom{n-i}{\ell} A_i = (q^{k-\ell}-1)\binom{n}{\ell},\ 0 \leq \ell \leq k-1$$

αποτελούν ένα τριγωνικό σύστημα με αγνώστους τα A_i, οπότε, λύνοντας το σύστημα ως άσκηση, μπορείτε να επαληθεύσετε τον ισχυρισμό. ό.έ.δ.

Αξίζει να σημειωθεί ότι, σε όλους τους κώδικες μέγιστης απόστασης με παραμέτρους $[n,\, k,\, d]$ επί ενός σώματος $\mathbb{F}$, η διασπορά βαρών είναι η ίδια και **δεν** εξαρτάται από τη δομή τους.

2.6.1 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Έστω $\mathcal{C}$ ο κώδικας επί του $\mathbb{Z}_3$ με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Δείξτε ότι ο $\mathcal{C}$ είναι κώδικας μέγιστης απόστασης.

3. Εξετάστε αν ο τριαδικός κώδικας $\mathcal{C}$ με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

είναι κώδικας μέγιστης απόστασης.

4. Έστω α μια πρωταρχική κυβική ρίζα της μονάδας επί του $\mathbb{Z}_2$. Ως γνωστόν, το σύνολο $\mathbb{F} = \{\, 0,\, 1,\, \alpha,\, \alpha^2 \,\}$ είναι σώμα. Δείξτε ότι ο κώδικας $\mathcal{C}$ επί του $\mathbb{F}$ με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}$$

είναι κώδικας μέγιστης απόστασης.

Να βρεθεί ο δυϊκός κώδικας του κώδικα $\mathcal{C}$ και να επαληθεύσετε ότι και αυτός είναι κώδικας μέγιστης απόστασης.

5. Να κατασκευάσετε έναν τριαδικό κώδικα μέγιστης απόστασης με μήκος 4 και διάσταση 2.

6. Εξετάστε αν υπάρχουν τριαδικοί κώδικες μέγιστης απόστασης με παραμέτρους $[5,\, 3,\, d]$, $[6,\, 3,\, d]$ και $[n,\, 2,\, d]$ για $n \geq 5$.

7. Να κατασκευάσετε όλους τους κώδικες μέγιστης απόστασης επί του $\mathbb{Z}_5$ με διάσταση 2 και μήκη $4,\, 5,\, 6$.

Υπάρχει πενταδικός κώδικας μέγιστης απόστασης με διάσταση 2 και μήκος $n \geq 7$;

8. Για $k \geq 2$ να κατασκευάσετε κώδικες μέγιστης απόστασης επί του $\mathbb{Z}_{11}$ με μήκος n όσο το δυνατόν μεγαλύτερο.

9. Να δείξετε ότι σε κάθε κώδικα μέγιστης απόστασης η ακτίνα κάλυψης είναι μικρότερη από την ελάχιστη απόστασή του.

Βιβλιογραφία

Berlekamp, E. R. *"Algebraic Coding Theory"*. Laguna Hills, CA: Aegean Park Press, 1984.

Hall, J.I. *Notes on Coding Theory*. (σε ηλεκτρονική μορφή). www.math.msu.edu/~jhall.

Hamming, R. *"Coding and Information Theory"*. Prentice-Hall, Englewood Cliffs 2^{nd} Edition, 1986.

Herstein, I. N. *"Abstract Algebra"*. New York: Macmillan, 1990.

Hill, R. *"A First Course in Coding Theory"*. Oxford University Press, Oxford, 1986.

Huffman, C. W. and Pless, V. . *"Fundamentals of Error-Correcting Codes"*. Cambridge University Press, 2003.

Lidl, R. and Niederreiter H. . *"Introduction to finite fields and their applications"*. Cambridge University Prees, 2000.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*. Wiley, New York, 1998.

Roman, S. *"Coding and Information Theory"*. Springer-Verlag, 1992.

Ron M. Roth. *"Introduction to Coding Theory"*. Cambridge University Press, 2006.

Vermani, L. *"Elements of Algebraic Coding Theory"*. Chapman and Hall, London, 1996.

Walker, J. L. *"Codes and Curves"*, volume 7 of *Student Mathematical Library*. AMS, 2000.

Σ. Ανδρεαδάκης. *Θεωρία Galois*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1992.

Σ. Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1993.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

ΚΕΦΑΛΑΙΟ 3

Πολυωνυμικοί-Κυκλικοί Κώδικες

Στα προηγούμενα ασχοληθήκαμε με τους γραμμικούς κώδικες και είδαμε πώς η δομή ενός γραμμικού κώδικα, ως διανυσματικού χώρου, καθιστά τις διαδικασίες κωδικοποίησης και αποκωδικοποίησης περισσότερο αποτελεσματικές. Εδώ θα ασχοληθούμε με ειδικές κατηγορίες γραμμικών κωδίκων. Ο τρόπος, με τον οποίο ορίζονται, τους καθιστά εύχρηστους ως προς τον χειρισμό τους. Για τον λόγο αυτό παρουσιάζουν τόσο θεωρητικό, όσο και πρακτικό ενδιαφέρον.

3.1 Πολυωνυμικοί κώδικες

Έστω $\mathbb{F}_{m-1}[x]$ το σύνολο όλων των πολυωνύμων με βαθμό μικρότερο ή ίσον του $m-1$ και συντελεστές από το σώμα $\mathbb{F}$.

Πρόταση 3.1.1. *Έστω* $\alpha(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_{m-1}[x]$. *Η απεικόνιση* $\psi : \mathbb{F}_{m-1}[x] \longrightarrow \mathbb{F}^m$ *με* $\psi(\alpha(x)) = (a_0, a_1, \dots, a_{m-1})$ *είναι ένας ισομορφισμός διανυσματικών χώρων.*

Απόδειξη. Η απόδειξη είναι απλή και αφίεται ως άσκηση. ό.έ.δ.

Από την προηγούμενη πρόταση βλέπουμε ότι μπορούμε να ταυτίσουμε πολυώνυμα με διατεταγμένες $m-$άδες και αντίστροφα διατεταγμένες $m-$άδες με πολυώνυμα. Κατά συνέπεια, όπως θα δούμε, μπορούμε να ταυτίσουμε κώδικες με σύνολα πολυωνύμων.

Επίσης, αν $\alpha(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$ είναι ένα πολυώνυμο, μπορούμε να ορίσουμε το **βάρος** του $w(\alpha(x)) = w(a_0\, a_1 \cdots a_{m-1})$, δηλαδή το πλήθος των μη μηδενικών συντελεστών του.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα.

Επιλέγουμε και σταθεροποιούμε ένα μη μηδενικό πολυώνυμο:

$$\gamma(x) = c_0 + c_1x + \cdots + c_kx^k \in \mathbb{F}_k[x].$$

Για κάθε $\alpha(x) = a_0+a_1x+\cdots+a_{m-1}x^{m-1} \in \mathbb{F}_{m-1}[x]$ το πολυώνυμο $\alpha(x)\cdot\gamma(x)$ είναι ένα πολυώνυμο βαθμού το πολύ $m+k-1$.

Πρόταση 3.1.2. *Η απεικόνιση $\vartheta : \mathbb{F}_{m-1}[x] \longrightarrow \mathbb{F}_{m+k-1}[x]$ με $\vartheta(\alpha(x)) = \alpha(x)\cdot\gamma(x)$ είναι μια 1 - 1 γραμμική απεικόνιση. Επομένως, η εικόνα $\vartheta(\mathbb{F}_{m-1}[x])$ είναι ένας διανυσματικός υπόχωρος του $\mathbb{F}_{m+k-1}[x]$ διάστασης m.*

Απόδειξη. Για $\alpha(x), \beta(x) \in \mathbb{F}_{m-1}[x]$ και $\lambda, \mu \in \mathbb{F}$ ως γνωστόν ισχύει:

$$(\lambda\alpha(x) + \mu\beta(x)) \cdot \gamma(x) = \lambda(\alpha(x) \cdot \gamma(x)) + \mu(\beta(x)) \cdot \gamma(x)).$$

Οπότε έπεται το αποτέλεσμα. ό.έ.δ.

Έστω $\alpha(x)\cdot\gamma(x) = r_0+r_1x+\cdots r_{m+k-1}x^{m+k-1}$. Σύμφωνα με την Πρόταση 3.1.1, μπορούμε να ταυτίσουμε το στοιχείο $\alpha(x) \cdot \gamma(x)$ του διανυσματικού χώρου $\vartheta(\mathbb{F}_{m-1}[x])$ με το στοιχείο $(r_0, r_1, \ldots, r_{m+k-1})$ του $\mathbb{F}^{m+k}$

Τα προηγούμενα θα μπορούσαν να εκφρασθούν ως εξής:

$$\mathbb{F}^m \xrightarrow{\psi^{-1}} \mathbb{F}_{m-1}[x] \xrightarrow{\vartheta} \mathbb{F}_{m+k-1}[x] \xrightarrow{\psi} \mathbb{F}^{m+k}.$$

Προσοχή! Στην προηγούμενη σχέση η συνάρτηση ψ^{-1} εφαρμόζεται από το $\mathbb{F}^m$ στο $\mathbb{F}_{m-1}[x]$, ενώ η συνάρτηση ψ από το $\mathbb{F}_{m+k-1}[x]$ στο $\mathbb{F}^{m+k}$. Αυτό **δεν** πρέπει να προκαλεί σύγχυση καθότι, γενικά, με ψ θα συμβολίζουμε την απεικόνιση που απεικονίζει ένα (οποιοδήποτε) πολυώνυμο στο αντίστοιχο 'διάνυσμα' των συντελεστών του.

Ορισμός 3.1.3. *Το σύνολο:*

$$\mathcal{C} = \{\, \psi(\vartheta(\alpha(x))) = \psi(\alpha(x)\cdot\gamma(x)) = (r_0, r_1, \dots, r_{m+k-1}) \mid \alpha(x) \in \mathbb{F}_{m-1}[x] \,\}$$

θα λέγεται ένας ***πολυωνυμικός κώδικας*** *με πολυώνυμο γεννήτορα (ή πολυώνυμο κωδικοποίησης) το πολυώνυμο* $\gamma(x)$*.*

Πρόταση 3.1.4. *Ένας πολυωνυμικός κώδικας είναι ένας γραμμικός κώδικας.*

Απόδειξη. Η απόδειξη είναι άμεση από τα προηγούμενα. ό.έ.δ.

Παρατηρήσεις 3.1.5.

1. Οι παράμετροι ενός πολυωνυμικού κώδικα εξαρτώνται τόσο από το πολυώνυμο γεννήτορα, όσο και από το φυσικό αριθμό m που χαρακτηρίζει τον χώρο $\mathbb{F}_{m-1}[x]$, ο οποίος είναι το πεδίο ορισμού της συνάρτησης ϑ. Συγκεκριμένα, το μήκος του είναι ίσο με $n = m + k$ και η διάστασή του ίση με m (γιατί;).

2. Αν ως πηγή (βλέπε σελίδα 5) πάρουμε το σύνολο $\mathbb{F}^m$, τότε η συνάρτηση κωδικοποίησης είναι η σύνθεση των απεικονίσεων ψ^{-1}, ϑ και ψ, δηλαδή $f = \psi \circ \vartheta \circ \psi^{-1}$

3. Πολλές φορές στα επόμενα θα *ταυτίζουμε*, όπως προείπαμε, χωρίς ιδιαίτερη μνεία, τις (κωδικο)λέξεις με πολυώνυμα, όπως και τα στοιχεία της πηγής με πολυώνυμα. (Για τον λόγο αυτό οι δείκτες στην αρίθμηση των χαρακτήρων σε μια (κωδικο)λέξη θα αρχίζουν από το 0).

4. Η ελάχιστη απόσταση ενός πολυωνυμικού κώδικα είναι ίση με το μικρότερο πλήθος των μη μηδενικών συντελεστών των πολυωνύμων $\alpha(x)\cdot\gamma(x)$, όπου $\alpha(x) \in \mathbb{F}_{m-1}[x]$. Η απόδειξη δεν είναι δύσκολη, αρκεί να θυμηθούμε το Θεώρημα 2.1.3.

5. Έστω $\gamma(x) = c_0 + c_1 x + \cdots + c_k x^k$ το πολυώνυμο γεννήτορας ενός πολυωνυμικού κώδικα. Αν ο σταθερός όρος c_0 είναι μηδέν, τότε σε όλες τις (κωδικο)λέξεις ο πρώτος χαρακτήρας είναι μηδέν, όμοια, αν ο συντελεστής c_k είναι μηδέν, τότε ο τελευταίος χαρακτήρας σε όλες τις (κωδικο)λέξεις είναι μηδέν. Αλλά τότε οι χαρακτήρες αυτοί δεν προσφέρουν τίποτε στην κωδικοποίηση, οπότε ο κώδικας μπορεί να συμπτυχθεί ως προς αυτές τις συντεταγμένες (βλέπε σελίδα 46). Επομένως,

στα επόμενα θα υποτίθεται ότι ο σταθερός όρος και ο μεγιστοβάθμιος συντελεστής στο πολυώνυμο γεννήτορα είναι μη μηδενικοί.

Παράδειγμα 3.1.6. Θεωρούμε το πολυώνυμο $\gamma(x) = 1+x+x^3 \in \mathbb{Z}_2[x]$ και $\mathcal{C}$ τον αντίστοιχο πολυωνυμικό κώδικα μήκους 6. Ας υπολογίσουμε τα στοιχεία του και ταυτόχρονα τη συνάρτηση κωδικοποίησης f από την πηγή $\mathbb{Z}_2^3$ στον κώδικα $\mathcal{C}$.

Έστω $(a_0, a_1, a_2) \in \mathbb{Z}_2^3$. Σχηματίζουμε το πολυώνυμο $\alpha(x) = a_0 + a_1x + a_2x^2$ και κάνουμε τον πολλαπλασιασμό $\alpha(x) \cdot \gamma(x) = a_0 + (a_0 + a_1)x + (a_1 + a_2)x^2 + (a_0 + a_2)x^3 + a_1x^4 + a_2x^5$. Επομένως, η συνάρτηση κωδικοποίησης είναι η $f(a_0, a_1, a_2) = (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2, a_1, a_2)$ και ο κώδικας $\mathcal{C} = \{ (a_0, a_0 + a_1, a_1 + a_2, a_0 + a_2, a_1, a_2) \mid (a_0, a_1, a_2) \in \mathbb{Z}_2^3 \}$.

Ας υπολογίσουμε έναν γεννήτορα πίνακα του κώδικα $\mathcal{C}$. Τα στοιχεία: $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$ αποτελούν μια βάση του $\mathbb{Z}_2^3$ και η απεικόνιση f είναι 1-1, επομένως οι εικόνες των στοιχείων της βάσης μέσω της f αποτελούν μια βάση του κώδικα. Έχουμε ότι $f(1, 0, 0) = (1, 1, 0, 1, 0, 0)$, $f(0, 1, 0) = (0, 1, 1, 0, 1, 0)$, $f(0, 0, 1) = (0, 0, 1, 1, 0, 1)$. Άρα, ένας γεννήτορας πίνακας του $\mathcal{C}$ είναι ο:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$ είναι ο πίνακας:

$$\mathrm{P} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

καθότι ισχύει $\mathrm{GP}^t = \mathbf{0}$ (Πρόταση 2.2.12).

Η ελάχιστη απόσταση του κώδικα είναι ίση με 3, σύμφωνα με την Πρόταση 2.2.25, (η πρώτη, δεύτερη και τέταρτη στήλη είναι γραμμικά εξαρτημένες, ενώ ανά δύο όλες οι στήλες είναι γραμμικά ανεξάρτητες).

Πρόταση 3.1.7. *Έστω $\mathcal{C}$ ένας πολυωνυμικός κώδικας μήκους n με πολυώνυμο γεννήτορα το $\gamma(x) = c_0 + c_1x + \cdots + c_kx^k$. Ένας γεννήτορας πίνακας*

του $\mathcal{C}$ είναι ο $(n-k)\times n$ πίνακας:

$$\mathrm{G} = \begin{pmatrix} c_0 & c_1 & \cdots & c_k & 0 & 0 & \cdots & 0 \\ 0 & c_0 & \cdots & c_{k-1} & c_k & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & c_0 & c_1 & \cdots & c_k \end{pmatrix}$$

Απόδειξη. Η διάσταση του κώδικα $\mathcal{C}$ είναι ίση με $m = n-k$, αφού η σύνθεση $\psi \circ \vartheta$ είναι 1-1.

Στην πρώτη γραμμή του πίνακα G τις $k+1$ πρώτες θέσεις καταλαμβάνουν οι συντελεστές του $c_0, c_1, \ldots, c_k$ του πολυωνύμου γεννήτορα και οι υπόλοιπες θέσεις είναι μηδενικά. Κάθε επόμενη γραμμή σχηματίζεται με μια κυκλική μετάθεση των στοιχείων της αμέσως προηγούμενης γραμμής έως ότου φθάσουμε στην τελευταία γραμμή, όπου οι τελευταίες $k+1$ θέσεις είναι $c_0, c_1, \ldots, c_k$. Επομένως, η τάξη του πίνακα είναι ίση με m.

Ο πολλαπλασιασμός ενός στοιχείου $(a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}^m$ (από αριστερά) με τον πίνακα G δίνει τους συντελεστές του γινομένου $\alpha(x)\cdot\gamma(x)$, όπου $\alpha(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} \in \mathbb{F}_{m-1}[x]$ και $\gamma(x) = c_0 + c_1 x + \cdots + c_k x^k$ το πολυώνυμο γεννήτορας. Άρα, ο κώδικας $\mathcal{C}$ συμπίπτει με τον κώδικα που έχει τον πίνακα G ως γεννήτορα πίνακα. ό.έ.δ.

Σχόλιο 3.1.8. Για την απόδειξη της προηγουμένης πρότασης θα μπορούσαμε να επιχειρηματολογήσουμε και ως εξής:

Η απεικόνιση $\psi \circ \vartheta$ είναι 1-1, οπότε η εικόνα της βάσης $\{1, x, \ldots, x^{m-1}\}$ του διανυσματικού χώρου $\mathbb{F}_{m-1}[x]$ δίνει μια βάση του κώδικα $\mathcal{C}$, της οποίας τα στοιχεία αποτελούν τις γραμμές του πίνακα G.

Έχουμε δει, στην παράγραφο 2.4.3, ότι σε έναν γραμμικό κώδικα μήκους n ένα διάνυσμα λάθους $\mathbf{e} = e_0\, e_1 \cdots e_{n-1}$ δεν ανιχνεύεται, αν και μόνο αν και αυτό είναι μια (κωδικο)λέξη. Για τους πολυωνυμικούς κώδικες έχουμε.

Πρόταση 3.1.9. *Σε έναν πολυωνυμικό κώδικα $\mathcal{C}$ ένα διάνυσμα λάθους $\mathbf{e} = e_0\, e_1 \cdots e_{n-1}$ δεν ανιχνεύεται αν και μόνο αν το αντίστοιχο πολυώνυμο $e(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$ είναι πολλαπλάσιο του πολυωνύμου γεννήτορα του κώδικα.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια των προηγουμένων και αφίεται ως άσκηση. ό.έ.δ.

Η επομένη πρόταση αποτελεί μια ικανή συνθήκη, ώστε ένας πολυωνυμικός κώδικας να διορθώνει τουλάχιστον ένα λάθος.

Πρόταση 3.1.10. *Έστω $\mathcal{C}$ ένας πολυωνυμικός κώδικας μήκους n με πολυώνυμο γεννήτορα $\gamma(x)$. Υποθέτουμε ότι το $\gamma(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής $x^r + c \in \mathbb{F}_{n-1}[x]$. Τότε η ελάχιστη απόσταση του $\mathcal{C}$ είναι τουλάχιστον τρία.*

Απόδειξη. Έστω $\gamma(x) = c_0 + c_1 x + \cdots + c_k x^k$. Κάθε στοιχείο του κώδικα διαιρείται από το $\gamma(x)$. Πρέπει να αποδείξουμε ότι δεν υπάρχει (κωδικο)λέξη με βάρος το πολύ 2. Από την Παρατήρηση 3.1.5$_4$ έπεται ότι αρκεί να αποδείξουμε ότι δεν υπάρχουν πολυώνυμα της μορφής $x^i + cx^j \in \mathbb{F}_{n-1}[x]$ με $i > j$ τα οποία να διαιρούνται από το $\gamma(x)$. Επειδή $c_0 \neq 0$ (βλέπε Παρατήρηση 3.1.5$_5$), έχουμε ότι τα πολυώνυμα $\gamma(x)$ και x^ℓ είναι σχετικά πρώτα για κάθε ℓ. Επομένως, αν υποθέσουμε ότι ένα πολυώνυμο της μορφής $x^i + cx^j = x^j(x^{i-j} + c)$ διαιρείται από το $\gamma(x)$, τότε θα έπρεπε το $x^{i-j} + c$ να διαιρείται από το $\gamma(x)$, άτοπο. ό.έ.δ.

Όπως παρατηρούμε το αποτέλεσμα που βρήκαμε για την ελάχιστη απόσταση του κώδικα στο Παράδειγμα 3.1.6, συνάδει με την προηγούμενη πρόταση, καθότι το πολυώνυμο γεννήτορας $\gamma(x) = 1 + x + x^3$ δεν διαιρεί κανένα από τα πολυώνυμα $x^4 + 1$ και $x^5 + 1$.

Υπενθυμίζουμε (βλέπε Ορισμός Α΄.3.4) ότι ο εκθέτης ενός πολυωνύμου $g(x)$ είναι ο μικρότερος θετικός ακέραιος k με την ιδιότητα το $g(x)$ να διαιρεί το $x^k - 1$.

Πρόταση 3.1.11. *Θεωρούμε έναν πολυωνυμικό κώδικα μήκους n επί του $\mathbb{Z}_2$, με πολυώνυμο γεννήτορα της μορφής $\gamma(x) = (x+1)h(x)$, όπου ο εκθέτης k του $h(x)$ είναι μεγαλύτερος του n. Τότε κάθε διάνυσμα λάθους με βάρος το πολύ δύο ανιχνεύεται. Επίσης, ανιχνεύονται και διανύσματα λάθους της μορφής $\mathbf{e}(x) = x^i + x^j + x^{j+1}$, της μορφής $\mathbf{e}(x) = x^i + x^{i+1} + x^j$ και της μορφής $\mathbf{e}(x) = x^i + x^{i+1} + x^j + x^{j+1}$.*

Απόδειξη. Επειδή ο εκθέτης του $h(x)$ είναι μεγαλύτερος του n, το πολυώνυμο γεννήτορας δεν διαιρεί κανένα πολυώνυμο της μορφής x^i+x^j, $i+1 \leq j \leq n-1$ ή x^i, όπως και πολυώνυμα της μορφής $x^i+x^j+x^{j+1}$, της μορφής $x^i+x^{i+1}+x^j$ και της μορφής $x^i + x^{i+1} + x^j + x^{j+1}$ (γιατί;)[1]. Οπότε το αποτέλεσμα έπεται από την Πρόταση 3.1.9. ό.έ.δ.

Η σημασία της προηγουμένης πρότασης έγκειται στο γεγονός ότι ενδέχεται να έχουμε έναν κώδικα με ελάχιστη απόσταση ίση με τρία και να μπορεί να ανιχνεύει ακόμα και τέσσερα το πλήθος λάθη (σύγκρινε με το Θεώρημα 1.3.14).

Βέβαια, τα επιπλέον λάθη που μπορεί να ανιχνευθούν είναι *δίδυμα* λάθη, δηλαδή σε μία (κωδικο)λέξη κατά την μετάδοση επήλθε αλλοίωση σε δύο διαδοχικούς χαρακτήρες.

Τώρα θα αποδείξουμε (δίνοντας ένα παράδειγμα) ότι ο δυϊκός κώδικας ενός πολυωνυμικού κώδικα δεν είναι κατ' ανάγκη πολυωνυμικός κώδικας.

Παράδειγμα 3.1.12. Έστω $\mathcal{C}$ ο δυαδικός πολυωνυμικός κώδικας μήκους 7 με πολυώνυμο γεννήτορα το $\gamma(x) = 1 + x + x^3$. Ένας γεννήτορας πίνακας είναι ο:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Ως γνωστόν, ένα στοιχείο $\mathbf{x} = x_1\, x_2\, x_3\, x_4\, x_5\, x_6\, x_7$ ανήκει στον δυϊκό κώδικα, αν και μόνο αν $\mathrm{G}\mathbf{x}^t = \mathbf{0}$. Από την τελευταία σχέση έπεται ότι ένας πίνακας ελέγχου ισοτιμίας για τον $\mathcal{C}$ είναι ο:

$$\mathrm{P} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

[1] Θα χρειασθεί να αποδείξετε (για να την εφαρμόσετε) την εξής απλή άσκηση: Ένα πολυώνυμο με συντελεστές από το $\mathbb{Z}_2$ διαιρείται με το $x+1$, αν και μόνο αν έχει άρτιο το πλήθος όρους.

(γιατί;). Επομένως, ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ έχει ως γεννήτορα πίνακα τον πίνακα P. Αν ο $\mathcal{C}^{\perp}$ ήταν πολυωνυμικός, θα είχε ένα γεννήτορα πολυώνυμο, έστω $g(x) = 1 + c_1x + c_2x^2 + c_3x^3 + c_4x^4$. Για κάθε πολύωνυμο $a_0 + a_1x + a_2x^2$ με συντελεστές από το $\mathbb{Z}_2$, οι συντελεστές του γινομένου $(a_0 + a_1x + a_2x^2)g(x)$ αποτελούν μια (κωδικο)λέξη του $\mathcal{C}^{\perp}$, την $(a_0\, a_1\, a_2)$P. Εκτελούμε τον παραπάνω πολλαπλασιασμό πολυωνύμων, τον πολλαπλασιασμό $(a_0\, a_1\, a_2)$P και συγκρίνουμε τα δύο αποτελέσματα. Πρέπει να ισχύει:

$$\begin{aligned} a_0 &= a_0 \\ a_0c_1 + a_1 &= a_1 \\ a_0c_2 + a_1c_1 + a_2 &= a_2 \\ a_0c_3 + a_1c_2 + a_2c_1 &= a_0 + a_1 \\ a_0c_4 + a_1c_3 + a_2c_2 &= a_1 + a_2 \\ a_1c_4 + a_2c_3 &= a_0 + a_1 + a_2 \\ a_2c_4 &= a_0 + a_2 \end{aligned}$$

Από τη δεύτερη και τρίτη ισότητα έπεται ότι τα c_1 και c_2 πρέπει να είναι ίσα με μηδέν, οπότε η τέταρτη ισότητα γίνεται $a_0c_3 = a_0 + a_1$. Η ισότητα αυτή θα πρέπει να ισχύει για κάθε $a_0, a_1 \in \mathbb{Z}_2$. Αυτό όμως είναι αδύνατον (γιατί;). Άρα, ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ δεν είναι πολυωνυμικός.

3.1.1 Ασκήσεις

1. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας και την ελάχιστη απόσταση στις ακόλουθες περιπτώσεις πολυωνυμικών δυαδικών κωδίκων με αντίστοιχα πολυώνυμα γεννήτορες $1+x+x^2$, $1+x+x^3$, $1+x^2$, $1+x^3$ και με μήκος 5 ή 8.

2. Στην προηγούμενη άσκηση, σε κάθε περίπτωση, να εξετάσετε ποίοι από τους αντίστοιχους δυϊκούς κώδικες είναι πολυωνυμικοί.

3. Να δώσετε ικανή και αναγκαία συνθήκηκ, ώστε ένας πολυωνυμικός κώδικας να είναι κώδικας μέγιστης απόστασης.

4. Να μελετήσετε όλους τους πολυωνυμικούς κώδικες μήκους πέντε επί του σώματος $\mathbb{Z}_3$.

3.2 Κυκλικοί κώδικες

Μια ειδική, αλλά η πλέον ενδιαφέρουσα, κατηγορία πολυωνυμικών κωδίκων είναι οι κυκλικοί κώδικες. Οι κυκλικοί κώδικες έχουν πλούσια αλγεβρική δομή, η οποία τους καθιστά αποτελεσματικούς και όπως θα δούμε στα επόμενα, οι πλέον σημαντικές οικογένειες κωδίκων περιλαμβάνουν κώδικες ισοδύναμους με κυκλικούς κώδικες.

Ορισμός 3.2.1. *Ένας γραμμικός κώδικας $\mathcal{C}$ μήκους n, επί του πεπερασμένου σώματος $\mathbb{F}$, θα λέγεται κυκλικός, αν για κάθε (κωδικο)λέξη $\mathbf{c} = c_0\, c_1 \cdots c_{n-1}$, η λέξη που προκύπτει με μια κυκλική μετάθεση των χαρακτήρων της κατά ένα βήμα, δηλαδή η λέξη $c_{n-1}\, c_0\, c_1 \cdots c_{n-2}$, είναι και αυτή στοιχείο του κώδικα.*

Από τον ορισμό έπεται αμέσως ότι για κάθε $k \in \mathbb{N}$ με $1 \leq k \leq n-1$ η λέξη $c_k \cdots c_{n-1}\, c_0\, c_1 \cdots c_{k-1}$ είναι και αυτή στοιχείο του κώδικα.

Παραδείγματα 3.2.2. 1. Οι ακραίες περιπτώσεις του μηδενικού κώδικα και του κώδικα που είναι όλος ο διανυσματικός χώρος $\mathbb{F}^n$, αποτελούν τετριμμένα παραδείγματα κυκλικών κωδίκων.

2. Προφανώς, ο επαναληπτικός κώδικας:

$$\mathcal{R}_p(k) = \{\ \underbrace{00\cdots0}_{k-\text{φορές}}\ ,\ \underbrace{11\cdots1}_{k-\text{φορές}}\ , \ldots, \underbrace{(p-1)\,(p-1)\cdots(p-1)}_{k-\text{φορές}}\}$$

είναι κυκλικός.

3. Ο δυαδικός κώδικας: $\mathcal{C} = \{\,000,\, 101,\, 011,\, 110\,\}$ προφανώς είναι κυκλικός κώδικας.

4. Ο δυαδικός πολυωνυμικός κώδικας $[7,\, 4,\, 3]\mathcal{C}$ του Παραδείγματος 3.1.12 με γεννήτορα πίνακα:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

είναι εύκολο να διαπιστώσουμε ότι είναι ένας κυκλικός κώδικας.

5. Ο δυαδικός κώδικας $\mathcal{C} = \{\, 0000,\ 1001,\ 0110,\ 1111 \,\}$ δεν είναι κυκλικός (γιατί;). Αντιμεταθέτοντας όμως τους χαρακτήρες της τρίτης και τέταρτης θέσης λαμβάνουμε τον κώδικα $\mathcal{D} = \{\, 0000,\ 1010,\ 0101,\ 1111 \,\}$, ο οποίος είναι κυκλικός. Δηλαδή υπάρχουν μη κυκλικοί γραμμικοί κώδικες οι οποίοι είναι ισοδύναμοι με κυκλικούς κώδικες.

6. Ο κώδικας $\mathcal{E}_n$ που αποτελείται από όλες τις λέξεις μήκους n με άθροισμα χαρακτήρων ίσον με μηδέν (βλέπε Παράδειγμα 2.1.2$_5$) είναι ένας κυκλικός κώδικας (γιατί;)

Όπως και στην προηγουμένη παράγραφο, σύμφωνα με την Πρόταση 3.1.1, θα ταυτίζουμε γραμμικούς κώδικες μήκους n με υποχώρους του $\mathbb{F}_{n-1}[x]$.

Έστω τώρα ένας γραμμικός κώδικας $\mathcal{C}$ μήκους n και $a_0\, a_1 \cdots a_{n-1}$ ένα στοιχείο του. Σύμφωνα με τα προηγούμενα, στο στοιχείο αυτό αντιστοιχούμε το πολυώνυμο $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Πολλαπλασιάζοντας το πολυώνυμο αυτό με x έχουμε $x(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n$. Αν στην τελευταία σχέση *αντικαταστήσουμε* το x^n με το 1, έχουμε το πολυώνυμο $a_{n-1} + a_0 x + a_1 x^2 + \cdots + a_{n-2}x^{n-1}$, οπότε παρατηρούμε ότι οι συντελεστές $a_{n-1}\, a_0\, a_1 \cdots a_{n-2}$ του τελευταίου πολυωνύμου αντιστοιχούν σε μια κυκλική μετάθεση κατά μια θέση των χαρακτήρων της (κωδικο)λέξης $a_0\, a_1 \cdots a_{n-1}$. Όμοια, μια κυκλική μετάθεση κατά k το πλήθος θέσεις *αντιστοιχεί* σε πολλαπλασιασμό του πολυωνύμου $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ με x^k και *αντικατάσταση* του x^n με το 1. Επομένως, είναι φανερό ότι οι κυκλικοί κώδικες έχουν σχέση με την *αντικατάσταση* του x^n με το 1. Η διαδικασία όμως αυτή δεν είναι τίποτε άλλο από το να διαιρέσουμε ένα πολυωνύμο με το $x^n - 1$ και να κρατήσουμε το υπόλοιπο της διαίρεσης. Πράγματι, έστω $\phi(x) \in \mathbb{F}[x]$, από την ταυτότητα της διαίρεσης πολυωνύμων έχουμε ότι υπάρχουν (μοναδικά) $\pi(x),\ \upsilon(x) \in \mathbb{F}[x]$, τέτοια ώστε $\phi(x) = \pi(x) \cdot (x^n - 1) + \upsilon(x)$ και $\upsilon(x) = 0$ ή $deg(\upsilon(x)) \leq n - 1$. Οπότε για $x^n = 1$ στη θέση του $\phi(x)$ έχουμε το υπόλοιπο $\upsilon(x)$.

Προσοχή! Όταν λέμε αντικαθιστούμε το x^n με το 1, εννοούμε ότι αντικαθιστούμε το πολυώνυμο x^n με το σταθερό πολυώνυμο 1 και **όχι** ότι το x^n λαμβάνει την τιμή 1.

Έστω $\tau_1(x), \tau_2(x) \in \mathbb{F}_{n-1}[x]$. Από την ταυτότητα της διαίρεσης πολυωνύμων έχουμε ότι υπάρχουν (μοναδικά) $\pi(x), \upsilon(x) \in \mathbb{F}_{n-1}[x]$, τέτοια ώστε $\tau_1(x) \cdot \tau_2(x) = \pi(x) \cdot (x^n - 1) + \upsilon(x)$ και $\upsilon(x) = 0$ ή $deg(\upsilon(x)) \leq n-1$. Στο σύνολο $\mathbb{F}_{n-1}[x]$ ορίζουμε έναν *πολλαπλασιασμό* πολυωνύμων ως εξής:

$$\tau_1(x) \odot \tau_2(x) =: \upsilon(x),$$

όπου $\upsilon(x)$ είναι το υπόλοιπο της προηγούμενης διαίρεσης. Ο πολλαπλασιασμός αυτός θα λέγεται **πολλαπλασιασμός** $\bmod (x^n - 1)$.

Για παράδειγμα, αν $x^3+x+1, x^2+x+1 \in \mathbb{Z}_2[x]$, τότε $(x^3+x+1)\cdot(x^2+x+1) = x^5+x+1 = (x+1)\cdot(x^4+1)+x \in Z_2[x]$, οπότε $(x^3+x+1)\odot(x^2+x+1) = x$.

Δεν είναι δύσκολο να δούμε ότι το σύνολο $\mathbb{F}_{n-1}[x]$ με πράξεις την πρόσθεση πολυωνύμων και τον πολλαπλασιασμό $\bmod (x^n - 1)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. (Ως άσκηση μπορείτε να ελέγξετε την προσεταιριστική ιδιότητα του πολλαπλασιασμού.)

Σημείωση: Στα επόμενα πολλές φορές, όταν δεν υπάρχει κίνδυνος σύγχυσης, τον πολλαπλασιασμό $\bmod (x^n - 1)$ θα τον συμβολίζουμε $\tau_1(x) \cdot \tau_2(x)$, όπως τον συνήθη πολλαπλασιασμό πολυωνύμων.

Χρησιμοποιώντας την έννοια του ιδεώδους και την έννοια του δακτυλίου πηλίκων, μπορούμε να περιγράψουμε κομψά την παραπάνω διαδικασία και τους κυκλικούς κώδικες.

Έστω $\mathbb{F}[x]$ ο δακτύλιος όλων των πολυωνύμων με συντελεστές από το σώμα $\mathbb{F}$ και $\langle x^n - 1\rangle$ το (κύριο) ιδεώδες το παραγόμενο από το πολυώνυμο x^n-1. Δηλαδή $\langle x^n-1\rangle = \{\, \sigma(x)\cdot(x^n-1) \mid \sigma(x) \in \mathbb{F}[x] \,\}$. Ο δακτύλιος πηλίκων $\mathbb{F}[x]/\langle x^n-1\rangle$ αποτελείται από όλα τα σύμπλοκα της μορφής $\tau(x)+\langle x^n-1\rangle$ με $\tau(x) \in \mathbb{F}[x]$. Δύο στοιχεία $\tau_1(x)+\langle x^n-1\rangle$ και $\tau_2(x)+\langle x^n-1\rangle$ του $\mathbb{F}[x]/\langle x^n-1\rangle$ είναι ίσα, αν και μόνο αν η διαφορά $\tau_1(x)-\tau_2(x)$ ανήκει στο ιδεώδες $\langle x^n-1\rangle$ ή ισοδύναμα διαιρείται από το x^n-1.

Πρόταση 3.2.3. *Η απεικόνιση $\varphi : \mathbb{F}_{n-1}[x] \longrightarrow \mathbb{F}[x]/\langle x^n-1\rangle$ με $\varphi(\tau(x)) = \tau(x)+\langle x^n-1\rangle$ είναι ένας ισομορφισμός δακτυλίων.*

Απόδειξη. Ο έλεγχος ότι η απεικόνιση φ πληροί τις παραπάνω ιδιότητες είναι απλός και αφίεται ως άσκηση. ό.έ.δ.

Ο προηγούμενος ισομορφισμός μας επιτρέπει να *ταυτίσουμε* τους δύο δακτυλίους και στα επόμενα θα τους συμβολίζουμε χωρίς διάκριση με $\mathcal{R}_n$ ($\mathcal{R}_n := \mathbb{F}_{n-1}[x] \cong_{\varphi} \mathbb{F}[x]/\langle x^n - 1\rangle$).

Μέσω αυτού του ισομορφισμού είναι φανερό γιατί αντικαθιστούμε το x^n με το 1, καθότι $x^n + \langle x^n - 1\rangle = 1 + \langle x^n - 1\rangle$.

Έστω τώρα $\mathcal{C}$ ένας κώδικας μήκους n, δηλαδή $\mathcal{C} \subseteq \mathbb{F}^n$. Από την Πρόταση 3.1.1 και την προηγούμενη πρόταση, επειδή οι απεικονίσεις φ και ψ^{-1} είναι 1-1, στα επόμενα θα μπορούμε να ταυτίσουμε τον κώδικα $\mathcal{C}$ με την εικόνα του και να τον θεωρούμε ως υποσύνολο του $\mathcal{R}_n$.

Θεώρημα 3.2.4. *Ένας κώδικας $\mathcal{C}$ είναι κυκλικός, αν και μόνο αν είναι ένα ιδεώδες του δακτυλίου $\mathcal{R}_n$.*

Απόδειξη. Υποθέτουμε ότι ο κώδικας είναι κυκλικός. Τότε για: $\alpha_1(x), \alpha_2(x) \in \mathcal{C} \subseteq \mathcal{R}_n$ έχουμε ότι:

$$\alpha_1(x) - \alpha_2(x) \in \mathcal{C}, \qquad (i)$$

αφού ο $\mathcal{C}$ είναι γραμμικός.

Έστω τώρα $\alpha(x) \in \mathcal{C}$ και $\tau(x) = r_0 + r_1 x + \cdots + r_k x^k \in \mathcal{R}_n$. Από τα προηγούμενα έχουμε ότι ο πολλαπλασιασμός του $\alpha(x)$ με x αντιστοιχεί με μια κυκλική μετάθεση κατά μια θέση, δηλαδή $x \cdot \alpha(x) \in \mathcal{C}$, αφού ο $\mathcal{C}$ είναι κυκλικός, όμοια $x^2 \cdot \alpha(x), \ldots, x^k \cdot \alpha(x) \in \mathcal{C}$. Επομένως:

$$\tau(x) \cdot \alpha(x) = r_0\alpha(x) + r_1 x\alpha(x) + \cdots + r_k x^k \alpha(x) \in \mathcal{C}. \qquad (ii)$$

(Δεν ξεχνάμε ότι ο πολλαπλασιασμός πολυωνύμων είναι $\mod (x^n - 1)$.) Από τις σχέσεις (i) και (ii) έπεται ότι ο $\mathcal{C}$ είναι ένα ιδεώδες του $\mathcal{R}_n$.

Αντίστροφα, υποθέτουμε ότι ο κώδικας $\mathcal{C}$ είναι ένα ιδεώδες του $\mathcal{R}_n$, δηλαδή ισχύουν οι (i) και (ii). Αν στη θέση του $\tau(x)$ στη σχέση (ii) θέσουμε ένα σταθερό πολυώνυμο, αποδεικνύουμε [σε συνδυασμό με τη σχέση (i)] ότι ο κώδικας είναι γραμμικός. Αν στη θέση του $\tau(x)$ στη σχέση (ii) θέσουμε το πολυώνυμο x, αποδεικνύουμε ότι ο κώδικας είναι κυκλικός. ό.έ.δ.

Από το προηγούμενο θεώρημα έπεται ότι για να υπολογίσουμε όλους τους κυκλικούς κώδικες μήκους n (πρέπει και) αρκεί να υπολογίσουμε όλα τα ιδεώδη του δακτυλίου $\mathcal{R}_n$.

Ένας τρόπος κατασκευής κυκλικών κωδίκων (και όπως θα δούμε στα επόμενα ο μοναδικός) είναι να θεωρήσουμε τα κύρια ιδεώδη του δακτυλίου $\mathcal{R}_n$. Έστω $p(x) \in \mathcal{R}_n$. Τότε το (κύριο) ιδεώδες το παραγόμενο από το $p(x)$ αποτελείται από όλα τα πολλαπλάσια του $p(x)$, δηλαδή $\langle\, p(x)\,\rangle = \{\, r(x)\cdot p(x) \mid r(x) \in \mathcal{R}_n \,\}$. Σύμφωνα με τα προηγούμενα το $\mathcal{C} = \langle\, p(x)\,\rangle = \{\, r(x)\cdot p(x) \mid r(x) \in \mathcal{R}_n \,\}$ είναι ένας κυκλικός κώδικας που παράγεται από το πολυώνυμο $p(x)$.

Παράδειγμα 3.2.5. Έστω $\mathcal{C}$ ο δυαδικός κυκλικός κώδικας $\langle\, 1+x^2\,\rangle = \{\, r(x)\cdot (1+x^2) \mid r(x) \in \mathcal{R}_3 \,\}$. Το $\mathcal{R}_3$ αποτελείται από οκτώ στοιχεία (τα δυνατά υπόλοιπα της διαίρεσης ενός πολυωνύμου $r(x) \in \mathbb{Z}_2[x]$ με το x^3-1), δηλαδή $\mathcal{R}_3 = \{\, 0,\, 1,\, x,\, 1+x,\, x^2,\, 1+x^2,\, x+x^2,\, 1+x+x^2 \,\}$. Οπότε κάνοντας τους πολλαπλασιασμούς ($\bmod (x^3-1)$), βρίσκουμε ότι $\mathcal{C} = \{\, 0,\, 1+x,\, 1+x^2,\, x+x^2 \,\}$. Δηλαδή $\mathcal{C} = \{\, 000,\, 110,\, 101,\, 011 \,\}$, ο κώδικας του Παραδείγματος 3.2.2$_2$.

Θεώρημα 3.2.6. *Έστω $\mathcal{C}$ ένας μη μηδενικός κυκλικός κώδικας μήκους n. Τότε υπάρχει μοναδικό μονικό πολυώνυμο $\gamma(x) \in \mathcal{R}_n$ ελαχίστου βαθμού, έτσι ώστε $\mathcal{C} = \langle \gamma(x) \rangle$. Επιπλέον, το πολυώνυμο $\gamma(x)$ διαιρεί το πολυώνυμο $x^n - 1$.*

Απόδειξη. Έστω $\alpha(x),\, \beta(x) \in \mathcal{C}$ δύο διαφορετικά μονικά πολυώνυμα με τον μικρότερο δυνατόν βαθμό. Ο κώδικας είναι γραμμικός, επομένως η διαφορά $\alpha(x) - \beta(x) \in \mathcal{C}$ έχει βαθμό μικρότερο από τον βαθμό των $\alpha(x)$ και $\beta(x)$. Πολλαπλασιάζοντας το $\alpha(x) - \beta(x)$ με τον αντίστροφο συντελεστή του μεγιστοβαθμίου όρου, έχουμε ένα πολυώνυμο, το οποίο ανήκει στον κώδικα $\mathcal{C}$, είναι μονικό και έχει βαθμό μικρότερο από τον βαθμό των $\alpha(x)$ και $\beta(x)$, άτοπο.

Έστω $\gamma(x)$ το μοναδικό μονικό πολυώνυμο ελαχίστου βαθμού στον $\mathcal{C}$ και $\alpha(x) \in \mathcal{C}$. Από την ταυτότητα της διαίρεσης στο $\mathbb{F}[x]$ έχουμε ότι υπάρχουν πολυώνυμα $\pi(x),\, \upsilon(x) \in \mathbb{F}[x]$, τέτοια ώστε $\alpha(x) = \pi(x)\cdot\gamma(x) + \upsilon(x)$ με $\upsilon(x) = 0$ ή $deg(\upsilon(x)) < deg(\gamma(x))$. Από το Θεώρημα 3.2.4 έπεται ότι $\upsilon(x) = \alpha(x) - \pi(x)\cdot\gamma(x) \in \mathcal{C}$. Επειδή το $\gamma(x)$ είναι ελαχίστου βαθμού (και ο κώδικας γραμμικός), έπεται ότι $\upsilon(x) = 0$ και επομένως $\mathcal{C} = \langle \gamma(x) \rangle$.

Επίσης, από την ταυτότητα της διαίρεσης στο $\mathbb{F}[x]$ έχουμε ότι υπάρχουν

πολυώνυμα $\pi_1(x), \upsilon_1(x) \in \mathbb{F}[x]$, τέτοια ώστε $x^n - 1 = \pi_1(x) \cdot \gamma(x) + \upsilon_1(x)$ με $\upsilon_1(x) = 0$ ή $deg(\upsilon_1(x)) < deg(\gamma(x))$. Αλλά $x^n - 1 = 0 \in \mathcal{R}_n$. Επομένως, $\upsilon_1(x) = -\pi_1(x) \cdot \gamma(x) \in \mathcal{C} = \langle \gamma(x) \rangle$. Άρα $\upsilon_1(x) = 0$. ό.έ.δ.

Παρατήρηση 3.2.7. Για όσους είναι εξοικειωμένοι με τις στοιχειώδεις ιδιότητες των ιδεωδών και του δακτυλίου πηλίκων, το προηγούμενο θεώρημα είναι μια μερική περίπτωση της εξής γενικής πρότασης:

Για τους μη εξοικειωμένους με την έννοια του ιδεώδους συνιστάται να ανατρέξουνε σε ένα βιβλίο Βασικής Άλγεβρας, για παράδειγμα σε ένα από τα Ανδρεαδάκης [1993], Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη [2013] και Herstein, I. N. [1990].

Έστω $\mathbb{F}$ ένα σώμα (όχι κατ' ανάγκη πεπερασμένο). Κάθε ιδεώδες του δακτυλίου $\mathbb{F}[x]$ είναι κύριο. Αν $I = \langle r(x) \rangle$, $J = \langle s(x) \rangle$ είναι ιδεώδη του $\mathbb{F}[x]$ με $I \subseteq J$, τότε το πολυώνυμο $s(x)$ διαιρεί το $r(x)$. Επιπλέον, κάθε ιδεώδες του δακτυλίου $\mathbb{F}[x]/I$ είναι της μορφής K/I, όπου K είναι ένα ιδεώδες του $\mathbb{F}[x]$ με $I \subseteq K$.

Η απόδειξη είναι (ακριβώς) ίδια με την απόδειξη της προηγούμενης πρότασης.

Το μοναδικό μονικό πολυώνυμο $\gamma(x)$, που υπάρχει από το προηγούμενο θεώρημα, θα λέγεται το **πολυώνυμο γεννήτορας** του κώδικα $\mathcal{C}$.

Εδώ θα θέλαμε να επισημάνουμε ότι ένας κυκλικός κώδικας $\mathcal{C}$ ως κύριο ιδεώδες του δακτυλίου $\mathcal{R}_n$ ενδέχεται να παράγεται από περισσότερα του ενός πολυωνύμων, δηλαδή να υπάρχουν περισσότερα του ενός πολυώνυμα $f(x) \in \mathcal{R}_n$ έτσι ώστε $\mathcal{C} = \langle f(x) \rangle$, **όμως** υπάρχει μόνο ένα πολυώνυμο γεννήτορας.

Στο προηγούμενο παράδειγμα ο κώδικας $\mathcal{C} = \langle 1 + x^2 \rangle$ παράγεται μεν από το πολυώνυμο $1 + x^2$, αλλά το πολυώνυμο γεννήτορας είναι το $1 + x$ (γιατί;)

Μπορούμε να δώσουμε έναν χαρακτηρισμό για το πότε ένα πολυώνυμο στον δακτύλιο $\mathcal{R}_n$ παράγει έναν κυκλικό κώδικα.

Πρόταση 3.2.8. *Έστω $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με πολυώνυμο γεννήτορα $\gamma(x)$ και $r(x) \in \mathcal{R}_n$.*

Το $r(x)$ παράγει τον $\mathcal{C}$ (ως κύριο ιδεώδες), αν και μόνο αν

$$\text{μκδ}(r(x),\, x^n - 1) = \gamma(x).$$

Αν και μόνο αν κάθε ρίζα του $r(x)$ είναι ρίζα του $\gamma(x)$.

Απόδειξη. Υποθέτουμε ότι το $r(x)$ παράγει τον κώδικα $\mathcal{C}$. Τότε ισχύει ότι $\gamma(x) = \alpha(x)r(x)$. Επίσης, επειδή το $\gamma(x)$ παράγει τον κώδικα, έχουμε ότι $r(x) = \beta(x)\gamma(x)$. Δηλαδή στον δακτύλιο $\mathcal{R}_n =: \mathbb{F}[x]/\langle x^n - 1\rangle$ τα πολυώνυμα $\alpha(x)$ και $\beta(x)$ το ένα είναι αντίστροφο του άλλου. Αυτό σημαίνει ότι $\alpha(x)\beta(x) = 1+\delta(x)(x^n-1)$ στον δακτύλιο $\mathbb{F}[x]$, δηλαδή $\text{μκδ}(\beta(x),\, x^n-1) = 1$. Συνεπώς, $\text{μκδ}(r(x),\, x^n - 1) = \text{μκδ}(\beta(x)\gamma(x),\, x^n - 1) = \gamma(x)$, αφού το $\gamma(x)$ διαιρεί το $x^n - 1$.

Αντίστροφα, υποθέτουμε ότι $\text{μκδ}(\, r(x),\, x^n - 1\,) = \gamma(x)$, δηλαδή το $\gamma(x)$ διαιρεί το $r(x)$. Επομένως, κάθε πολλαπλάσιο του $r(x)$ είναι και πολλαπλάσιο του $\gamma(x)$ στον δακτύλιο $\mathcal{R}_n$. Αυτό σημαίνει ότι $\langle\, r(x)\,\rangle \subseteq \mathcal{C}$. Επίσης, από το ότι $\text{μκδ}(\, r(x),\, x^n-1\,) = \gamma(x)$, έχουμε ότι $\gamma(x) = \sigma(x)r(x)+\phi(x)(x^n-1)$, αλλά $x^n - 1 = 0 \in \mathcal{R}_n$. Συνεπώς, $\gamma(x) = \sigma(x)r(x) \in \mathcal{R}_n$, άρα $\langle\, r(x)\,\rangle \supseteq \mathcal{C}$.

Με την υπόθεση τώρα ότι το $r(x)$ παράγει τον κώδικα, έχουμε ότι $\gamma(x) = \alpha(x)r(x)$. Επίσης, επειδή το $\gamma(x)$ παράγει τον κώδικα, έχουμε ότι $r(x) = \beta(x)\gamma(x)$. Συνεπώς, κάθε ρίζα του $r(x)$ είναι και ρίζα του $\gamma(x)$ και κάθε ρίζα του $\gamma(x)$ είναι και ρίζα του $r(x)$.

Αντίστροφα, αν οι ρίζες του $r(x)$ είναι ακριβώς οι ρίζες του $\gamma(x)$, δεδομένου ότι το $\gamma(x)$ διαιρεί το $x^n - 1$, έχουμε ότι $\gamma(x) = \text{μκδ}(\, r(x),\, x^n - 1\,)$, δηλαδή το το $r(x)$ παράγει τον κώδικα, από το πρώτο μέρος της απόδειξης. ό.έ.δ.

Οι ρίζες του πολυωνύμου γεννήτορα ενός κυκλικού κώδικα θα ονομάζονται **σημεία μηδενισμού** ή απλώς **μηδενικά** του κώδικα.

Σημείωση: Στην απόδειξη της προηγουμένης πρότασης τα πολυώνυμα άλλοτε θεωρούνται ως στοιχεία του δακτυλίου $\mathbb{F}[x]$ και άλλοτε ως στοιχεία του δακτυλίου πηλίκων $\mathcal{R}_n =: \mathbb{F}[x]/\langle x^n - 1\rangle$. Αυτό, όπως άλλωστε έχουμε επισημάνει, δεν πρέπει να μας δημιουργεί σύγχυση, αρκεί να είμαστε προσεκτικοί κάθε φορά σε ποιόν δακτύλιο αναφερόμαστε.

Θεώρημα 3.2.9. *Ένα μονικό πολυώνυμο $g(x) \in \mathcal{R}_n$ είναι το πολυώνυμο γεννήτορας ενός κυκλικού κώδικα $\mathcal{C} \subseteq \mathcal{R}_n$, αν και μόνο αν το $g(x)$ διαιρεί το $x^n - 1$.*

Απόδειξη. Η μια κατεύθυνση έχει ήδη αποδειχθεί στο Θεώρημα 3.2.6.

Υποθέτουμε ότι το $g(x)$ διαιρεί το $x^n - 1$, δηλαδή $x^n - 1 = t(x) \cdot g(x)$. Έστω $\mathcal{C}$ ο κυκλικός κώδικας $\langle\, g(x) \,\rangle$. Από το προηγούμενο θεώρημα υπάρχει το πολυώνυμο γεννήτορας, έστω $\gamma(x)$, του $\mathcal{C}$. Υποθέτουμε ότι $\gamma(x) \neq g(x)$. Το $\gamma(x)$ είναι το πολυώνυμο γεννήτορας και το $g(x)$ μονικό, επομένως ο βαθμός του είναι (γνήσια) μικρότερος από τον βαθμό του $g(x)$. Επειδή $\gamma(x) \in \mathcal{C} = \langle\, g(x) \,\rangle$, υπάρχει πολυώνυμο $r(x)$, έτσι ώστε $\gamma(x) = g(x) \cdot r(x)$. Ο τελευταίος πολλαπλασιασμός είναι $\mod (x^n - 1)$. Αυτό σημαίνει ότι υπάρχει πολυώνυμο $\pi(x)$, έτσι ώστε $\gamma(x) = g(x) \cdot r(x) + \pi(x) \cdot (x^n - 1)$. Πολλαπλασιάζοντας την τελευταια σχέση με $t(x)$ έχουμε $t(x) \cdot \gamma(x) = t(x) \cdot (g(x) \cdot r(x) + \pi(x) \cdot (x^n - 1)) = (t(x) \cdot g(x)) \cdot r(x) + t(x) \cdot \pi(x) \cdot (x^n - 1)$. Αλλά $x^n - 1 = t(x) \cdot g(x)$, οπότε, αντικαθιστώντας στην τελευταία σχέση, έχουμε $t(x) \cdot \gamma(x) = (x^n - 1) \cdot r(x) + t(x) \cdot \pi(x) \cdot (x^n - 1) = (x^n - 1) \cdot (r(x) + t(x) \cdot \pi(x))$. Από την τελευταία σχέση έχουμε ότι ο βαθμός του γινομένου $t(x) \cdot \gamma(x)$ είναι μεγαλύτερος ή ίσος του γινομένου $t(x) \cdot g(x)$. Αυτό έρχεται σε αντίφαση με το ότι ο βαθμός του $\gamma(x)$ είναι (γνήσια) μικρότερος από τον βαθμό του $g(x)$. Άρα $g(x) = \gamma(x)$. ό.έ.δ.

Από τα δύο προηγούμενα θεωρήματα είναι φανερό ότι το πρόβλημα του προσδιορισμού όλων των κυκλικών κωδικών μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$ είναι ισοδύναμο με τον προσδιορισμό της ανάλυσης του πολυωνύμου $x^n - 1$ σε γινόμενο (αναγώγων) παραγόντων επί του $\mathbb{F}$.

Εδώ πρέπει να επισημάνουμε ότι αν $n = p^r \cdot m$, όπου p είναι η χαρακτηριστική του σώματος $\mathbb{F}$, με p να μην διαιρεί τον m, τότε $x^n - 1 = (x^m - 1)^{p^r}$. Επομένως, το πρόβλημα ανάγεται στην παραγοντοποίηση πολυωνύμων της μορφής $x^n - 1$ με p να μην διαιρεί τον n.[2]

Παράδειγμα 3.2.10. Θεωρούμε το πολυώνυμο $x^3 - 1 \in \mathbb{Z}_2[x]$. Προφανώς, $x^3 - 1 = (x + 1)(x^2 + x + 1)$. Επομένως υπάρχουν τέσσερεις διαιρέτες του

[2] Για τον λόγο αυτό, θα υποθέτουμε *σιωπηλά* (χωρίς βλάβη της γενικότητας) ότι ο p δεν διαιρεί τον n.

x^3-1, οι 1, $x+1$, x^2+x+1 και $(x+1)(x^2+x+1)=x^3-1$. Οι αντίστοιχοι κυκλικοί κώδικες είναι οι εξής:

$$\begin{aligned}
\langle 1\rangle &= \mathcal{R}_3 = \{\,000,\,001,\,010,\,011,\,100,\,101,\,110,\,111\,\}\\
\langle x+1\rangle &= \{\,0,\,1+x,\,x+x^2,\,1+x^2\,\} = \{\,000,\,110,\,011,\,101\,\}\\
\langle x^2+x+1\rangle &= \{\,0,\,1+x+x^2\,\} = \{\,000,\,111\,\}\\
\langle x^3-1\rangle &= \{\,0\,\} = \{\,000\,\}
\end{aligned}$$

Από το Θεώρημα 3.2.6 έχουμε ότι ένας κυκλικός κώδικας είναι πολυωνυμικός, επομένως μπορούμε να αποδείξουμε μια πρόταση ανάλογη με την Πρόταση 3.1.7.

Πρόταση 3.2.11. *Έστω $\mathcal{C}\subseteq\mathcal{R}_n$ ένας κυκλικός κώδικας με πολυώνυμο γεννήτορα $\gamma(x)=c_0+c_1x+\cdots+c_kx^k$. Τότε $c_0\neq 0$, η διάστασή του είναι ίση με $n-k$ και ένας γεννήτορας πίνακας είναι ο $(n-k)\times n$ πίνακας:*

$$\mathrm{G}=\begin{pmatrix}
c_0 & c_1 & \cdots & c_k & 0 & 0 & \cdots & 0\\
0 & c_0 & \cdots & c_{k-1} & c_k & 0 & \cdots & 0\\
\vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots\\
0 & 0 & \cdots & 0 & c_0 & c_1 & \cdots & c_k
\end{pmatrix}$$

Απόδειξη. Υποθέτουμε ότι $c_0=0$. Τότε το $x^{n-1}\gamma(x)=x^{-1}\gamma(x)$ ανήκει στον κώδικα και έχει βαθμό ίσον με $k-1$, μικρότερο από τον βαθμό του $\gamma(x)$, άτοπο.

Η απόδειξη τώρα είναι παρόμοια με την απόδειξη της Πρότασης 3.1.7. ό.έ.δ.

Παρατηρήσεις 3.2.12.

1. Στην περίπτωση των πολυωνυμικών κωδίκων είχαμε δει ότι μπορούμε να υποθέσουμε ότι ο σταθερός όρος του πολυωνύμου γεννήτορα είναι διάφορος του μηδενός (βλέπε Παρατήρηση 3.1.5 $_5$). Στους κυκλικούς κώδικες αποδείξαμε ότι ο σταθερός όρος του πολυωνύμου γεννήτορα είναι διάφορος του μηδενός.

2. Δεν είναι δύσκολο να δούμε ότι το σύνολο:

$$\{\,\gamma(x),\,x\gamma(x),\,x^2\gamma(x),\,\ldots\,,\,x^{n-k-1}\gamma(x)\,\}$$

είναι μια βάση του κώδικα $\mathcal{C}$ (γιατί;), επομένως έχουμε μια άλλη απόδειξη της προηγουμένης πρότασης.

3. Στην προηγούμενη πρόταση, από τον ορισμό του πολυωνύμου γεννήτορα, έπεται ότι $c_k = 1$. Στη συγκεκριμμένη περίπτωση θα μπορούσαμε να υποθέσουμε ότι ο c_k δεν είναι κατ' ανάγκην ίσος με 1, καθότι γενικά ισχύει ότι τα πολυώνυμα $\varphi(x)$ και $a\varphi(x)$ παράγουν το ίδιο ιδεώδες για κάθε μη μηδενικό στοιχείο a του σώματος.

Παράδειγμα 3.2.13. Θεωρούμε το πολυώνυμο $x^4 - 1 \in \mathbb{Z}_3[x]$. Προφανώς, $x^4 - 1 = (x-1)(x+1)(x^2+1)$. Επομένως, υπάρχουν οκτώ διαιρέτες του $x^4 - 1$, οι 1, $x-1$, $x+1$, x^2+1, $(x-1)(x+1)$, $(x-1)(x^2+1)$, $(x+1)(x^2+1)$ και $x^4 - 1$. Οι γεννήτορες πίνακες των αντίστοιχων κυκλικών κωδίκων είναι κατά σειρά οι εξής:

$$I_4, \quad \begin{pmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 & -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$$

Εδώ θα πρέπει να επισημάνουμε ότι κάθε πολυωνυμικός κώδικας δεν είναι κατ' ανάγκη κυκλικός κώδικας. Πράγματι, στο παράδειγμα 3.1.6 ο δυαδικός πολυωνυμικός κώδικας μήκους 6 με πολυώνυμο γεννήτορα $1+x+x^3$ δεν είναι κυκλικός, αφού το $1\,1\,1\,0\,0\,1$ είναι (κωδικο)λέξη, ενώ το $1\,1\,1\,1\,0\,0$ δεν είναι.

Έστω $\mathcal{C}_1, \mathcal{C}_2 \in \mathcal{R}_n$ δύο κυκλικοί κώδικες. Υπενθυμίζουμε ότι το άθροισμά τους (ως άθροισμα διανυσματικών υποχώρων) ορίζεται ως εξής:

$$\mathcal{C}_1 + \mathcal{C}_2 = \{\mathbf{c}_1 + \mathbf{c}_2 \mid \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2\}.$$

Πρόταση 3.2.14. *Έστω $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{R}_n$ κυκλικοί κώδικες με πολυώνυμα γεννήτορες $\gamma_1(x)$ και $\gamma_2(x)$ αντίστοιχα, τότε έχουμε:*

1. *$\mathcal{C}_1 \subseteq \mathcal{C}_2$, αν και μόνο αν το $\gamma_2(x)$ διαιρεί το $\gamma_1(x)$.*

2. *Η τομή $\mathcal{C}_1 \cap \mathcal{C}_2$ είναι κυκλικός κώδικας με πολυώνυμο γεννήτορα το ελάχιστο κοινό πολλαπλάσιο των $\gamma_1(x)$ και $\gamma_2(x)$.*

3. *Το άθροισμα $\mathcal{C}_1 + \mathcal{C}_2$ είναι κυκλικός κώδικας με πολυώνυμο γεννήτορα τον μέγιστο κοινό διαιρέτη των $\gamma_1(x)$ και $\gamma_2(x)$.*

Απόδειξη. Ως γνωστόν, το άθροισμα και η τομή ιδεωδών είναι ιδεώδες, οπότε η απόδειξη έπεται από το θεώρημα 3.2.4, με τις λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Υποθέτουμε, ότι $x^n - 1 = \prod_{i=1}^{k} m_i(x)$ είναι η ανάλυση του $x^n - 1$ σε γινόμενο μονικών αναγώγων πολυωνύμων επί του σώματος $\mathbb{F}$. Για κάθε $i = 1, \ldots, k$ έστω $\mathcal{C}_i$ ο κυκλικός κώδικας με πολυώνυμο γεννήτορα το πολυώνυμο $m_i(x)$. Από την προηγούμενη πρόταση έχουμε ότι δεν υπάρχει κυκλικός κώδικας (εκτός από τον ίδιο τον $\mathcal{R}_n$), ο οποίος να περιέχει τον κώδικα $\mathcal{C}_i$. Με αυτή την έννοια οι κώδικες $\mathcal{C}_i$ είναι *μέγιστοι*. Προφανώς, κάθε κυκλικός κώδικας, με πολυώνυμο γεννήτορα $\gamma(x)$, περιέχεται στους αντίστοιχους μέγιστους κυκλικούς κώδικες με πολυώνυμα γεννήτορες ανάγωγους παράγοντες του $\gamma(x)$.

Δυϊκά, για κάθε $i = 1, 2, \ldots, k$, έστω $\mu_i(x) = \frac{x^n-1}{m_i(x)}$ και $\mathcal{D}_i$ ο κυκλικός κώδικας με πολυώνυμο γεννήτορα αντίστοιχα το πολυώνυμο $\mu_i(x)$. Πάλι από την προηγούμενη πρόταση έχουμε ότι δεν υπάρχει κυκλικός κώδικας (εκτός από τον μηδενικό) που να περιέχεται στους κώδικες $\mathcal{D}_i$. Με αυτή την έννοια οι κώδικες αυτοί είναι *ελάχιστοι*. Προφανώς, κάθε ελάχιστος κώδικας $\mathcal{D}_i$ περιέχεται σε όλους τους κυκλικούς κώδικες των οποίων το πολυώνυμο γεννήτορας δεν διαιρείται από το πολυώνυμο $m_i(x)$. Επ' αυτού θα επανέλθουμε αργότερα (βλέπε Πρόταση 3.2.34).

3.2.1 Το πολυώνυμο ελέγχου ενός κυκλικού κώδικα

Έστω $\mathcal{C}$ ένας $[n, k]$ κυκλικός κώδικας με πολυώνυμο γεννήτορα $\gamma(x)$. Από το Θεώρημα 3.2.6 υπάρχει (μοναδικό) μονικό πολυώνυμο $\delta(x)$, έτσι ώστε $x^n - 1 = \gamma(x) \cdot \delta(x)$. Από την Πρόταση 3.2.11 έχουμε ότι ο βαθμός του $\gamma(x)$ είναι ίσος με $n - k$, άρα ο βαθμός του $\delta(x)$ είναι ίσος με k.

Το πολυώνυμο $\delta(x)$ θα λέγεται **πολυώνυμο ελέγχου** για τον κυκλικό κώδικα $\mathcal{C}$.

Η έννοια του πολυωνύμου ελέγχου στους κυκλικούς κώδικες είναι *παράλληλη* με την έννοια του πίνακα ελέγχου ισοτιμίας, όπως θα δούμε στα επόμενα.

Θεώρημα 3.2.15. *Έστω $\mathcal{C} \subseteq \mathcal{R}_n$ ένας κυκλικός κώδικας με πολυώνυμο γεννήτορα $\gamma(x)$ και πολυώνυμο ελέγχου $\delta(x)$. Τότε μπορούμε να περιγράψουμε τα στοιχεία του $\mathcal{C}$ ως εξής: Ένα $c(x) \in \mathcal{R}_n$ ανήκει στον κώδικα $\mathcal{C}$ αν και μόνο αν $c(x) \cdot \delta(x) = 0$.*

(Υπενθυμίζουμε ότι ο πολλαπλασιασμός γίνεται $\mod (x^n - 1)$.)

Απόδειξη. Από το θεώρημα 3.2.6 έχουμε ότι $\mathcal{C} = \langle \gamma(x) \rangle$. Έστω $c(x) \in \mathcal{C}$, τότε υπάρχει $\alpha(x) \in \mathcal{R}_n$, έτσι ώστε $c(x) = \alpha(x) \cdot \gamma(x)$ και άρα:

$$c(x) \cdot \delta(x) = \alpha(x) \cdot \gamma(x) \cdot \delta(x) = 0(\mod (x^n - 1).$$

Αντίστροφα, υποθέτουμε ότι $c(x) \cdot \delta(x) = 0(\mod (x^n - 1)$. Από την ταυτότητα της διαίρεσης στο $\mathbb{F}[x]$ έχουμε ότι υπάρχουν πολυώνυμα $\pi(x), \upsilon(x) \in \mathbb{F}[x]$, τέτοια ώστε:

$$c(x) = \pi(x) \cdot \gamma(x) + \upsilon(x) \text{ με } \upsilon(x) = 0 \text{ ή } deg(\upsilon(x)) < deg(\gamma(x)) = n - k.$$

Αν υποθέσουμε ότι το $\upsilon(x)$ δεν είναι το μηδενικό πολυώνυμο, από τη σχέση $c(x) \cdot \delta(x) = 0(\mod (x^n - 1)$ έπεται ότι:

$$\upsilon(x) \cdot \delta(x) = 0(\mod (x^n - 1).$$

Αυτό σημαίνει ότι το πολυώνυμο $x^n - 1$ διαιρεί το $\upsilon(x) \cdot \delta(x)$ στο $\mathbb{F}[x]$. Αλλά ο βαθμός του γινομένου $\upsilon(x) \cdot \delta(x)$ είναι μικρότερος του $(n-k)+k = n$, άτοπο, άρα $\upsilon(x) = 0$ και επομένως $c(x) = \pi(x) \cdot \gamma(x) \in \mathcal{C}$. ό.έ.δ.

Η ισότητα $c(x) \cdot \delta(x) = 0(\mod (x^n - 1)$ επάγει κατά έναν φυσιολογικό τρόπο μια σχέση *ορθογωνιότητας* στο $\mathcal{R}_n$, η οποία οδηγεί στον υπολογισμό ενός πίνακα ελέγχου ισοτιμίας για έναν κυκλικό κώδικα, καθώς και στην περιγραφή του δυϊκού του κώδικα.

Θεώρημα 3.2.16. *Έστω $\mathcal{C}$ ένας $[n, k]$ κυκλικός κώδικας με πολυώνυμο γεννήτορα $\gamma(x)$ και πολυώνυμο ελέγχου $\delta(x) = h_0 + h_1 x + \cdots + h_k x^k$. Τότε ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$ είναι ο ο $(n-k) \times n$ πίνακας:*

$$\mathrm{H} = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}.$$

Επιπλέον, ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι και αυτός κυκλικός και παράγεται από το πολυώνυμο:

$$d(x) = h_k + h_{k-1} x + \cdots + h_0 x^k.$$

Απόδειξη. Από το προηγούμενο θεώρημα έχουμε ότι το πολυώνυμο $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ ανήκει στον κώδικα $\mathcal{C}$, αν και μόνο αν $c(x) \cdot \delta(x) = 0$. Εδώ ο πολλαπλασιασμός είναι $(\mod (x^n - 1)$. Αυτό σημαίνει ότι το πολυώνυμο $x^n - 1$ πρέπει να διαιρεί το γινόμενο $c(x) \cdot \delta(x)$. Κάνοντας τον πολλαπλασιασμό $c(x) \cdot \delta(x)$ και απαιτώντας το υπόλοιπο της διαίρεσης με το $x^n - 1$ να είναι ίσον με 0 έχουμε ότι οι συντελεστές των $x^k, x^{k+1}, \ldots, x^{n-1}$ πρέπει να είναι 0. Δηλαδή έχουμε ότι:

$$\begin{array}{ccccccccc} c_0 h_k & + & c_1 h_{k-1} & + & \cdots & + & c_k h_0 & = & 0 \\ c_1 h_k & + & c_2 h_{k-1} & + & \cdots & + & c_{k+1} h_0 & = & 0 \\ \vdots & & \vdots & & \vdots & & \vdots & \vdots & \vdots \\ c_{n-k-1} h_k & + & c_{n-k} h_{k-1} & + & \cdots & + & c_{n-1} h_0 & = & 0 \end{array}.$$

Από τις τελευταίες σχέσεις βλέπουμε ότι η (κωδικο)λέξη $c_0\, c_1 \cdots c_{n-1}$ είναι ορθογώνια ως προς τη λέξη $h_k\, h_{k-1} \cdots h_0\, 0 \cdots 0$ και τις λέξεις που προέρχονται από κυκλικές μεταθέσεις των χαρακτήρων της. Δηλαδή οι γραμμές του πίνακα H είναι στοιχεία του δυϊκού κώδικα $\mathcal{C}^\perp$. Έχουμε επισημάνει ότι το πολυώνυμο ελέγχου $\delta(x) = h_0 + h_1 x + \cdots + h_k x^k$ είναι μονικό, δηλαδή $h_k = 1$. Αυτό σημαίνει ότι οι $n - k$ το πλήθος γραμμές του πίνακα H είναι γραμμικά ανεξάρτητες, άρα ο πίνακας H είναι γεννήτορας πίνακας του $\mathcal{C}^\perp$, δηλαδή πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{C}$.

Παρατηρούμε ότι $d(x) = h_k + h_{k-1}x + \cdots + h_0x^k = x^k \cdot \delta(x^{-1})$. Επομένως, από τη σχέση $(x^{-1})^n - 1 = \gamma(x^{-1}) \cdot \delta(x^{-1})$ έχουμε $((x^{-1})^n - 1) \cdot x^k = \gamma(x^{-1}) \cdot x^k \cdot \delta(x^{-1}) = \gamma(x^{-1}) \cdot d(x)$, δηλαδή $((x^{-1})^n - 1) \cdot x^k \cdot x^{n-k} = x^{n-k} \cdot \gamma(x^{-1}) \cdot d(x)$. Από την τελευταία σχέση έπεται ότι $x^n - 1 = (-x^{n-k} \cdot \gamma(x^{-1})) \cdot d(x)$. Επειδή το πολυώνυμο γεννήτορας $\gamma(x)$ είναι βαθμού $n-k$, η έκφραση $-x^{n-k} \cdot \gamma(x^{-1})$ είναι ένα πολυώνυμο με συντελεστές από το σώμα $\mathbb{F}$. Άρα, το πολυώνυμο $d(x)$ διαιρεί το $x^n - 1$. Επομένως, από την Πρόταση 3.2.11 έχουμε ότι το ιδεώδες $\langle d(x) \rangle$ είναι ένας κυκλικός κώδικας με γεννήτορα πίνακα τον πίνακα H, δηλαδή ο δυϊκός κώδικας $\mathcal{C}^\perp$ είναι κυκλικός. ό.έ.δ.

Παρατηρήσεις 3.2.17.

1. Το πολυώνυμο $d(x) = h_k + h_{k-1}x + \cdots + h_0x^k$ παράγει μεν τον δυϊκό κώδικα $\mathcal{C}^\perp$, αλλά δεν είναι το πολυώνυμο γεννήτορας, διότι δεν είναι μονικό. Το πολυώνυμο γεννήτορας είναι το $h_0^{-1} \cdot d(x)$.

2. Όπως βλέπουμε το πολυώνυμο ελέγχου $\delta(x) = h_0 + h_1x + \cdots + h_kx^k$ του κυκλικού κώδικα $\mathcal{C}$ δεν παράγει τον δυϊκό κώδικα $\mathcal{C}^\perp$, αλλά τον παράγει το *αμοιβαίο* πολυώνυμο $d(x) = h_k + h_{k-1}x + \cdots + h_0x^k$, του οποίου οι συντελεστές είναι οι συντελεστές του $\delta(x)$ με την αντίστροφη σειρά.

3. Γενικά το αμοιβαίο πολυώνυμο $\overline{\phi(x)}$ ενός πολυωνύμου:

$$\phi(x) = a_k + a_{k-1}x + \cdots + a_0x^k$$

είναι το πολυώνυμο $x^k\phi(x^{-1})$. Επομένως, στη συγκεκριμένη περίπτωση το πολυώνυμο $\delta(x^{-1}) = x^{n-k}d(x)$ ανήκει στον κώδικα $\mathcal{C}^\perp$.

Είναι εύκολο να δούμε ότι το αμοιβαίο πολυώνυμο ενός γινομένου πολυωνύμων ισούται με το γινόμενο των αντιστοίχων αμοιβαίων πολυωνύμων των παραγόντων (αποδείξτε το!).

4. Από την απόδειξη του προηγουμένου θεωρήματος μπορούμε εύκολα να συνάγουμε το ακόλουθο αποτέλεσμα. Ένας $[n, k, d]$ κυκλικός κώδικας με πολυώνυμο γενήτορα $\gamma(x)$ είναι αυτοδυϊκός, αν και μόνο αν $\gamma(x) = -\frac{x^n-1}{x^{n-k} \cdot \gamma(x^{-1})}$ (γιατί;)

5. Επισημαίνουμε ότι στο Παράδειγμα 3.1.12 είχαμε δει ότι ο δυϊκός ενός πολυωνυμικού κώδικα δεν είναι κατ' ανάγκη, πολυωνυμικός, ενώ ο δυϊκός ενός κυκλικού κώδικα είναι κυκλικός.

6. Στα προηγούμενα (όπως και στα επόμενα), όπου εμφανίζεται το σύμβολο x^{-1} οι πράξεις γίνονται στο σώμα $\mathbb{F}(x)$ των ρητών εκφράσεων, αλλά το αποτέλεσμα είναι πολυώνυμο που ανήκει στον δακτύλιο $\mathbb{F}[x]$.

Παράδειγμα 3.2.18. Όπως στο Παράδειγμα 3.2.13, θεωρούμε το πολυώνυμο $x^4-1=(x-1)(x+1)(x^2+1)\in\mathbb{Z}_3[x]$. Προφανώς ο κυκλικός κώδικας $\mathcal{C}$ με πολυώνυμο γεννήτορα x^2+1 έχει ως γεννήτορα πίνακα τον πίνακα:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

ως πολυώνυμο ελέγχου το πολυώνυμο $(x-1)(x+1)=x^2-1$ και, επομένως, ως πίνακα ελέγχου ισοτιμίας τον πίνακα:

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Ένας κυκλικός κώδικας $\mathcal{C}$ μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$ είναι διανυσματικός υπόχωρος του $\mathcal{R}_n$, επομένως υπάρχει ένας συμπληρωματικός υπόχωρος M, έτσι ώστε $\mathcal{C}\oplus M=\mathcal{R}_n$. Το συμπλήρωμα M αφενός μεν δεν είναι μοναδικό, αφετέρου δεν είναι κατ' ανάγκη κυκλικός κώδικας (γιατί;). Το ερώτημα που προκύπτει είναι:
Υπάρχει κυκλικός κώδικας $\overline{\mathcal{C}}$, έτσι ώστε $\mathcal{C}\oplus\overline{\mathcal{C}}=\mathcal{R}_n$;

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα και $x^n-1\in\mathbb{F}[x]$. Τότε για κάθε ανάλυση $x^n-1=\gamma(x)\delta(x)$ σε γινόμενο δύο παραγόντων ορίζονται δύο κυκλικοί κώδικες μήκους n $\mathcal{C}$ και $\overline{\mathcal{C}}$ με πολυώνυμα γεννήτορες $\gamma(x)$ και $\delta(x)$ αντίστοιχα.

Πρόταση 3.2.19. *Με τις προηγούμενες υποθέσεις, ο $\mathcal{R}_n$ ως διανυσματικός χώρος είναι το ευθύ άθροισμα των $\mathcal{C}$ και $\overline{\mathcal{C}}$.*

Απόδειξη. Η απόδειξη είναι άμεση από τον τρόπο ορισμού του κώδικα $\overline{\mathcal{C}}$. ό.έ.δ.

Παρατήρηση 3.2.20. Ο κυκλικός κώδικας $\overline{\mathcal{C}}$, ο οποίος ορίσθηκε προηγουμένως, ονομάζεται το **κυκλικό συμπλήρωμα** του κώδικα $\mathcal{C}$, έχει ως πολυώνυμο γεννήτορα το πολυώνυμο ελέγχου του κώδικα $\mathcal{C}$ και **δεν** είναι ο δυϊκός κώδικας $\mathcal{C}^{\perp}$.

Έχουμε παρατηρήσει (Παράδειγμα $3.2.2_6$) ότι ο κώδικας $\mathcal{E}_n$ που αποτελείται από όλες τις λέξεις μήκους n με άθροισμα χαρακτήρων ίσον με μηδέν είναι ένας κυκλικός κώδικας. Αυτό δεν σημαίνει ότι κάθε γραμμικός κώδικας μηδενικού αθροίσματος είναι κυκλικός.

Για παράδειγμα, ο δυαδικός κώδικας $\{\,0000,\ 1100,\ 0011,\ 1111\,\}$ είναι γραμμικός και μηδενικού αθροίσματος, αλλά δεν είναι κυκλικός.

Στο επόμενο θεώρημα δίνουμε έναν χαρακτηρισμό των κυκλικών κωδίκων μηδενικού αθροίσματος.

Θεώρημα 3.2.21. *Έστω $\mathcal{E}_n$ ο κυκλικός κώδικας επί του αλφαβήτου $\mathbb{F}$, του οποίου τα στοιχεία είναι όλες οι λέξεις μήκους n με μηδενικό άθροισμα χαρακτήρων. Το πολυώνυμο γεννήτορας του $\mathcal{E}_n$ είναι το $x-1$ και κάθε κυκλικός κώδικας $\mathcal{C}$ μήκους n με πολυώνυμο γεννήτορα $\gamma(x)$ είναι κώδικας μηδενικού αθροίσματος, αν και μόνο αν το $x-1$ διαιρεί το $\gamma(x)$.*

Απόδειξη. Έστω $\mathcal{D}$ ο κυκλικός κώδικας του οποίου το πολυώνυμο γεννήτορας είναι το πολυώνυμο $x-1$. Ο $\mathcal{D}$ είναι διάστασης $n-1$ (Πρόταση 3.2.11) και μηδενικού αθροίσματος, διότι κάθε στοιχείο του είναι της μορφής:

$$-a_1\,(a_1-a_2)\,(a_2-a_3)\cdots(a_{(n-2)}-a_{n-1})\,a_{n-1}. \qquad \text{(γιατί;)}$$

Επομένως $\mathcal{D}\subseteq\mathcal{E}_n$. Ο κώδικας $\mathcal{E}_n$ δεν είναι διάστασης n, αφού υπάρχουν λέξεις με άθροισμα χαρακτήρων που δεν είναι ίσο με μηδέν. Άρα, από τη σχέση $\mathcal{D}\subseteq\mathcal{E}_n$ έχουμε ότι $\mathcal{D}=\mathcal{E}_n$.

Τα υπόλοιπα έπονται από την Πρόταση 3.2.14. ό.έ.δ.

Παράδειγμα 3.2.22. Στο Παράδειγμα 3.2.18 ο κυκλικός κώδικας $\mathcal{C}$ με πολυώνυμο γεννήτορα x^2+1 περιέχει λέξεις μη μηδενικού αθροίσματος. Το πολυώνυμο ελέγχου είναι το $(x-1)(x+1)=x^2-1$ και, επομένως, ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ είναι κώδικας μηδενικού αθροίσματος.

3.2.2 Κυκλικοί κώδικες και ρίζες της μονάδας

Όπως είχαμε επισημάνει στη σελίδα 180 το πρόβλημα του προσδιορισμού όλων των κυκλικών κωδίκων μήκους n είναι ισοδύναμο με τον προσδιορισμό της ανάλυσης του πολυωνύμου x^n-1 σε γινόμενο (αναγώγων) πολυωνύμων. Το πρόβλημα αυτό είναι πολύ δύσκολο στη γενικότητά του. Έχουν επινοηθεί διάφορες μέθοδοι 'παραγοντοποίησης' του πολυωνύμου x^n-1. Εδώ δεν θα ασχοληθούμε με την παραγοντοποίηση αυτή. Θα τη θεωρήσουμε δεδομένη και θα δώσουμε μια διαφορετική παρουσίαση των κυκλικών κωδίκων χρησιμοποιώντας τις $n-$οστές ρίζες της μονάδας.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $x^n-1 \in \mathbb{F}[x]$. Υποθέτουμε ότι $x^n-1 = \prod_{i=1}^{k} m_i(x)$ είναι η ανάλυση του σε γινόμενο μονικών αναγώγων πολυωνύμων επί του $\mathbb{F}$. Υποθέτουμε ότι ω είναι μια ρίζα του πολυωνύμου x^n-1. Η ω βρίσκεται σε μια επέκταση του σώματος $\mathbb{F}$ και μηδενίζει έναν (μόνο) από τους παράγοντες $m_i(x)$. Επομένως, για ένα πολυώνυμο $f(x) \in \mathbb{F}[x]$ έχουμε $f(\omega)=0$, αν και μόνο αν υπάρχει $\pi(x) \in \mathbb{F}[x]$ έτσι ώστε $f(x) = \pi(x) \cdot m_i(x)$. Μεταβαίνοντας στον δακτύλιο πηλίκο $\mathcal{R}_n = \mathbb{F}[x]/\langle x^n-1\rangle$ βλέπουμε ότι το ω είναι ρίζα του πολυωνύμου $f(x)$, αν και μόνο αν το $f(x)$ ανήκει στον κυκλικό κώδικα $\langle m_i(x)\rangle$.

Από την προηγούμενη συζήτηση μπορούμε να συνάγουμε το επόμενο θεώρημα.

Θεώρημα 3.2.23. *Έστω $g(x) = r_1(x)\cdot r_2(x)\cdots r_s(x)$ ένα γινόμενο (μονικών) αναγώγων παραγόντων του x^n-1. Υποθέτουμε ότι $\{\rho_1, \rho_2, \ldots, \rho_\nu\}$ είναι οι ρίζες του $g(x)$. Τότε ο κυκλικός κώδικας ο παραγόμενος από το $g(x)$ είναι ίσος με:*

$$\mathcal{C} = \langle g(x)\rangle = \{\, f(x) \in \mathcal{R}_n \mid f(\rho_1)=0, f(\rho_2)=0, \ldots, f(\rho_\nu)=0\,\}.$$

Επιπλέον, είναι αρκετό να επιλέξουμε μόνο μία ρίζα ξ_i από κάθε ανάγωγο παράγοντα $r_i(x)$, $i=1,\ldots,s$ και να ισχύει:

$$\mathcal{C} = \langle g(x)\rangle = \{\, f(x) \in \mathcal{R}_n \mid f(\xi_1)=0, f(\xi_2)=0, \ldots, f(\xi_s)=0\,\}.$$

Απόδειξη. Οι ρίζες $\{\rho_1, \rho_2, \ldots, \rho_\nu\}$ του πολυωνύμου $g(x)$ ανήκουν στο σώμα ριζών $\mathbb{E}$ του πολυωνύμου x^n-1, επομένως αν ένα πολυώνυμο $f(x) \in \mathcal{R}_n$

ανήκει στον κυκλικό κώδικα $\mathcal{C} = \langle g(x) \rangle$, προφανώς μηδενίζεται από τα $\rho_1, \rho_2, \dots, \rho_\nu$, άρα:

$$\mathcal{C} = \langle g(x) \rangle \subseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \dots, f(\rho_\nu) = 0 \}.$$

Αντίστροφα, ένα πολυώνυμο $f(x) \in \mathcal{R}_n$, που μηδενίζεται από τα $\rho_1, \rho_2, \dots, \rho_\nu$, στο σώμα $\mathbb{E}$ θα έχει την ανάλυση $f(x) = g(x) \cdot \pi(x)$ με $\pi(x) \in \mathbb{F}[x]$ [γιατί το $\pi(x) \in \mathbb{F}[x]$ και όχι γενικά $\pi(x) \in \mathbb{E}[x]$;]. Άρα:

$$\mathcal{C} = \langle g(x) \rangle \supseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \dots, f(\rho_\nu) = 0 \}.$$

Από κάθε ανάγωγο παράγοντα $r_i(x)$, $i = 1, \dots, s$ επιλέγουμε μια ρίζα ξ_i. Αν ο βαθμός του $r_i(x)$ είναι d_i, τότε οι άλλες ρίζες του $r_i(x)$ είναι οι $\xi_i^q, \xi_i^{q^2}, \dots, \xi_i^{q^{d_i-1}}$. Όπου q είναι το πλήθος των στοιχείων του σώματος $\mathbb{F}$.

Πράγματι (ιδέ και Θεώρημα Α΄.3.18), από τη σχέση $(r_i(\xi_i))^q = r_i(\xi_i^q)$ έχουμε ότι οι $\xi_i, \xi_i^q, \xi_i^{q^2}, \dots, \xi_i^{q^{d_i-1}}$ είναι οι ρίζες του $r_i(x)$, αφού είναι διακεκριμένες. Επομένως έχουμε ότι $\{ f(x) \in \mathcal{R}_n \mid f(\xi_1) = 0, f(\xi_2) = 0, \dots, f(\xi_s) = 0 \} \subseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \dots, f(\rho_\nu) = 0 \}$. Αλλά, προφανώς, ισχύει $\{ f(x) \in \mathcal{R}_n \mid f(\xi_1) = 0, f(\xi_2) = 0, \dots, f(\xi_s) = 0 \} \supseteq \{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \dots, f(\rho_\nu) = 0 \}$. Οπότε έπεται το αποτέλεσμα. ό.έ.δ.

Παρατηρήσεις 3.2.24. 1. Οι ρίζες $\xi_i, \xi_i^q, \xi_i^{q^2}, \dots, \xi_i^{q^{d_i-1}}$ του πολυωνύμου $r_i(x)$ είναι πράγματι διακεκριμένες, διότι αν υποθέσουμε ότι $\xi_i^{q^\kappa} = \xi_i^{q^\lambda}$ με $0 \leq \kappa < \lambda \leq d_i - 1$, τότε $\xi_i^{q^\kappa} = \xi_i^{q^\lambda} = (\xi_i^{q^\kappa})^{q^{\lambda-\kappa}}$, δηλαδή $(\xi_i^{q^\kappa})^{q^{\lambda-\kappa}} - \xi_i^{q^\kappa} = 0$. Από την τελευταία σχέση έχουμε ότι το $\xi_i^{q^\kappa}$ είναι ρίζα του πολυωνύμου $x^{q^{\lambda-\kappa}} - x$. Άρα, το $\xi_i^{q^\kappa}$ είναι κοινή ρίζα του ανάγωγου πολυωνύμου $r_i(x)$ και του πολυωνύμου $x^{q^{\lambda-\kappa}} - x$. Δηλαδή το $r_i(x)$ διαιρεί το $x^{q^{\lambda-\kappa}} - x$. Από γνωστό Θεώρημα[3] έχουμε ότι ο βαθμός d_i του $r_i(x)$ πρέπει να διαιρεί τη διαφορά $\lambda - \kappa$, άτοπο. Επομένως, οι ρίζες $\xi_i, \xi_i^q, \xi_i^{q^2}, \dots, \xi_i^{q^{d_i-1}}$ είναι διακεκριμένες (βλέπε και το Θεώρημα Α΄.3.18).

[3] Το Θεώρημα που επικαλούμαστε είναι το εξής:
(Πόρισμα Α΄.3.17) Έστω $\mathbb{F}$ πεπερασμένο σώμα με q το πλήθος στοιχεία και $r(x) \in \mathbb{F}[x]$ ανάγωγο πολυώνυμο. Τότε το $r(x)$ διαιρεί το πολυώνυμο $x^{q^n} - x$, αν και μόνο αν ο βαθμός του $r(x)$ διαιρεί το n.

2. Θα μπορούσαμε να αναδιατυπώσουμε το προηγούμενο θεώρημα ως εξής:

   Έστω $\{\rho_1, \rho_2, \dots, \rho_\nu\}$ κάποιες ρίζες του πολυωνύμου $x^n - 1$, τότε το σύνολο $\{f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \dots, f(\rho_\nu) = 0\}$ είναι ένας κυκλικός κώδικας με πολυώνυμο γεννήτορα το ελάχιστο κοινό πολλαπλάσιο των ελαχίστων πολυωνύμων των ριζών $\rho_1, \rho_2, \dots, \rho_\nu$.

   Η απόδειξη είναι εύκολη και αφίεται ως άσκηση. [Μπορούμε να παραβάλουμε το αποτέλεσμα αυτό με την Πρόταση 3.2.14(2)].

Στην παράγραφο 2.3.2 είχαμε δει ότι, αν έχουμε ένα πεπερασμένο σώμα $\mathbb{K}$ και ένα υπόσωμά του $\mathbb{F}$, τότε από έναν κώδικα $\mathcal{C}$ επί του $\mathbb{K}$ μπορούμε να κατασκευάσουμε έναν (υπο)κώδικα επί του υποσώματος $\mathbb{F}$. Εδώ θα δούμε πώς ένας (ήδη δεδομένος) κυκλικός κώδικας επί ενός σώματος $\mathbb{F}$ θα μπορούσε να θεωρηθεί ως υποκώδικας ενός άλλου κώδικα ορισμένου επί ενός υπερσώματος του $\mathbb{F}$.

Η θεώρηση αυτή των κυκλικών κωδίκων μας επιτρέπει να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας ενός κυκλικού κώδικα με διαφορετικό τρόπο από αυτόν που αναφέρεται στο Θεώρημα 3.2.16.

Έστω $\{\rho_1, \rho_2, \dots, \rho_\nu\}$ ένα σύνολο ριζών του πολυωνύμου $x^n - 1$. Ένα πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R}_n = \mathbb{F}[x]/\langle x^n - 1\rangle$ έχει ρίζα το ρ_i, αν και μόνο αν $a_0 + a_1\rho_i + \cdots + a_{n-1}\rho_i^{n-1} = 0$.

Οι ρίζες ρ_i βρίσκονται σε μια επέκταση, έστω $\mathbb{E}$, του σώματος $\mathbb{F}$. Επομένως, το πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R}_n$ έχει ρίζες τα ρ_i, $i = 1, \dots, \nu$, αν και μόνο αν οι συντελεστές του ικανοποιούν τη σχέση:

$$\mathbf{a} \cdot \mathrm{H}^t = \mathbf{0},$$

όπου:

$$\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \quad \text{και} \quad \mathrm{H} = \begin{pmatrix} 1 & \rho_1^1 & \cdots & \rho_1^{n-1} \\ 1 & \rho_2^1 & \cdots & \rho_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \rho_\nu^1 & \cdots & \rho_\nu^{n-1} \end{pmatrix}.$$

Τα στοιχεία του πίνακα H είναι στοιχεία του σώματος $\mathbb{E}$. Όμως το σώμα $\mathbb{E}$ μπορεί να θεωρηθεί ως διανυσματικός χώρος επί του $\mathbb{F}$ με διάσταση έστω r. Επιλέγουμε και σταθεροποιούμε μια βάση του $\mathbb{E}$ ως προς $\mathbb{F}$. Για κάθε $i = 1, \dots, \nu$ και κάθε $j = 0, \dots, n-1$ θα συμβολίζουμε με $[r_i^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση του ρ_i^j ως γραμμικού συνδυασμού των στοιχείων αυτής της βάσης με συντελεστές από το σώμα $\mathbb{F}$.

Η σχέση $a_0 + a_1\rho_i + \cdots + a_{n-1}\rho_i^{n-1} = 0$ ισχύει, αν και μόνο αν $a_0 + a_1[r_i^1] + \cdots + a_{n-1}[r_i^{n-1}] = \mathbf{0}$, όπου το $\mathbf{0}$ παριστά το μηδενικό διάνυσμα στήλη.

Η τελευταία σχέση θα μπορούσε να εκφραστεί με τη βοήθεια πινάκων ως εξής:

Κατασκευάζουμε τον πίνακα:

$$\mathrm{P} = \begin{pmatrix} [r_1^0] & [r_1^1] & \cdots & [r_1^{n-1}] \\ [r_2^0] & [r_2^1] & \cdots & [r_2^{n-1}] \\ \vdots & \vdots & \vdots & \vdots \\ [r_\nu^0] & [r_\nu^1] & \cdots & [r_\nu^{n-1}] \end{pmatrix}.$$

Οπότε έχουμε: $\mathbf{a} \cdot \mathrm{P}^{\perp} = \mathbf{0}$. Ο πίνακας P είναι ένας $\nu \times n$ πίνακας, του οποίου τα στοιχεία (προς το παρόν) είναι διανύσματα στήλες.

Αν αναπτύξουμε την κάθε στήλη $[r_i^j]$, η οποία έχει μήκος ίσον με r, από τον πίνακα P, προκύπτει ένας $\nu r \times n$ πίνακας $\overline{\mathrm{H}}$ με στοιχεία από το (υπό)σωμα $\mathbb{F}$. Οπότε από τα προηγούμενα έχουμε ότι είναι ο πίνακας ελέγχου ισοτιμίας για τον κυκλικό κώδικα $\{ f(x) \in \mathcal{R}_n \mid f(\rho_1) = 0, f(\rho_2) = 0, \dots, f(\rho_\nu) = 0 \}$.

Παρατήρηση 3.2.25. Οι γραμμές του πίνακα που κατασκευάσαμε με τον παραπάνω τρόπο δεν είναι κατ' ανάγκη γραμμικά ανεξάρτητες, οπότε αν θέλουμε να έχουμε έναν γεννήτορα πίνακα του δυϊκού κώδικα πρέπει να διαγράψουμε μερικές από αυτές και να κρατήσουμε το μεγαλύτερο δυνατόν πλήθος γραμμικά ανεξαρτήτων γραμμών.

Παράδειγμα 3.2.26. Έστω $\mathcal{C}$ ο κυκλικός κώδικας μήκους 7 επί του $\mathbb{Z}_2$ με πολυώνυμο γεννήτορα $\gamma(x) = x^3 + x + 1$. Αν ρ είναι μία ρίζα του $\gamma(x)$, τότε οι άλλες δύο ρίζες του $\gamma(x)$ είναι οι ρ^2 και ρ^4 (γιατί;). Σύμφωνα με το προηγούμενο θεώρημα ένα στοιχείο του κώδικα θα είναι ένα πολυώνυμο $f(x) \in \mathcal{R}_7$ με την ιδιότητα $f(\rho) = f(\rho^2) = f(\rho^4) = 0$.

Έστω $\mathbb{E} = \mathbb{Z}_2(\rho)$. Το σώμα $\mathbb{E}$ έχει βαθμό επέκτασης επί του $\mathbb{Z}_2$ ίσον με 3 και μια βάση του $\mathbb{E}$ επί του $\mathbb{Z}_2$ είναι το σύνολο $\{1, \rho, \rho^2\}$.

Επομένως, ένα πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_6x^6 \in \mathcal{R}_7$ έχει ρίζα το ρ, αν και μόνο αν $a_0 + a_1\rho + \cdots + a_6\rho^6 = 0$.

Δηλαδή το πολυώνυμο $f(x) = a_0 + a_1x + \cdots + a_6x^6 \in \mathcal{R}_7$, αν και μόνο αν οι συντελεστές του ικανοποιούν τη σχέση: $\mathbf{a} \cdot \mathrm{H}^t = \mathbf{0}$, όπου:

$$\mathbf{a} = (a_0, a_1, \ldots, a_6) \quad \text{και} \quad \mathrm{H} = \begin{pmatrix} 1 & \rho^1 & \cdots & \rho^6 \end{pmatrix}.$$

Εκφράζουμε κάθε στοιχείο του πίνακα H ως γραμμικό συνδυασμό των στοιχείων της βάσης $\{1, \rho, \rho^2\}$ με συντελεστές από το $\mathbb{Z}_2$ (κάντε το!), οπότε σύμφωνα με τα προηγούμενα προκύπτει ο πίνακας:

$$\overline{\mathrm{H}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

ο οποίος είναι ένας πίνακας ελέγχου ισοτιμίας για τον κυκλικό κώδικα $\mathcal{C}$ μήκους 7 επί του $\mathbb{Z}_2$ με πολυώνυμο γεννήτορα $\gamma(x) = x^3 + x + 1$.

Παρατηρήσεις 3.2.27. 1. Το πολυώυμο $\gamma(x) = x^3 + x + 1$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο σώμα $\mathbb{E}$ ως $\gamma(x) = x^3+x+1 = (x-\rho)(x-\rho^2)(x-\rho^4)$. Ο πίνακας $\mathrm{H} = \begin{pmatrix} 1 & \rho^1 & \cdots & \rho^6 \end{pmatrix}$ με στοιχεία από το $\mathbb{E}$ είναι ο πίνακας ελέγχου ισοτιμίας ενός κυκλικού κώδικα $\mathcal{D}$ επί του $\mathbb{E}$ με πολυώνυμο γεννήτορα το $\delta(x) = x-\rho$, το οποίο διαιρεί το $\gamma(x) = x^3 + x + 1 = (x-\rho)(x-\rho^2)(x-\rho^4)$. Συνεπώς $\mathcal{C} \subseteq \mathcal{D}$. Μάλιστα δε ισχύει $\mathcal{C} = \mathcal{D}_{\mathbb{Z}_2}$.

2. Επειδή ένα πολυώνυμο:

$$f(x) = a_0 + a_1x + \cdots + a_6x^6 \in \mathcal{R}_6 = \mathbb{Z}_2[x]/\langle x^7 - 1\rangle$$

με ρίζα το ρ έχει ρίζα και το ρ^2, αν αντί του πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & \rho^1 & \cdots & \rho^6 \end{pmatrix}$$

πάρουμε τον πίνακα:

$$\mathrm{T} = \begin{pmatrix} 1 & \rho^1 & \cdots & \rho^6 \\ 1 & \rho^2 & \cdots & \rho^{12} \end{pmatrix}$$

με στοιχεία από το $\mathbb{E}$, ο πίνακας T είναι ο πίνακας ελέγχου ισοτιμίας ένος κυκλικού κώδικα $\mathcal{E}$ επί του $\mathbb{E}$ με πολυώνυμο γεννήτορα το $\eta(x) = (x-\rho)(x-\rho^2)$, το οποίο διαιρεί το $\gamma(x) = x^3+x+1 = (x-\rho)(x-\rho^2)(x-\rho^4)$. Συνεπώς $\mathcal{C} \subseteq \mathcal{E}$. Μάλιστα δε ισχύει $\mathcal{C} = \mathcal{E}_{\mathbb{Z}_2}$. Δηλαδή έχουμε δύο κώδικες επί του $\mathbb{E}$, των οποίων η τομή με το $\mathbb{Z}_2^7$ ισούται με τον κώδικα $\mathcal{C}$.

Όπως είδαμε από το παράδειγμα και τις παρατηρήσεις, για τον κυκλικό κώδικα $\mathcal{C}$ ισχύει $\mathcal{C} = \mathcal{D}_{\mathbb{Z}_2}$, όπου και ο κώδικας $\mathcal{D}$ είναι κυκλικός.

Ισχύει και το αντίστροφο.

Πρόταση 3.2.28. *Έστω $\mathbb{K}$ ένα σώμα και $\mathbb{F}$ ένα υπόσωμά του. Αν $\mathcal{D}$ είναι ένας κυκλικός κώδικας επί του $\mathbb{K}$, τότε ο κώδικας $\mathcal{C} = \mathcal{D}_{\mathbb{F}}$ είναι κυκλικός.*

Απόδειξη. Θεωρούμε το πολυώνυμο $x^n - 1$, όπου n είναι το μήκος του κώδικα, μια φορά με συντελεστές από το $\mathbb{K}$ και μια φορά με συντελεστές από το $\mathbb{F}$. Έστω $x^n-1 = \mu_1(x)\mu_2(x)\cdots\mu_k(x)$ η ανάλυσή του σε ανάγωγους παράγοντες επί του $\mathbb{K}$ και $x^n - 1 = m_1(x)m_2(x)\cdots m_r(x)$ η ανάλυσή του σε ανάγωγους παράγοντες επί του $\mathbb{F}$. Αν $\delta(x) \in \mathbb{K}[x]$ είναι το πολυώνυμο γεννήτορας του κώδικα $\mathcal{D}$, τότε (αναδιατάσοντας εν ανάγκη τους δείκτες) μπορούμε να υποθέσουμε ότι $\delta(x) = \mu_1(x)\mu_2(x)\cdots\mu_\nu(x)$, ($\nu \leq k$). Όμως κάθε ανάγωγος παράγοντας $\mu_i(x)$ διαιρεί έναν (μόνο) παράγοντα από τους $m_j(x)$ (η διαίρεση γίνεται στο σώμα $\mathbb{K}$). Έστω $\gamma(x) = m_{j_1}(x)m_{j_2}(x)\cdots m_{j_\tau}(x) \in \mathbb{F}[x]$, όπου $m_{j_\ell}(x)$, $\ell = 1, \ldots, \tau$ είναι μόνο οι ανάγωγοι παράγοντες στο $\mathbb{F}[x]$, οι οποίοι διαιρούνται από (τουλάχιστον) ένα $\mu_i(x)$, $i = 1, 2, \ldots, \nu$.

Είναι εύκολο να δούμε ότι ο κυκλικός κώδικας $\mathcal{C} = \langle \gamma(x) \rangle$ ισούται με $\mathcal{D}_{\mathbb{F}} = \mathcal{D} \cap \mathbb{F}^n$. ό.έ.δ.

3.2.3 Ο αδύναμος γεννήτορας ενός κυκλικού κώδικα

Όπως έχουμε ήδη επισημάνει, ο προσδιορισμός όλων των κυκλικών κωδίκων μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$ ανάγεται στο πρόβλημα της παραγοντοποίησης του πολυωνύμου x^n-1. Παρότι έχουν αναπτυχθεί μέθοδοι προσδιορισμού των n-στών ριζών της μονάδας, το όλο εγχείρημα δεν είναι εύκολο.

Θα δούμε μια διαφορετική προσέγγιση περιγραφής/προσδιορισμού ενός κυκλικού κώδικα.

Υπενθυμίζουμε ότι σε έναν δακτύλιο R ένα στοιχείο $e \in R$ ονομάζεται αδύναμο αν $e^2 = e$.

Έχουμε δει προηγουμένως ότι ένας κυκλικός κώδικας, εκτός από το πολυώνυμο γεννήτορα, ενδέχεται να παράγεται και από άλλο πολυώνυμο.

Θα δούμε τώρα ότι για κάθε κυκλικό κώδικα $\mathcal{C}$ μήκους n υπάρχει μοναδικό πολυώνυμο $\epsilon(x) \in \mathcal{R}_n$ με τις ιδιότητες:

$\alpha)$ Το $\epsilon(x)$ παράγει τον κώδικα $\mathcal{C}$.

$\beta)$ Το $\epsilon(x)$ είναι μοναδιαίο στοιχείο του κώδικα $\mathcal{C}$, δηλαδή $\epsilon(x) \cdot c(x) = c(x)$ για κάθε $c(x) \in \mathcal{C}$.

$\gamma)$ Το $\epsilon(x)$ είναι *αδύναμο*, δηλαδή $(\epsilon(x))^2 = \epsilon(x)$.

Έστω $\gamma(x)$ και $\delta(x)$ αντίστοιχα τα πολυώνυμα γεννήτορας και ελέγχου για τον κυκλικό κώδικα $\mathcal{C}$. Από τον τρόπο ορισμού τους ($\gamma(x) \cdot \delta(x) = x^n - 1$) έχουμε ότι είναι σχετικά πρώτα, επομένως υπάρχουν πολυώνυμα $\alpha(x)$, $\beta(x)$ έτσι ώστε:

$$\alpha(x) \cdot \gamma(x) + \beta(x) \cdot \delta(x) = 1. \qquad (*)$$

Έστω $\epsilon(x) = \alpha(x) \cdot \gamma(x)$. Αν θεωρήσουμε τον πολλαπλασιασμό $\mod (x^n - 1)$ (βλέπε τη σχετική συζήτηση πριν από την Πρόταση 3.2.3 στη σελίδα 174), τότε το πολυώνυμο $\epsilon(x) = \alpha(x) \cdot \gamma(x)$ ανήκει στον κυκλικό κώδικα $\mathcal{C}$. Επίσης, γνωρίζουμε (Θεώρημα 3.2.15) ότι ένα πολυώνυμο $c(x) \in \mathcal{R}_n$ είναι στοιχείο του κώδικα, αν και μόνο αν $c(x) \cdot \delta(x) = 0$ (υπενθυμίζουμε ότι ο πολλαπλασιασμός γίνεται $\mod (x^n - 1)$). Επομένως, από την σχέση $(*)$ για κάθε $c(x) \in \mathcal{C}$ έχουμε ότι $\alpha(x) \cdot \gamma(x) \cdot c(x) + \beta(x) \cdot \delta(x) \cdot c(x) = c(x)$, δηλαδή $\epsilon(x) \cdot c(x) = c(x)$. Η τελευταία σχέση αποδεικνύει ότι το $\epsilon(x)$ αφενός μεν είναι μοναδιαίο στοιχείο του $\mathcal{C}$, αφετέρου παράγει τον $\mathcal{C}$, αφού κάθε στοιχείο του είναι πολλαπλάσιο του $\epsilon(x)$.

Πολλαπλασιάζοντας και τα δύο μέλη της $(*)$ με το $\epsilon(x)$, εύκολα βλέπουμε ότι πράγματι ισχύει $(\epsilon(x))^2 = \epsilon(x)$.

Τέλος, το $\epsilon(x)$ είναι μοναδικό, διότι γενικά σε έναν δακτύλιο αν υπάρχει μοναδιαίο αυτό είναι μοναδικό.

Παρατηρήσεις 3.2.29. 1. Το πολυώνυμο $\epsilon(x)$ που πληροί τις παραπάνω ιδιότητες ονομάζεται **αδύναμος γεννήτορας** για τον κυκλικό κώδικα $\mathcal{C}$ και η σχέση $(*)$ μας δίνει τον τρόπο υπολογισμού του, αν γνωρίζουμε το πολυώνυμο γεννήτορα.

Αντίστροφα, αν γνωρίζουμε τον αδύναμο γεννήτορα $\epsilon(x)$ ενός κυκλικού κώδικα $\mathcal{C}$, τότε για το πολυώνυμο γεννήτορα έχουμε:

$$\gamma(x) = \text{μκδ}(\epsilon(x), x^n - 1).$$

Πράγματι, έχουμε ότι $\epsilon(x) = \alpha(x) \cdot \gamma(x)$, επομένως:

$$\text{μκδ}(\epsilon(x),\ x^n - 1) = (\alpha(x) \cdot \gamma(x), \gamma(x) \cdot \delta(x)) = \gamma(x),$$

αφού, όπως έπεται από την $(*)$, τα $\alpha(x)$ και $\delta(x)$ είναι σχετικά πρώτα.

2. Τα προηγούμενα συνάδουν με την Πρόταση 3.2.8, όπου εκεί υπάρχει ένας γενικός χαρακτηρισμός πότε ένα πολυώνυμο παράγει έναν κυκλικό κώδικα.

3. Πρέπει να παρατηρήσουμε ότι κάθε άλλο στοιχείο του κώδικα που πληροί τις ιδιότητες $\alpha)$ και $\gamma)$ συμπίπτει αναγκαστικά με το $\epsilon(x)$ [άρα πληροί και την ιδιότητα $\beta)$]. Πράγματι, αν $\vartheta(x)$ είναι ένα άλλο αδύναμο στοιχείο του κώδικα, το οποίο τον παράγει, τότε για το $\epsilon(x)$ θα έχουμε ότι $\epsilon(x) = p(x)\cdot\vartheta(x) = p(x)\cdot(\vartheta(x))^2 = (p(x)\cdot\vartheta(x))\cdot\vartheta(x) = \epsilon(x)\cdot\vartheta(x) = \vartheta(x)$.

Προς διάκριση, σε έναν κυκλικό κώδικα $\mathcal{C}$ με πολυώνυμο γεννήτορα $\gamma(x)$ και αδύναμο γεννήτορα $\epsilon(x)$, θα συμβολίζουμε $\mathcal{C} = \langle\, \gamma(x) \,\rangle = [[\, \epsilon(x) \,]]$.

Παραδείγματα 3.2.30. 1. Έστω το πολυώνυμο $x^4 - 1 \in \mathbb{Z}_3[x]$. Προφανώς, $x^4 - 1 = (x-1)(x+1)(x^2+1)$. Αν $\mathcal{C}$ είναι ο κυκλικός κώδικας με πολυώνυμο γεννήτορα $x^2 + 1$, τότε το πολυώνυμο $\epsilon(x) = 2x^2 + 2 \in \mathcal{R}_4$ πληροί τις παραπάνω ιδιότητες (να κάνετε τον έλεγχο!).

2. Έστω $\mathcal{C}$ ο κυκλικός κώδικας επί του $\mathbb{Z}_3$ μήκους 11 και με γεννήτορα πολυώνυμο $\gamma(x) = x^5 + x^4 - x^3 + x^2 - 1$. Επειδή ο κώδικας είναι μήκους 11, θεωρούμε την ανάλυση του $x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 -$

x^3+x^2-x-1) σε γινόμενο αναγώγων παραγόντων. Με την βοήθεια της Ευκλείδιας διαίρεσης πολυωνύμων υπολογίζουμε τα πολυώνυμα $\alpha(x)$ και $\beta(x)$ στον δακτύλιο $\mathbb{Z}_3[x]$ έτσι ώστε μκδ$(\alpha(x)(x^5+x^4-x^3+x^2-1),\ \beta(x)(x-1)(x^5-x^3+x^2-x-1)) = 1$.

Μετά από πράξεις (να κάνετε τον έλεγχο!) βρίσκουμε ότι $\alpha(x) = -x^5+x^4+x^2$, οπότε το πολυώνυμο $\epsilon(x) = \alpha(x)\gamma(x) = (-x^5+x^4+x^2)(x^5+x^4-x^3+x^2-1) = -x^{10}-x^8-x^7-x^6-x^2 \in \mathcal{R}_{11}$ είναι ο αδύναμος γεννήτορας του κυκλικού κώδικα, δηλαδή $\mathcal{C} = \langle x^5+x^4-x^3+x^2-1 \rangle = [[-x^{10}-x^8-x^7-x^6-x^2]]$.

Στην Πρόταση 3.2.11 είχαμε δει ότι, αν γνωρίζουμε το πολυώνυμο γεννήτορα ενός κυκλικού κώδικα, μπορούμε να υπολογίσουμε έναν γεννήτορα πίνακά του. Κάτι ανάλογο ισχύει αν γνωρίζουμε τον αδύναμο γεννήτορα ενός κυκλικού κώδικα.

Πρόταση 3.2.31. *Έστω $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n και διάστασης k επί ενός πεπερασμένου σώματος $\mathbb{F}$. Υποθέτουμε ότι το πολυώνυμο $\epsilon(x) = \sum_{i=0}^{n-1} e_i x^i$ είναι ο αδύναμος γεννήτορας του $\mathcal{C}$. Τότε ο $k \times n$ πίνακας:*

$$\begin{pmatrix} e_0 & e_1 & e_2 & \cdots & e_{n-2} & e_{n-1} \\ e_{n-1} & e_0 & e_1 & \cdots & e_{n-3} & e_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ e_{n-k+1} & e_{n-k+2} & e_{n-k+3} & \cdots & e_{n-k-1} & e_{n-k} \end{pmatrix},$$

ο οποίος έχει ως πρώτη γραμμή τους συντελεστές του $\epsilon(x)$ και ως επόμενες γραμμές τις πρώτες $k-1$ το πλήθος κυκλικές μεταθέσεις των συντελεστών του $\epsilon(x)$, είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{C}$.

Απόδειξη. Είναι προφανές ότι πρέπει και αρκεί να αποδείξουμε ότι το σύνολο $\{ x\epsilon(x), x^2\epsilon(x), x^3\epsilon(x), \ldots, x^{k-1}\epsilon(x) \}$ είναι μια βάση του κώδικα $\mathcal{C}$. Δηλαδή αρκεί να δείξουμε ότι για κάθε πολυώνυμο $\alpha(x) \in \mathbb{F}[x]$, βαθμού το πολύ $k-1$, με την ιδιότητα $\alpha(x)\epsilon(x) = 0$, έπεται ότι το $\alpha(x)$ είναι το μηδενικό πολυώνυμο (γιατί;).

Έστω $\gamma(x)$ το πολυώνυμο γεννήτορας του κώδικα. Τότε από τη σχέση $\alpha(x)\epsilon(x) = 0$ έχουμε $\alpha(x)\epsilon(x)\gamma(x) = 0$, δηλαδή $\alpha(x)\gamma(x) = 0$, αφού το πο-

λυώνυμο $\epsilon(x)$ είναι μοναδιαίο. Από την τελευταία σχέση έπεται ότι $\alpha(x) = 0$, δεδομένου ότι το $\gamma(x)$ είναι το πολυώνυμο γεννήτορας του κώδικα.

ό.έ.δ.

Για τον αδύναμο γεννήτορα ενός κυκλικού κώδικα ισχύει μια πρόταση ανάλογη με την Πρόταση 3.2.14.

Πρόταση 3.2.32. *Έστω $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{R}_n$ κυκλικοί κώδικες με αδύναμους γεννήτορες τα πολυώνυμα $\epsilon_1(x)$ και $\epsilon_2(x)$ αντίστοιχα, τότε έχουμε.*

1. *$\mathcal{C}_1 \subseteq \mathcal{C}_2$, αν και μόνο αν $\epsilon_1(x)\epsilon_2(x) = \epsilon_1(x)$.*
2. *Η τομή $\mathcal{C}_1 \cap \mathcal{C}_2$ είναι κυκλικός κώδικας με αδύναμο γεννήτορα το πολυώνυμο $\epsilon_1(x)\epsilon_2(x)$.*
3. *Το άθροισμα $\mathcal{C}_1 + \mathcal{C}_2$ είναι κυκλικός κώδικας με αδύναμο γεννήτορα το πολυώνυμο $\epsilon_1(x) + \epsilon_2(x) - \epsilon_1(x)\epsilon_2(x)$.*

Απόδειξη.

1. Επειδή τα πολυώνυμα $\epsilon_1(x)$ και $\epsilon_2(x)$ παράγουν τους κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$, αντίστοιχα, έχουμε ότι $\mathcal{C}_1 \subseteq \mathcal{C}_2$, αν και μόνο αν υπάρχει πολυώνυμο $\alpha(x) \in \mathcal{R}_n$, έτσι ώστε:

$$\epsilon_1(x) = \alpha(x)\epsilon_2(x) = \alpha(x)(\epsilon_2(x)\epsilon_2(x)) = (\alpha(x)\epsilon_2(x))\epsilon_2(x) = \epsilon_1(x)\epsilon_2(x).$$

2. Το γινόμενο $\epsilon_1(x)\epsilon_2(x)$ ανήκει στην τομή $\mathcal{C}_1 \cap \mathcal{C}_2$ και προφανώς είναι αδύναμο στοιχείο, οπότε έπεται το αποτέλεσμα.

3. Είναι προφανές ότι $(\epsilon_1(x) + \epsilon_2(x) - \epsilon_1(x)\epsilon_2(x))^2 = \epsilon_1(x) + \epsilon_2(x) - \epsilon_1(x)\epsilon_2(x)$ και ότι για το (τυχαίο) στοιχείο $c_1(x)+c_2(x) \in \mathcal{C}_1+\mathcal{C}_2$ ισχύει ότι $(c_1(x)+c_2(x))(\epsilon_1(x)+\epsilon_2(x)-\epsilon_1(x)\epsilon_2(x)) = \cdots = c_1(x)+c_2(x)$, οπότε έπεται το αποτέλεσμα.

ό.έ.δ.

Στο Θεώρημα 3.2.16 είχαμε δει ότι, αν γνωρίζουμε το πολυώνυμο γεννήτορα ενός κυκλικού κώδικα, μπορούμε να υπολογίσουμε το πολυώνυμο γεννήτορα του δυϊκού κώδικα. Έδώ θα δούμε πως μπορούμε να υπολογίσουμε τον αδύναμο γεννήτορα του δυϊκού κώδικα από τον αδύναμο γεννήτορα του κώδικα.

Πρόταση 3.2.33. *Έστω $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n και διάστασης k επί ενός πεπερασμένου σώματος $\mathbb{F}$. Υποθέτουμε ότι το πολυώνυμο $\epsilon(x) = \sum_{i=0}^{n-1} e_i x^i$ είναι ο αδύναμος γεννήτορας του $\mathcal{C}$. Τότε ο αδύναμος γεννήτορας του δυϊκού κώδικα $\mathcal{C}^\perp$ είναι το πολυώνυμο $1 - \epsilon(x^{n-1}) \in \mathcal{R}_n$.*

Απόδειξη. Έστω $x^n - 1 = \gamma(x)\delta(x)$, όπου $\gamma(x)$ είναι το πολυώνυμο γεννήτορας του $\mathcal{C}$ και $\delta(x) = h_0 + h_1 x + \cdots h_k x^k$ το πολυώνυμο ελέγχου ισοτιμίας. Τότε το πολυώνυμο γεννήτορας του δυϊκού κώδικα είναι το $d(x) = h_0^{-1} x^k \delta(x^{-1}) = h_0^{-1} x^k \delta(x^{n-1}) \in \mathcal{R}_n$.

Έχουμε δει ότι ο αδύναμος γεννήτορας του κώδικα $\mathcal{C}$ είναι ίσος με $\epsilon(x) = \alpha(x)\cdot\gamma(x)$, όπου τα $\alpha(x)$ και $\beta(x)$ ικανοποιούν τη σχέση $\alpha(x)\cdot\gamma(x) + \beta(x)\cdot\delta(x) = 1$. Τότε έχουμε $d(x)(1 - \epsilon(x^{n-1})) = d(x) - h_0^{-1} x^k \delta(x^{n-1})\alpha(x^{n-1}) \cdot \gamma(x^{n-1}) = d(x)$. Η τελευταία ισότητα αποδυκνύει ότι το πολυώνυμο $1 - \epsilon(x^{n-1}) \in \mathcal{R}_n$ είναι το μοναδιαίο στον κώδικα $\mathcal{C}^\perp$. Άρα και γεννήτορας (γιατί;). Προφανώς είναι και αδύναμο στοιχείο (γιατί;). Οπότε ολοκληρώθηκε η απόδειξη. ό.έ.δ.

Έστω $x^n - 1 = \prod_{i=1}^{k} m_i(x)$ η ανάλυση του $x^n - 1$ σε γινόμενο μονικών αναγώγων πολυωνύμων επί του σώματος $\mathbb{F}$. Στη σελίδα 183 είχαμε δει ότι για κάθε $i = 1, \ldots, k$ ο αντίστοιχος κυκλικός κώδικας $\mathcal{C}_i$ με πολυώνυμο γεννήτορα το πολυώνυμο $m_i(x)$ είναι μέγιστος (ως ιδεώδες του δακτυλίου $\mathcal{R}_n$).

Επίσης, είχαμε δει ότι, αν $\mu_i(x) = \frac{x^n - 1}{m_i(x)}$, τότε, για κάθε $i = 1, 2, \ldots, k$, ο αντίστοιχος κυκλικός κώδικας $\mathcal{D}_i$ με πολυώνυμο γεννήτορα το $\mu_i(x)$, είναι ελάχιστος (ως ιδεώδες του δακτυλίου $\mathcal{R}_n$).

Εδώ μπορούμε να λεπτολογήσουμε περισσότερο.

Πρόταση 3.2.34. *Έστω $x^n - 1 = \prod_{i=1}^{k} m_i(x)$ η ανάλυση του $x^n - 1$ σε γινόμενο μονικών αναγώγων πολυωνύμων επί του σώματος $\mathbb{F}$. Για κάθε $i = 1, 2, \ldots, k$ έστω $\mu_i(x) = \frac{x^n - 1}{m_i(x)}$ και $\mathcal{D}_i$ ο αντίστοιχος κυκλικός κώδικας με πολυώνυμο γεννήτορα το $\mu_i(x)$ και αδύναμο γεννήτορα το πολυώνυμο $\epsilon_i(x)$. Τότε:*

i) Οι κώδικες $\mathcal{D}_i$ είναι τα μόνα (μη μηδενικά) ελάχιστα ιδεώδη του δακτυλίου $\mathcal{R}_n$.

ii) *Ο δακτύλιος* $\mathcal{R}_n$ *(ως διανυσματικός χώρος επί του* $\mathbb{F}$*) είναι το ευθύ άθροισμα των κυκλικών κωδίκων* $\mathcal{D}_i$, $i = 1, 2, \ldots, k$.

iii) *Για* $i \neq j$, $\epsilon_i(x) \cdot \epsilon_j(x) = 0$ *στον δακτύλιο* $\mathcal{R}_n$.

iv) $\sum_{i=1}^{k} \epsilon_i(x) = 1$ *στον δακτύλιο* $\mathcal{R}_n$.

v) *Κάθε κυκλικός κώδικας* $\mathcal{D}_i$ *έχει τη δομή σώματος, το οποίο περιέχει το σώμα* $\mathbb{F}$.

Απόδειξη. *i)* Η απόδειξη είναι άμεση από τον τρόπο ορισμού των κυκλικών κωδίκων $\mathcal{D}_i$.

ii) Θα δείξουμε πρώτα ότι το άθροισμα των $\mathcal{D}_i$ είναι ευθύ.

Πράγματι, για $i \neq j$ το άθροισμα $\sum_{i \neq j} \mathcal{D}_j$ έχει ως γεννήτορα πολυώνυμο τον $\text{μκδ}(\mu_j(x),\ i \neq j)$ (βλέπε Πρόταση 3.2.14). Πάλι από την ίδια πρόταση έχουμε ότι η τομή $\mathcal{D}_i \cap \sum_{i \neq j} \mathcal{D}_j$ έχει ως γεννήτορα πολυώνυμο το $\text{εκπ}(\mu_i(x),$, $\text{μκδ}(\mu_j(x),\ i \neq j))$.

Από τον τρόπο ορισμού των $\mu_i(x) = \frac{x^n-1}{m_i(x)}$ έπεται εύκολα ότι το πολυώνυμο $\text{εκπ}(\mu_i(x),\ ,\ \text{μκδ}(\mu_j(x),\ i \neq j))$ είναι πολαπλάσιο του $x^n - 1$, δηλαδή μηδέν στον δακτύλιο $\mathcal{R}_n$ και αυτό για κάθε $i = 1, 2, \ldots, k$. Άρα, το άθροισμα είναι ευθύ,

Έστω ότι ο βαθμός κάθε $m_i(x)$ είναι ίσος με d_i. Τότε η διάσταση κάθε κώδικα $\mathcal{D}_i$ είναι ίση με d_i (γιατί;). Συνεπώς, ο δακτύλιος $\mathcal{R}_n$ είναι το ευθύ άθροισμα των κυκλικών κωδίκων $\mathcal{D}_i$, αφού $\sum_{i=1}^{k} d_i = n$.

iii) Για $i \neq j$ το γινόμενο $\epsilon_i(x) \cdot \epsilon_j(x) \in \mathcal{D}_i \cap \mathcal{D}_j = 0$ στον δακτύλιο $\mathcal{R}_n$.

iv) Από την Πρόταση 3.2.32 έχουμε ότι το άθροισμα $\mathcal{D}_1 + \mathcal{D}_2$ έχει αδύναμο γεννήτορα το $\epsilon_1(x) + \epsilon_2(x) - \epsilon_1(x)\epsilon_2(x)$. Οπότε, από το προηγούμενο ερώτημα και με επαγωγή στο πλήθος k των κυκλικών κωδίκων $\mathcal{D}_i$, έπεται το αποτέλεσμα, καθότι ο αδύναμος γεννήτορας του $\mathcal{R}_n$ είναι το 1.

v) Επειδή κάθε $\mathcal{D}_i$ είναι ιδεώδες, το μόνο που απομένει να αποδειχθεί είναι να αποδείξουμε ότι κάθε μη μηδενικό στοιχείο του $\mathcal{D}_i$ είναι αντιστρέψιμο. Έστω $0 \neq \alpha(x) \in \mathcal{D}_i$. Επειδή το $\mathcal{D}_i$ είναι ελάχιστο έχουμε ότι $\mathcal{D}_i = \langle \alpha(x) \rangle$, δηλαδή $\epsilon_i(x) = \alpha(x)\beta(x)$ με $\beta(x) \in \mathcal{R}_n$. Τότε όμως $\beta(x)\epsilon_i(x) \in \mathcal{D}_i$ και $\epsilon_i(x) = \alpha(x)(\beta(x)\epsilon_i(x))$ με το $\beta(x)\epsilon_i(x)$ να είναι το αντίστροφο του $\alpha(x)$. ό.έ.δ.

Πόρισμα 3.2.35. *i) Κάθε κυκλικός κώδικας $\mathcal{C}$ μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$ είναι το ευθύ άθροισμα ελαχίστων κυκλικών κωδίκων.*

ii) Για κάθε (μη μηδενικό) αδύναμο στοιχείο $\epsilon(x)$ του δακτυλίου $\mathcal{R}_n$ υπάρχει ένα υποσύνολο δεικτών T από το σύνολο $\{1, 2, \dots, k\}$, έτσι ώστε $\epsilon(x) = \sum_{j\in T} \epsilon_j(x)$.

Απόδειξη. i) Έστω $x^n - 1 = \prod_{i=1}^{k} m_i(x)$ η ανάλυση σε γινόμενο μονικών αναγώγων πολυωνύμων. Αν $\gamma(x)$ είναι το πολυώνυμο γεννήτορας του $\mathcal{C}$, τότε υπάρχει ένα σύνολο δεικτών $S = \{i_1, i_2, \dots, i_\nu\}$, έτσι ώστε $\gamma(x) = m_{i_1}(x)m_{i_2}(x)\cdots m_{i_\nu}(x)$. Τότε, επειδή τα $m_i(x)$ είναι ανάγωγα και διαφορετικά μεταξύ τους[4] έπεται εύκολα ότι:

$$\gamma(x) = m_{i_1}(x)m_{i_2}(x)\cdots m_{i_\nu}(x) = \text{μκδ}(\,\mu_j(x),\ j \notin S\,)$$

(προσπαθήστε να το αποδείξετε!). Οπότε το αποτέλεσμα έπεται από τα προηγούμενα.

ii) Κάθε αδύναμο στοιχείο $\epsilon(x)$ ορίζει έναν κυκλικό κώδικα $\mathcal{C}$. Αν $\gamma(x) = m_{i_1}(x)m_{i_2}(x)\cdots m_{i_\nu}(x)$ είναι το πολυώνυμο γεννήτορας, τότε από το πρώτο μέρος έχουμε $\mathcal{C} = \langle\, \epsilon(x)\,\rangle = \langle\, \gamma(x)\,\rangle = \sum_{j\notin S}\langle \epsilon_j(x)\rangle = \langle \sum_{j\notin S} \epsilon_j(x)\rangle$. Οπότε έχουμε $\epsilon(x) = \sum_{j\notin S} \epsilon_j(x)$, καθότι αφενός μεν κάθε κυκλικός κώδικας παράγεται από ένα μόνο αδύναμο στοιχείο του αφ' ετέρου δε το άθροισμα αδυνάμων στοιχείων στην προκειμένη περίπτωση είναι αδύναμο. (Από την προηγουμένη πρόταση έχουμε ότι $\epsilon_i(x)\cdot\epsilon_j(x) = 0$ για $i \neq j$).

ό.έ.δ.

Σχόλιο 3.2.36. Λόγω των αποτελεσμάτων του προηγουμένου πορίσματος τα αδύναμα στοιχεία $\epsilon_i(x)$, τα οποία αντιστοιχούν στα πολυώνυμα $\mu_i(x) = \frac{x^n-1}{m_i(x)}$ και ορίζουν τους αντίστοιχους ελάχιστους κώδικες $\mathcal{D}_i$ ονομάζονται **πρωταρχικά αδύναμα στοιχεία**.

Από την Πρόταση 3.2.19 έπεται άμεσα και το επόμενο.

Πόρισμα 3.2.37. *Έστω $\mathcal{C}$ ο κυκλικός κώδικας μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$ με πολυώνυμο γεννήτορα $\gamma(x)$ και πολυώνυμο ελέγχου*

[4] Δεν ξεχνάμε ότι έχουμε υποθέσει ότι ο n είναι πρώτος προς την χαρακτηριστική του σώματος.

$\delta(x)$. Αν $\epsilon(x)$ είναι ο αδύναμος γεννήτορας του $\mathcal{C}$, τότε το πολυώνυμο $1-\epsilon(x)$ είναι ο αδύναμος γεννήτορας του κυκλικού κώδικα $\overline{\mathcal{C}} = \langle \delta(x) \rangle$.

Όπως έχουμε δει (ιδέ Παράδειγμα 3.2.2$_5$), αν έχουμε έναν κυκλικό κώδικα δεν έπεται κατ' ανάγκην ότι ένας μεταθετικά ισοδύναμος κώδικας θα είναι και αυτός κυκλικός. Οπότε γεννάται το ερώτημα:
Έστω $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n. Υπάρχει μετάθεση $\sigma \in S_n$, έτσι ώστε ο μεταθετικά ισοδύναμος κώδικας $\mathcal{C}_\sigma$ να είναι και αυτός κυκλικός;

Στο προηγούμενο κεφάλαιο (σελίδα 110) είχαμε ορίσει την μετάθεση πολλαπλασιαστή. Συγκεκριμένα για έναν φυσικό αριθμό n και κάθε ακέραιο a πρώτο προς τον n η απεικόνιση $\varrho_a(i) = ia(mod\, n)$ $i = 1, 2, \ldots, n$ ορίζει μια μετάθεση σε n σύμβολα, η οποία ονομάζεται πολλαπλασιαστής.

Έστω $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Θα δείξουμε ότι ο μεταθετικά ισοδύναμος κώδικας $\mathcal{C}_{\varrho_a}$ είναι και αυτός κυκλικός.

Ως γνωστόν, κάθε λέξη $c_0\, c_1 \cdots c_{n-1}$ αντιστοιχίζεται με το πολυώνυμο:

$$f(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathcal{R}_n = \mathbb{F}[x]/\langle x^n - 1 \rangle.$$

Εφαρμόζοντας την μετάθεση ϱ_a στις θέσεις των χαρακτήρων c_i, ο χαρακτήρας c_i μετατίθεται στη θέση $ia(mod\, n)$, δηλαδή (μεταβαίνοντας στα πολυώνυμα) είναι ο συντελεστής του $x^{ia(mod\, n)}$. Η παρατήρηση αυτή μας επιτρέπει να θεωρήσουμε την μετάθεση ϱ_a ως μια απεικόνιση $\varrho_a : \mathcal{R}_n \longrightarrow \mathcal{R}_n$ με $\varrho_a(f(x)) = f(x^a)$.
Προφανώς, η απεικόνιση αυτή είναι 1-1. Πράγματι, δύο διαφορετικά πολυώνυμα $f(x), g(x) \in \mathcal{R}_n$ έχουν διαφορετικούς συντελεστές σε τουλάχιστον μία θέση i, οπότε οι εικόνες τους θα διαφέρουν τουλάχιστον στη θέση $ia(modn)$. Επειδή ο δακτύλιος είναι πεπερασμένος, η απεικόνιση είναι και επί.

Πρόταση 3.2.38. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία, n ένας φυσικός αριθμός και a ένας ακέραιος πρώτος προς τον n.*

i) Η απεικόνιση ϱ_a είναι ένας αυτομορφισμός του δακτυλίου $\mathcal{R}_n$.

ii) Για κάθε αδύναμο στοιχείο $\epsilon(x)$ του $\mathcal{R}_n$ έχουμε ότι και η εικόνα του $\varrho_a(\epsilon(x))$ είναι αδύναμο στοιχείο.

iii) Για κάθε κυκλικό κώδικα $\mathcal{C}$ ο μεταθετικά ισοδύναμος $\mathcal{C}_{\varrho_a}$ κώδικας είναι και αυτός κυκλικός. Μάλιστα δε, αν το $\epsilon(x)$ είναι ένας αδύναμος γεννήτορας του κώδικα $\mathcal{C}$, τότε η εικόνα $\varrho_a(\epsilon(x))$ είναι αδύναμος γεννήτορας του $\mathcal{C}_{\varrho_a}$.

Απόδειξη. i) Έχουμε δει ότι η απεικόνιση $\varrho_a : \mathcal{R}_n \longrightarrow \mathcal{R}_n$ με $\varrho_a(f(x)) = f(x^a)$ είναι 1-1 και επί.

Από τον τρόπο ορισμού της είναι προφανές ότι για $f(x), g(x) \in \mathcal{R}_n$ ισχύει ότι $\varrho_a(f(x)+g(x)) = \varrho_a(f(x)) + \varrho_a(g(x))$ και $\varrho_a(f(x)\cdot g(x)) = \varrho_a(f(x))\cdot\varrho_a(g(x))$. Επομένως, η ϱ_a είναι αυτομορφισμός του δακτυλίου $\mathcal{R}_n$.

ii) Αν $\epsilon(x)$ είναι ένα αδύναμο στοιχείο του $\mathcal{R}_n$, τότε από τη σχέση $(\epsilon(x))^2 = \epsilon(x)$ έχουμε $\varrho_a((\epsilon(x))^2) = \varrho_a(\epsilon(x))$. Δηλαδή $(\varrho_a(\epsilon(x)))^2 = \varrho_a(\epsilon(x))$. Άρα, η εικόνα $\varrho_a(\epsilon(x))$ είναι αδύναμο στοιχείο.

iii) Δεδομένου ότι το σύνολο $\{\, x\epsilon(x),\, x^2\epsilon(x),\, x^3\epsilon(x),\, \ldots,\, x^{k-1}\epsilon(x)\,\}$ είναι μια βάση του κώδικα $\mathcal{C}$ (ιδέ την απόδειξη της Πρότασης 3.2.31), το σύνολο $\{\, \varrho_a(x\epsilon(x)),\, \varrho_a(x^2\epsilon(x)),\, \varrho_a(x^3\epsilon(x)),\, \ldots,\, \varrho_a(x^{k-1}\epsilon(x))\,\}$ είναι μια βάση του κώδικα $\mathcal{C}_{\varrho_a}$. Συνεπώς, ο κώδικας $\mathcal{C}_{\varrho_a}$ είναι κυκλικός με γεννήτορα το αδύναμο στοιχείο $\varrho_a(\epsilon(x))$.

ό.έ.δ.

Συνδυάζοντας την προηγούμενη πρόταση με την Πρόταση 3.2.8 έχουμε το ακόλουθο Πόρισμα.

Πόρισμα 3.2.39. *Έστω ένας κυκλικός κώδικας $\mathcal{C}$ μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Υποθέτουμε ότι το σύνολο των σημείων μηδενισμού του είναι το $\{\, \omega^{i_1}, \omega^{i_2}, \ldots, \omega^{i_{n-k}}\,\}$, όπου ω είναι μια πρωταρχική ρίζα της μονάδος. Για κάθε a ακέραιο πρώτο προς τον n το σύνολο $\{\, \omega^{bi_1}, \omega^{bi_2}, \ldots, \omega^{bi_{n-k}}\,\}$, όπου b είναι ο αντίστροφος του $a (\mathrm{mod}\, n)$, είναι το σύνολο σημείων μηδενισμού του κώδικα $\mathcal{C}_{\varrho_a}$.*

Απόδειξη. Έστω $\epsilon(x)$ ο αδύναμος γεννήτορας του κώδικα $\mathcal{C}$, τότε το $\varrho_a(\epsilon(x))$ είναι ο αδύναμος γεννήτορας του $\mathcal{C}_{\varrho_a}$. Τα σημεία μηδενισμού του κώδικα $\mathcal{C}$

είναι και ρίζες του $\epsilon(x)$ (ιδέ Πρόταση 3.2.8). Όμοια τα σημεία μηδενισμού του κώδικα $\mathcal{C}_{\varrho_a}$ είναι και ρίζες του $\varrho_a(\epsilon(x)) = \epsilon(x^a) mod(x^n - 1)$.

Το αποτέλεσμα έπεται από το γεγονός ότι η n-οστη ρίζα της μονάδος ω^j είναι ρίζα του $\epsilon(x^a) mod(x^n - 1)$, αν και μόνο αν η ω^{bj} είναι ρίζα του $\epsilon(x)$. ό.έ.δ.

Αν έχουμε ένα πεπερασμένο σώμα $\mathbb{F}$ με q το πλήθος στοιχεία και έναν κυκλικό κώδικα $\mathcal{C}$ επί του $\mathbb{F}$ μήκους n, όπου, όπως πάντα, υποθέτουμε ότι οι n και q είναι σχετικά πρώτοι, τότε ο πολλαπλασιαστής ϱ_q έχει ιδιαίτερη σημασία.

Για κάθε στοιχείο $g(x)$ του κώδικα $\mathcal{C}$ έχουμε ότι $\varrho_q(g(x)) = g(x^q) = (g(x))^q \in \mathcal{C}$, άρα $\varrho_q(\mathcal{C}) \subseteq \mathcal{C}$. Επειδή δε η ϱ_q είναι 1-1, είναι και επί του $\mathcal{C}$. Δηλαδή είναι ένας αυτομορφισμός του κώδικα $\mathcal{C}$.

Θα μπορούσαμε να λεπτολογήσουμε περισσότερο. Συγκεκριμένα, αν $\epsilon(x)$ είναι ο αδύναμος γεννήτορας του κυκλικού κώδικα $\mathcal{C}$, τότε από το Πόρισμα 3.2.35 έχουμε ότι $\epsilon(x) = \sum_{j=1}^{\nu} \epsilon_j(x)$, όπου κάθε $\epsilon_j(x)$ είναι πρωταρχικό αδύναμο στοιχείο. Τότε έχουμε:

$$\varrho_q(\epsilon(x)) = \varrho_q\left(\sum_{j=1}^{\nu} \epsilon_j(x)\right) = \sum_{j=1}^{\nu} \epsilon_j(x^q).$$

Τα πολυώνυμα $\epsilon_j(x)$ και $\epsilon_j(x^q) = (\epsilon_j(x))^q$ είναι αδύναμα στοιχεία που ανήκουν στον ελάχιστο κώδικα $\mathcal{D}_j$, άρα συμπίπτουν (ιδέ Άσκηση $3.2.5_{27}$). Επομένως, έχουμε ότι $\varrho_q(\epsilon(x)) = \epsilon(x)$.

Τα προηγούμενα αποτελούν την απόδειξη της επομένης πρότασης.

Πρόταση 3.2.40. *Έστω $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία, όπου, όπως πάντα, υποθέτουμε ότι οι n και q είναι σχετικά πρώτοι. Τότε ο πολλαπλασιαστής ϱ_q είναι ένας μεταθετικός αυτομορφισμός του $\mathcal{C}$. Μάλιστα δε, αν $\epsilon(x)$ είναι ο αδύναμος γεννήτορας του $\mathcal{C}$, ισχύει ότι $\varrho_q(\epsilon(x)) = \epsilon(x)$.*

3.2.4 Κωδικοποίηση και αποκωδικοποίηση με κυκλικούς κώδικες

Έστω $\mathcal{C}$ ένας $[n, k, d]$ κυκλικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$. Ο κώδικας $\mathcal{C}$ είναι γραμμικός, επομένως μπορούμε να εφαρμόσουμε

τις μεθόδους κωδικοποίησης και αποκωδικοποίησης που αναφέρονται στην Παράγραφο 2.4.

Επειδή όμως ο κώδικας είναι κυκλικός μπορούμε να εκμεταλλευτούμε την δομή του ως ιδεώδες του δακτυλίου $\mathcal{R}_n \simeq \mathbb{F}/\langle x^n - 1\rangle$ και να έχουμε αποτελεσματικότερους τρόπους κωδικοποίησης και αποκωδικοποίησης.

Έστω $\gamma(x)$ το πολυώνυμο γεννήτορας του κώδικα $\mathcal{C}$ και G ο γεννήτορας πίνακας, του οποίου οι γραμμές είναι κυκλικές μεταθέσεις των συντελεστών του πολυωνύμου $\gamma(x)$ (ιδέ Πρόταση 3.2.11). Αν έχουμε ένα πηγαίο μήνυμα $\mathbf{a} = (a_0, a_1, \dots, a_{k-1}) \in \mathbb{F}$, τότε ο γνωστός τρόπος κωδικοποίησης $\mathbf{a}$G θα μπορούσε να πραγματοποιηθεί ως εξής:

Στο στοιχείο $\mathbf{a} = (a_0, a_1, \dots, a_{k-1})$ αντιστοιχούμε το πολυώνυμο $\alpha(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ και αντί του πολλαπλασιασμού $\mathbf{a}$G εκτελούμε τον πολλαπλασιασμό πολυωνύμων $\alpha(x) \cdot \gamma(x)$ (ιδέ Θεώρημα 3.2.6).

Η κωδικοποίηση αυτή δεν είναι συστηματική. Θα μπορούσαμε να έχουμε μια συστηματική κωδικοποίηση ως εξής:

Αντί του προς κωδικοποίηση μηνύματος $\alpha(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ λαμβάνουμε το πολυώνυμο $x^{n-k} \cdot \alpha(x)$. Το πολυώνυμο αυτό είναι βαθμού το πολύ $n-1$ και εμπεριέχει το προς κωδικοποίηση μήνυμα στους συντελεστές των $x^{n-k}, x^{n-k+1}, \dots, x^{n-1}$.

Από την ταυτότητα της διαίρεσης έχουμε:

$$x^{n-k} \cdot \alpha(x) = \gamma(x)\pi(x) + \upsilon(x) \quad \text{με } deg(\upsilon(x)) < deg(\gamma(x)) \text{ ή } \upsilon(x) = 0.$$

Τότε όμως $x^{n-k} \cdot \alpha(x) - \upsilon(x) = \gamma(x)\pi(x) \in \mathcal{C}$, με το προς κωδικοποίηση μήνυμα $\alpha(x)$ να κωδικοποιήται (αμετάβλητο) ως $c(x) = \gamma(x)\pi(x) \in \mathcal{C}$ καταλαμβάνοντας τις θέσεις των συντελεστών των $x^{n-k}, x^{n-k+1}, \dots, x^{n-1}$, ενώ το υπόλοιπο πολυώνυμο $\upsilon(x)$ αποτελεί το τμήμα προστασίας από τους θορύβους.

Ένας άλλος τρόπος για συστηματική κωδικοποίηση βασίζεται στο πολυώνυμο ελέγχου του κώδικα.

Έστω $\gamma(x)$ το πολυώνυμο γεννήτορας του κώδικα. Το πολυώνυμο ελέγχου είναι το πολυώνυμο:

$$\frac{x^n - 1}{\gamma(x)} = \delta(x) = h_k x^k + h_{k-1}x^{k-1} + \cdots + h_1 x + h_0.$$

Ένας πίνακας ελέγχου του κώδικα $\mathcal{C}$ είναι ο $(n-k)\times n$ πίνακας:

$$\mathrm{H}=\begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{pmatrix}$$

(ιδέ Θεώρημα3.2.16).

Υποθέτουμε ότι έχουμε προς κωδικοποίηση το μήνυμα $\mathbf{a}=(a_0,a_1,\dots,a_{k-1})$ $\alpha(x)=a_0+a_1+\cdots+a_{k-1}x^{k-1}$ και θέλουμε μια συστηματική κωδικοποίηση, όπου στο κωδικοποιημένο μήνυμα οι πρώτοι k το πλήθος χαρακτήρες να αποτελούνται από τους χαρακτήρες του προς κωδικοποίηση μηνύματος.

Το κωδικοποιημένο μήνυμα θα είναι το:

$$\mathbf{c}=(c_0,c_1,\dots,c_{k-1},c_k,c_{k+1},\dots,c_{n-1}),$$

όπου $c_0=a_0, c_1=a_1,\dots,c_{k-1}=a_{k-1}$ και οι υπόλοιποι χαρακτήρες c_i, $i=k,\dots,n-1$ υπολογίζονται από τη σχέση $\mathbf{c}\cdot\mathrm{H}^t=0$. Δηλαδή έχουμε $c_i=h_0^{-1}(-\sum_{j=1}^{k}h_jc_{i-j})$.

Παράδειγμα 3.2.41. Έστω $\mathcal{C}$ ο δυαδικός κυκλικός κώδικας με παραμέτρους $[9,3,d]$ και γεννήτορα πολυώνυμο $\gamma(x)=1+x^3+x^6$. Υποθέτουμε ότι έχουμε προς κωδικοποίηση το μήνυμα $\mathbf{a}=(a_0,a_1,a_2)$. Σύμφωνα με τα προηγούμενα, μπορούμε να κωδικοποιήσουμε το μήνυμα κατά τρεις τρόπους:

Θεωρούμε το πολυώνυμο $\alpha(x)=a_0+a_1x+a_2x^2$. Εκτελούμε τον πολλαπλασιασμό:

$$\alpha(x)\cdot\gamma(x)=a_0+a_1x+a_2x^2+a_0x^3+a_1x^4+a_2x^5+a_1x^6+a_1x^7+a_2x^8,$$

οπότε το κωδικοποιημένο μήνυμα είναι το: $(a_0,a_1,a_2,a_0,a_1,a_2,a_1,a_1,a_2)$.

Αν θέλουμε συστηματική κωδικοποίηση, αντί του πολυωνύμου $\alpha(x)=a_0+a_1x+a_2x^2$, θεωρούμε το πολυώνυμο $x^{9-3}\cdot\alpha(x)$. Εκτελούμε τη διαίρεση με το πολυώνυμο γεννήτορα $1+x^3+x^6$ και βρίσκουμε υπόλοιπο $\upsilon(x)=a_2+a_0x+a_1x^2+0x^3+a_0x^4+a_1x^5$. Οπότε το κωδικοποιημένο μήνυμα είναι το $(a_2,a_0,a_1,0,a_0,a_1,a_0,a_1,a_2)$ με το πρώτο τμήμα των έξι χαρακτήρων να αποτελεί την προστασία του μηνύματος και το τελευταίο τμήμα των τριών

χαρακτήρων να αποτελεί το (αμετάβλητο) προς κωδικοποίηση μήνυμα (να κάνετε έλεγχο των πράξεων).

Αν θέλουμε συστηματική κωδικοποίηση με την βοήθεια του πολυωνύμου ελέγχου, θεωρούμε την ανάλυση $x^9-1 = \gamma(x)\cdot\delta(x) = (1+x^3+x^6)(x^3+1) \in \mathbb{Z}_2[x]$. Ένας πίνακας ελέγχου ισοτιμίας είναι ο:

$$\mathrm{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Οπότε το κωδικοποιημένο μήνυμα θα είναι το $\mathbf{c} = (c_0, c_1, c_2, c_3, \dots, c_8)$, όπου $c_0 = a_0, c_1 = a_1, c_2 = a_2$ και οι υπόλοιποι χαρακτήρες c_i, $i = 3, \dots, 8$ υπολογίζονται από τη σχέση $\mathbf{c}\cdot\mathrm{H}^t = 0$. Δηλαδή έχουμε $c_3 = a_0, c_4 = a_1, c_5 = a_2, c_6 = a_0, c_7 = a_1, c_8 = a_2$. Οπότε το κωδικοποιημένο μήνυμα είναι το $(a_0, a_1, a_2, a_0, a_1, a_2, a_0, a_1, a_2)$ με το πρώτο τμήμα των τριών χαρακτήρων να αποτελεί το (αμετάβλητο) προς κωδικοποίηση μήνυμα και το τελευταίο τμήμα των έξι χαρακτήρων να αποτελεί την προστασία του μηνύματος (να κάνετε έλεγχο των πράξεων).

Παρατηρήστε ότι, στο συγκεκριμένο παράδειγμα, η προστασία του μηνύματος επιτυγχάνεται με την επανάληψη του προς κωδικοποίηση μηνύματος άλλες δύο φορές. Οπότε κατά την αποκωδικοποίηση, αν μια από τις τρεις υπολέξεις (των τριών χαρακτήρων η κάθε μια) διαφέρει από τις δύο άλλες (ίσες) λέξεις, αμέσως ανιχνεύεται λάθος.

Η αποκωδικοποίηση με έναν κυκλικό κώδικα θα μπορούσε να γίνει με την βοήθεια μιας αντιπροσωπευτικής διάταξης (ιδέ Παράγραφο 2.4.1) ή με την βοήθεια του συνδρόμου (ιδέ Παράγραφο 2.4.4). Επειδή όμως ο κώδικας είναι κυκλικός, μπορούμε να ορίσουμε το σύνδρομο θεωρώντας τα στοιχεία του ως πολυώνυμα.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ κυκλικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$ με πολυώνυμο γεννήτορα $\gamma(x)$. Για κάθε πολυώνυμο $f(x) \in \mathbb{F}[x]$ από

την ταυτότητα της διαίρεσης πολυωνύμων έχουμε ότι υπάρχουν (μοναδικά) $\pi(x),\ \upsilon(x) \in \mathbb{F}[x]$ έτσι ώστε $f(x) = \pi(x)\gamma(x) + \upsilon(x)$ με $\upsilon(x) = 0$ ή $deg(\upsilon(x)) < deg(f(x))$.

Ορίζουμε την απεικόνιση:

$$\sigma : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/\langle\, \gamma(x)\,\rangle \simeq \mathbb{F}_{n-k-1}[x],$$

με $\sigma(f(x)) = \upsilon(x) + \langle\, \gamma(x)\,\rangle$.

Ορισμός 3.2.42. *Η εικόνα $\sigma(f(x))$ θα ονομάζεται το **σύνδρομο** του πολυωνύμου $f(x)$.*

Πρόταση 3.2.43. *1. Η απεικόνιση $\sigma : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/\langle\, \gamma(x)\,\rangle \simeq \mathbb{F}_{n-k-1}[x]$ είναι γραμμική, δηλαδή $\sigma(af(x) + bg(x)) = a\sigma(f(x)) + b\sigma(g(x))$ για όλα τα $f(x),\ g(x) \in \mathbb{F}[x]$ και για όλα τα $a,\ b \in \mathbb{F}$.*

2. $\sigma(f(x) + \phi(x)(x^n - 1)) = \sigma(f(x))$.

Απόδειξη. Η απόδειξη είναι εύκολη και αφίεται ως άσκηση. ό.έ.δ.

Παρατηρήσεις 3.2.44. 1. Από την προηγούμενη πρόταση είναι φανερό ότι θα μπορούσαμε να ορίσουμε μια άλλη απεικόνιση, την οποία θα συμβολίζουμε (χωρίς κίνδυνο σύγχυσης) πάλι με σ, ως εξής:

$$\sigma : \mathcal{R}_n \simeq \mathbb{F}[x]/\langle x^n - 1\rangle \longrightarrow \mathbb{F}[x]/\langle\, \gamma(x)\,\rangle \simeq \mathbb{F}_{n-k-1}[x]$$

με $\sigma(c(x) \mod (x^n - 1)) = \sigma(c(x))$.

Οπότε $\sigma(c(x)) = 0$, αν και μόνο αν $c(x) \in \mathcal{C}$.

Όπως επίσης, αν $c(x) \in \mathcal{C}$, τότε $\sigma(c(x) + e(x)) = \sigma(e(x))$.

Δηλαδή ένα πολυώνυμο $c(x) \in \mathcal{R}_n$ ανήκει στον κώδικα, αν και μόνο αν το σύνδρομό του ισούται με μηδέν.

2. Ο ορισμός του συνδρόμου που δώσαμε εδώ είναι ο ίδιος με τον ορισμό του συνδρόμου που δώσαμε στη σελίδα 136. (ιδέ Άσκηση 3.2.5 [29])

3. Αν $e_1(x), e_2(x) \in \mathcal{R}_n$ καθένα με βάρος $w(e_i(x)) \leq t$, όπου $t = \left[\frac{d-1}{2}\right]$, τότε είναι εύκολο να δούμε ότι από τη σχέση $\sigma(e_1(x)) = \sigma(e_2(x))$ έπεται $e_1(x) = e_2(x)$.

   Πράγματι, αν $\sigma(e_1(x)) = \sigma(e_2(x))$, επειδή η σ είναι γραμμική έχουμε ότι $e_1(x) - e_2(x) \in \mathcal{C}$, αλλά, επειδή έχουμε υποθέσει ότι $w(e_i(x)) \leq t$, όπου $t = \left[\frac{d-1}{2}\right]$, το βάρος $w(e_1(x) - e_2(x))$ είναι γνήσια μικρότερο από d, την ελάχιστη απόσταση του κώδικα, άτοπο, εκτός εάν $e_1(x) = e_2(x)$.

Πρόταση 3.2.45. *Έστω $f(x) \in \mathcal{R}_n$ και $\sigma(f(x))$ το σύνδρομό του, τότε $\sigma(xf(x)) = \sigma(x\sigma(f(x)))$.*

Απόδειξη. Από τον ορισμό έχουμε ότι $\sigma(xf(x)) = xf(x) - \pi_1(x)\gamma(x)$ και $\sigma(f(x)) = f(x) - \pi_2(x)\gamma(x)$. Ο βαθμός των πολυωνύμων $\sigma(xf(x))$ και $\sigma(f(x))$ είναι μικρότερος από τον βαθμό $n-k$ του πολυωνύμου γεννήτορα $\gamma(x)$.

Πολλαπλασιάζοντας τη δεύτερη σχέση με x έχουμε ότι $x\sigma(f(x)) = xf(x) - x\pi_2(x)\gamma(x)$. Το πολυώνυμο $x\sigma(f(x))$ είναι βαθμού το πολύ $n-k$, οπότε κάνοντας τη διαίρεση με το $\gamma(x)$ έχουμε $x\sigma(f(x)) = \pi_3(x)\gamma(x) + \sigma(x\sigma(f(x)))$.

Άρα, με τη βοήθεια της πρώτης σχέσης, αντικαθιστώντας διαδοχικά έχουμε ότι

$\sigma(x\sigma(f(x))) = x\sigma(f(x)) - \pi_3(x)\gamma(x) = (xf(x) - x\pi_2(x)\gamma(x)) - \pi_3(x)\gamma(x) = [(\sigma(xf(x)) + \pi_1(x)\gamma(x)) - x\pi_2(x)\gamma(x)] - \pi_3(x)\gamma(x) = \sigma(xf(x) + (\pi_1(x) - x\pi_2(x) - \pi_3(x))\gamma(x)$. Από την τελευταία σχέση, επειδή ο βαθμός και των δύο πολυωνύμων $\sigma(x\sigma(f(x)))$ και $\sigma(xf(x)$ είναι μικρότερος του $n-k$, έπεται η ισότητα. ό.έ.δ.

Από την προηγούμενη πρόταση έπεται ότι, αν $f(x) \in \mathcal{R}_n$ και $\sigma(f(x))$ το σύνδρομό του, τότε είναι εύκολο να υπολογίσουμε το σύνδρομο κάθε πολυωνύμου $g(x) \in \mathcal{R}_n$, το οποίο προκύπτει από το $f(x)$ με κυκλική μετάθεση των συντελεστών του.

Θα δούμε τώρα πώς, εκμεταλλευόμενοι την δομή ενός κυκλικού κώδικα, μπορούμε να πραγματοποιήσουμε την αποκωδικοποίηση με την βοήθεια του συνδρόμου.

Έστω $\mathcal{C}$ ένας $[n, k, d]$ κυκλικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$ με πολυώνυμο γεννήτορα $\gamma(x)$. Έστω ότι εστάλη η (κωδικο)λέξη $c(x)$ και ότι ελήφθη η λέξη $f(x)$. Η διαφορά $e(x) = f(x) - c(x)$ είναι το λάθος που υπεισήλθε. Υποθέτουμε ότι το βάρος του $e(x)$ είναι το πολύ ίσον με $t = \left[\frac{d-1}{2}\right]$, δηλαδή έχουν παρεισφρήσει το πολύ t το πλήθος λάθη και ότι το σύνδρομο της ληφθείσης λέξης έχει βάρος το πολύ t. Υπολογίζοντας το σύνδρομο της ληφθείσης λέξης έχουμε ότι $\sigma(f(x)) = \sigma(e(x) - c(x)) = \sigma(e(x))$. Οι δύο λέξεις $\sigma(e(x))$ και $e(x)$ έχουν βάρος το πολύ ίσον με t, επομένως από την τελευταία παρατήρηση έχουμε ότι $\sigma(e(x)) = e(x)$. Δηλαδή το (άγνωστο) πολυώνυμο λάθους ισούται με το (γνωστό) σύνδρομο της ληφθείσης λέξης. Επομένως, η αποκωδικοποίηση είναι πλέον εφικτή.

Όλα αυτά βεβαίως με την προϋπόθεση ότι το σύνδρομο της ληφθείσης λέξης έχει βάρος το πολύ t. Από την άλλη πλευρά μια από τις μεγαλύτερες δυσκολίες κατά την αποκωδικοποίηση είναι το μεγάλο πλήθος των αντιπροσώπων σε μια αντιπροσωπευτική διάταξη, το οποίο είναι ίσον με $|\ \mathbb{F}\ |^{n-k}$. Τα προβλήματα αυτά μπορούν να αντιμετωπισθούν με την εξής μέθοδο/αλγόριθμο.

Βήμα 1.

Λαμβάνουμε ως αντιπροσώπους όλα τα πολυώνυμα τα οποία έχουν βάρος το πολύ ίσον με t και τα οποία έχουν συντελεστή μεγιστοβαθμίου όρου μη μηδενικό. Δηλαδή όλα τα πολυώνυμα της μορφής $e(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ με $w(e(x)) \leq t$ και $a_{n-1} \neq 0$.

Τα πολυώνυμα αυτά **δεν** αποτελούν ένα πλήρες σύστημα αντιπροσώπων του κώδικα $\mathcal{C}$ στον διανυσματικό χώρο $\mathbb{F}^n$ όλων των λέξεων, αλλά, όπως θα δούμε, είναι αρκετά για να προχωρήσει η αποκωδικοποίηση.

Κατόπιν, υπολογίζουμε τα σύνδρομά τους.

Πρέπει να παρατηρήσουμε ότι δεν υπάρχουν $e_1(x)$ και $e_2(x)$ διαφορετικά μεταξύ τους, τα οποία να έχουν ίσα σύνδρομα (ιδέ Παρατήρηση 3.2.44$_3$).

Βήμα 2.

Έστω ότι εστάλη η (κωδικο)λέξη $c(x)$ και ελήφθη η λέξη $y(x) = c(x) + e(x)$. Οπότε για τα σύνδρομα έχουμε ότι $\sigma(y(x)) = \sigma(e(x))$ (ιδέ Παρατήρηση

3.2.44$_1$).

Βήμα 3.

Αν το σύνδρομο που υπολογίσαμε στο προηγούμενο βήμα βρίσκεται στον κατάλογο που κατασκευάσαμε στο πρώτο βήμα, τότε αμέσως υπολογίζουμε το αντίστοιχο πολυώνυμο λάθους και τελειώσαμε.

Το πιο πιθανόν όμως είναι το σύνδρομο να μην βρίσκεται στον κατάλογο, διότι όπως επισημάναμε δεν έχουμε πάρει ένα πλήρες σύστημα αντιπροσώπων. Στην περίπτωση αυτή μεταβαίνουμε στο επόμενο βήμα.

Βήμα 4.

Αρχίζουμε και υπολογίζουμε τα σύνδρομα των πολυωνύμων:

$$xy(x), x^2y(x), \dots, x^iy(x), \dots$$

έως ότου το $\sigma(x^iy(x))$ να βρεθεί στον κατάλογο που έχουμε κατασκευάσει στο πρώτο βήμα. Υποθέτουμε ότι το σύνδρομο $\sigma(x^iy(x))$ αντιστοιχεί στο πολυώνυμο λάθους $e_i(x)$. Τότε προφανώς (γιατί;) το πολυώνυμο $e(x) = x^{n-i}e_i(x)$ είναι το πολυώνυμο λάθους που παρεισέφρησε στην (κωδικο)λέξη $c(x)$, οπότε αποκωδικοποιούμε ως $c(x) = y(x) - e(x)$.

Στο τελευταίο βήμα φαίνεται ότι κάνουμε χρήση της κυκλικής δομής του κώδικα.

Παρατηρήσεις 3.2.46.

1. Η παραπάνω μέθοδος είναι γνωστή ως μέθοδος αποκωδικοποίησης Meggitt (για την ακρίβεια μια από τις διάφορες παραλλαγές της) και αποτελεί ειδική περίπτωση μιας γενικότερης μεθόδου αναφερόμενης στην βιβλιογραφία ως **παγίδευση λάθους** (Error trapping).

2. Όπως έχουμε επισημάνει, για να εφαρμοσθεί η μέθοδος αυτή, απαιτείται η προϋπόθεση ότι το σύνδρομο της ληφθείσης λέξης έχει βάρος το πολύ t. Αυτό δεν συμβαίνει εν γένει, οπότε είμαστε αναγκασμένοι να χρησιμοποιήσουμε ένα πλήρες σύστημα αντιπρωσώπων με τα αντίστοιχα σύνδρομά τους. Παρόλα ταύτα, όπως θα δούμε στην επομένη πρόταση, μπορούμε σε αρκετές περιπτώσεις να εξασφαλίσουμε ότι το σύνδρομο της ληφθείσης λέξης έχει βάρος το πολύ t.

Πρόταση 3.2.47. *Έστω $\mathcal{C}$ ένας $[n, k, d]$ κυκλικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$ με πολυώνυμο γεννήτορα $\gamma(x)$. Υποθέτουμε ότι κατά την μετάδοση (κωδικο)λέξεων παρεισφρέουν το πολύ $t = \left[\frac{d-1}{2}\right]$ το πλήθος λάθη, τα οποία όμως εμφανίζονται σε εύρος $r = n - k$ το πλήθος διαδοχικών συντεταγμένων (συμπεριλαμβανομένης και της περίπτωσης όπου η λέξη θεωρείται στεφάνη και μερικά από τα λάθη εμφανίζονται σε ένα αρχικό τμήμα της λέξης και μερικά σε ένα τελικό τμήμα). Τότε υπάρχει κυκλική μετάθεση της λέξης, της οποίας το σύνδρομο έχει βάρος το πολύ ίσον με t.*

Απόδειξη. Υποθέτουμε ότι εστάλη η (κωδικο)λέξη $c(x)$ και ελήφθη η λέξη $c(x)+e(x) = y(x) = a_0+a_1x+\cdots+a_ix^i+\cdots+a_{i+r}x^{i+r}+\cdots+a_{n-1}x^{n-1}+a_nx^n$, όπου τα t το πλήθος λάθη έχουν παρεισφρήσει στο τμήμα $a_ix^i+\cdots+a_{i+r}x^{i+r}$. Εφαρμόζοντας διαδοχικές κυκλικές μεταθέσεις στην $y(x)$ λαμβάνουμε την λέξη $y_i(x) = a_ix^i + \cdots + a_{i+r}x^{i+r} + \cdots + a_{n-1}x^{n-1} + a_nx^n + a_0 + a_1x + \cdots + a_{i-1}x^{i-1}$. Οπότε εφαρμόζοντας αντίστοιχες κυκλικές μεταθέσεις στις $c(x)$ και $e(x)$ έχουμε $y_i(x) = c_i(x)+e_i(x)$ με την $c_i(x)$ να ανήκει και αυτή στον κώδικα και τα λάθη να είναι εντοπισμένα στις r πρώτες θέσεις. Δηλαδή το $e_i(x)$ έχει βάρος το πολύ t και βαθμό μικρότερο του $r = n-k = deg(\gamma(x))$. Συνεπώς, το σύνδρομο $\sigma(y_i(x)) = \sigma(e_i(x)) = e_i(x)$ έχει βάρος το πολύ ίσον με t. ό.έ.δ.

Θα κλείσουμε την παράγραφο με ένα παράδειγμα για να δούμε πώς εφαρμόζεται η παραπάνω μέθοδος.

Παράδειγμα 3.2.48. Έστω $\mathcal{C}$ ο δυαδικός κυκλικός κώδικας με παραμέτρους $[15, 7, 5]$ και πολυώνυμο γεννήτορα $\gamma(x) = 1 + x^4 + x^6 + x^7 + x^8$. Επειδή η ελάχιστη απόσταση είναι ίση με $d = 5$, έχουμε ότι ο κώδικας διορθώνει το πολύ δύο λάθη.

Βήμα 1.

Κατασκευάζουμε έναν πίνακα (σχήμα 3.1) με δύο στήλες. Στην πρώτη στήλη τοποθετούμε όλα τα πιθανά διανύσματα λάθους, βάρους το πολύ 2, και με μη μηδενικό το συντελεστή του x^{14}.

Υπολογίζουμε τα αντίστοιχα σύνδρομα και τα τοποθετούμε στη δεύτερη στήλη. Τα σύνδρομα είναι το υπόλοιπο της διαίρεσης των πολυωνύμων της

$e(x)$	$\sigma(e(x))$
x^{14}	$x^3+x^5+x^6+x^7$
$x^{13}+x^{14}$	$x^2+x^3+x^4+x^7$
$x^{12}+x^{14}$	$x+x^4+x^6+x^7$
$x^{11}+x^{14}$	$1+x^2+x^4+x^5+x^6+x^7$
$x^{10}+x^{14}$	$x+x^2+x^3$
x^9+x^{14}	$1+x+x^3+x^4+x^7$
x^8+x^{14}	$1+x^3+x^4+x^5$
x^7+x^{14}	$x^3+x^5+x^6$
x^6+x^{14}	$x^3+x^5+x^7$
x^5+x^{14}	$x^3+x^6+x^7$
x^4+x^{14}	$x^3+x^4+x^5+x^6+x^7$
x^3+x^{14}	$x^5+x^6+x^7$
x^2+x^{14}	$x^2+x^3+x^5+x^6+x^7$
$x+x^{14}$	$x+x^3+x^5+x^6+x^7$
$1+x^{14}$	$1+x^3+x^5+x^6+x^7$

Σχήμα 3.1: Πίνακας συνδρόμων πολυωνύμων

πρώτης στήλης με το πολυώνυμο γεννήτορα. Μπορούμε να αποφύγουμε τις πολλές διαιρέσεις και να συντομεύσουμε τους υπολογισμούς επικαλούμενοι τις Προτάσεις 3.2.43 και 3.2.45. Για παράδειγμα, με τη βοήθεια της σχέσης $\sigma(xf(x)) = \sigma(x\sigma(f(x)))$, υπολογίζουμε διαδοχικά όλα τα υπόλοιπα της διαίρεσης των x^i με το πολυώνυμο $\gamma(x) = 1+x^4+x^6+x^7+x^8$ και μετά για το υπόλοιπο της διαίρεσης του x^i+x^j με το $\gamma(x) = 1+x^4+x^6+x^7+x^8$ απλώς προσθέτουμε τα επιμέρους υπόλοιπα.

Βήμα 2.

Έστω ότι εστάλησαν οι (κωδικο)λέξεις $c_1(x)$, $c_2(x)$ και ελήφθησαν οι λέξεις $y_1(x) = 1+x+x^2+x^4+x^5+x^6+x^9+x^{14}$ και $y_2(x) = 1+x^4+x^7+x^9+x^{10}+x^{12}$ αντίστοιχα. Υπολογίζουμε τα αντίστοιχα σύνδρομα και βρίσκουμε $\sigma(y_1(x)) = \sigma(e_1(x)) = x^2+x^3+x^5+x^6+x^7$ και $\sigma(y_2(x)) = \sigma(e_2(x)) = x+x^2+x^3+x^4+x^5$.

Βήμα 3.

Για τα σύνδρομα που υπολογίσαμε στο προηγούμενο βήμα, στην μεν πρώτη περίπτωση παρατηρούμε ότι στο σύνδρομο $x^2 + x^3 + x^5 + x^6 + x^7$ αντιστοιχεί το λάθος $e_1(x) = x^2 + x^{14}$, οπότε αποκωδικοποιούμε ως $c_1(x) = y_1(x) - e_1(x) = 1 + x + x^4 + x^5 + x^6 + x^9$ και έχουμε τελειώσει.

Στη δεύτερη όμως περίπτωση παρατηρούμε ότι το σύνδρομό της δεν αντιστοιχεί σε κανένα (πιθανόν) λάθος από την πρώτη στήλη του πίνακα, οπότε μεταβαίνουμε στο επόμενο βήμα.

Βήμα 4.

Αρχίζουμε και υπολογίζουμε τα σύνδρομα των πολυωνύμων:

$$xy_2(x),\ x^2y_2(x),\ \ldots,\ x^iy_2(x),\ \ldots$$

έως ότου το $\sigma(x^iy(x))$ να βρεθεί στον κατάλογο που έχουμε κατασκευάσει στο πρώτο βήμα. Παρατηρούμε ότι στο $\sigma(x^2y_2(x)) = x^3 + x^4 + x^5 + x^6 + x^7$ αντιστοιχεί το πολυώνυμο λάθους $e(x) = x^4 + x^{14}$, οπότε το πολυώνυμο $e_2(x) = x^{15-2}e(x) = x^{17} + x^{27} = x^2 + x^{12} \in \mathcal{R}_n$ είναι το λάθος που παρεισέφρησε, οπότε αποκωδικοποιούμε ως $c_2(x) = y_2(x) - e_2(x) = 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$

3.2.5 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Ποίοι από τους ακόλουθους κώδικες είναι κυκλικοί; Στην περίπτωση που κάποιος είναι κυκλικός υπολογίστε το πολυώνυμο γεννήτορα και τον πίνακα ελέγχου ισοτιμίας.

   i) $\mathcal{C} = \{\, 00000,\ 10110,\ 01101,\ 11011 \,\}$.

   ii) $\mathcal{D} = \{\, \mathbf{x} \in \mathbb{Z}_3^n \mid w(\mathbf{x}) \equiv 0 \mod 3 \,\}$.

   iii) $\mathcal{E} = \{\, x_1x_2\cdots x_n \in \mathbb{Z}_3^n \mid \sum_{i=1}^{n} x_i \equiv 0 \mod 3 \,\}$.

3. Έστω $\mathcal{C}$ ο δυαδικός κυκλικός κώδικας μήκους 7 με γενήτορα πολυώνυμο $x^3 + x + 1$. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας του $\mathcal{C}$. Στον πίνακα που θα βρείτε να εφαρμόσετε μια μετάθεση στις στήλες του, έτσι ώστε ο γραμμικός κώδικας που έχει ως πίνακα ελέγχου ισοτιμίας τον

νέο πίνακα να μην είναι κυκλικός. Άρα, να συμπεράνετε ότι υπάρχουν κυκλικοί κώδικες που είναι ισοδύναμοι με μη κυκλικούς κώδικες.

4. Έστω $\mathcal{C}$ ένας γραμμικός κώδικας με γεννήτορα πίνακα G. Δείξτε ότι αρκεί από κάθε κυκλική μετάθεση των στοιχείων κάθε γραμμής του πίνακα G να προκύπτει μια (κωδικο)λέξη για να είναι ο κώδικας κυκλικός.

5. Να δείξετε ότι ο δυαδικός κυκλικός κώδικας $\mathcal{C}$ μήκους n με γεννήτορα πολυώνυμο $\gamma(x)$ είναι συμπληρωματικά αναλλοίωτος (βλέπε Πρόταση 2.1.4), αν και μόνο αν και μόνο αν το πολυώνυμο $x^{n-1}+\cdots+x^2+x+1$ διαιρείται με το $\gamma(x)$.

   Ισοδύναμα, αν και μόνο αν το $x+1$ δεν διαιρεί το $\gamma(x)$.

6. Δείξτε ότι ο δυαδικός κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο $\gamma(x)$ περιέχει την λέξη $11\cdots1$, αν και μόνο αν $\gamma(1)\neq 0$.

7. Έστω $\mathcal{C}$ ένας κυκλικός δυαδικός κώδικας περιττού μήκους. Δείξτε ότι ο $\mathcal{C}$ περιέχει μια (κωδικο)λέξη περιττού βάρους, αν και μόνο αν $11\cdots1\in\mathcal{C}$.

8. Έστω $\mathcal{C}$ ένας κυκλικός δυαδικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο $\mathcal{C}$ περιέχει τουλάχιστον μια (κωδικο)λέξη περιττού βάρους. Δείξτε ότι το υποσύνολο όλων των (κωδικο)λέξεων αρτίου βάρους αποτελεί έναν κυκλικό υποκώδικα και να υπολογίσετε το πολυώνυμο γεννήτορα.

9. Για τον επαναληπτικό κώδικα:

$$\mathcal{R}_p(k)=\{\underbrace{00\cdots0}_{k-\text{φορές}},\ \underbrace{11\cdots1}_{k-\text{φορές}},\ \ldots,\underbrace{(p-1)\,(p-1)\cdots(p-1)}_{k-\text{φορές}}\}$$

   να υπολογίσετε το πολυώνυμο γεννήτορα, έναν πίνακα ελέγχου ισοτιμίας και τον δυϊκό του κώδικα.

10. Έστω p ένας πρώτος αριθμός και n ένας θετικός ακέραιος. Υπάρχει $p-$αδικός κυκλικός κώδικας μήκους n; (Να διακρίνετε πρώτα την περίπτωση που οι p και n είναι σχετικά πρώτοι.)

11. Πόσοι τριαδικοί κυκλικοί κώδικες μήκους 8 υπάρχουν; Για καθέναν από αυτούς να βρείτε έναν πίνακα ελέγχου ισοτιμίας.

12. (α΄) Να βρεθούν όλοι οι δυαδικοί κυκλικοί κώδικες μήκους 7. Για κάθε έναν από αυτούς να βρείτε το πολυώνυμο ελέγχου και έναν αδύναμο γεννήτορα. Ποίοι απ' αυτούς είναι ελάχιστοι, ποίοι μέγιστοι; Να κάνετε ένα διάγραμμα όπου να διατάξετε όλους αυτούς τους κώδικες ως προς τη σχέση 'του περιέχεσθαι'.

    (β΄) Να βρεθούν όλα τα ζεύγη $\mathcal{C}_1$, $\mathcal{C}_2$ δυαδικών κυκλικών κωδίκων μήκους 7 με την ιδιότητα $\mathcal{C}_1 \cap \mathcal{C}_2 = \mathbf{0}$ και $\mathcal{C}_1 + \mathcal{C}_2 = \mathbb{Z}_2^7$.

    (γ΄) Να εκφράσετε κάθε δυαδικό κυκλικό κώδικα μήκους 7 ως άθροισμα ελαχίστων κωδίκων.

    (Θεωρήστε γνωστό ότι $x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$.)

13. Να βρεθούν όλοι οι κυκλικοί κώδικες μήκους 11 επί του σώματος $\mathbb{Z}_3$. Για κάθε έναν από αυτούς να βρείτε το πολυώνυμο ελέγχου και έναν αδύναμο γεννήτορα. Ποίοι απ' αυτούς είναι ελάχιστοι, ποίοι μέγιστοι; Να κάνετε ένα διάγραμμα όπου να διατάξετε όλους αυτούς τους κώδικες ως προς τη σχέση 'του περιέχεσθαι'. (Θεωρήστε γνωστό ότι $x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1)$.)

14. Έστω $\mathcal{C}$ ένας κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο $\mathcal{C}$ είναι αυτο-ορθογώνιος (δηλαδή $\mathcal{C} \subseteq \mathcal{C}^\perp$). Δείξτε ότι το $x - 1$ διαιρεί το $\gamma(x)$.

15. Δείξτε ότι ένας αυτο-ορθογώνιος κυκλικός κώδικας είναι κώδικας μηδενικού αθροίσματος.

16. Δείξτε ότι ο κυκλικός κώδικας $\mathcal{C}$ με γεννήτορα πολυώνυμο $\gamma(x)$ και πολυώνυμο ελέγχου $\delta(x)$ είναι αυτο-ορθογώνιος, αν και μόνο αν το αμοιβαίο πολυώνυμο του $\delta(x)$ διαιρεί το $\gamma(x)$.

17. Έστω $\mathcal{C}$ ένας κυκλικός μήκους n κώδικας με γεννήτορα πολυώνυμο $\gamma(x)$. Υποθέτουμε ότι ο δυϊκός κώδικας $\mathcal{C}^\perp$ έχει γεννήτορα πολυώνυμο το πο-

λυώνυμο $d(x)$. Αν $x^n - 1 = \gamma(x) \cdot \sigma(x)$, δείξτε ότι για κάθε ρίζα ξ του πολυωνύμου $d(x)$ το ξ^{-1} είναι ρίζα του $\sigma(x)$.

18. Ένας κώδικας λέγεται **αναστρέψιμος**, αν για κάθε (κωδικο)λέξη $\mathbf{c} = c_0c_1 \cdots c_{n-1}$ έπεται ότι και η λέξη $c_{n-1}c_{n-2} \cdots c_0$ είναι στοιχείο του κώδικα. Δείξτε ότι ένας κυκλικός κώδικας $\mathcal{C}$ με πολυώνυμο γεννήτορα $\gamma(x)$ είναι αναστρέψιμος, αν και μόνο αν για κάθε ρίζα ξ του πολυωνύμου $\gamma(x)$ έπεται ότι και η ξ^{-1} είναι ρίζα του $\gamma(x)$.

19. Να δώσετε ικανή και αναγκαία συνθήκη, ώστε ένας κυκλικός κώδικας να είναι κώδικας μέγιστης απόστασης.

20. Δείξτε ότι ο κυκλικός κώδικας $\mathcal{C}$ είναι κώδικας μέγιστης απόστασης, αν και μόνο αν το κυκλικό συμπλήρωμά του $\overline{\mathcal{C}}$ είναι κώδικας μέγιστης απόστασης. (Για τον ορισμό του κυκλικού συμπληρώματος ιδέ την Παρατήρηση 3.2.20.)

21. Έστω $\mathcal{C}$ ένας κυκλικός κώδικας και $\overline{\mathcal{C}}$ το κυκλικό συμπλήρωμά του. Δείξτε ότι $\mathcal{C}^{\perp} = \varrho_{-1}(\overline{\mathcal{C}})$.

22. Έστω $\mathcal{C}$ ένας κυκλικός κώδικας με πολυώνυμο γεννήτορα $\gamma(x)$. Τί συνθήκες πρέπει να πληροί το πολυώνυμο $\gamma(x)$, ώστε ο δυϊκός κώδικας $\mathcal{C}^{\perp}$ να ισούται με το κυκλικό συμπλήρωμα $\overline{\mathcal{C}}$;

23. Έστω $\mathcal{C}$ ο δυαδικός επαναληπτικός κώδικας μήκους 7. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας του με δύο τρόπους.

    Μια φορά θεωρώντας το πολυώνυμο ελέγχου ισοτιμίας και μια θεωρώντας την επέκταση $\mathbb{E} = \mathbb{Z}_2(a)$, όπου a είναι ρίζα του πολυωνύμου x^3+x+1, και κατασκευάζοντας έναν κώδικα $\mathcal{D}$ επί του $\mathbb{E}$, ώστε $\mathcal{C} = \mathcal{D}_{\mathbb{Z}_2}$.

24. Έστω $\mathcal{C}$ ένας κυκλικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$ με πολυώνυμο γεννήτορα $\gamma(x)$. Δείξτε ότι το υποσύνολο $\mathcal{C}_0$, το οποίο αποτελείται από όλες τις (κωδικο)λέξεις μηδενικού αθροίσματος είναι κυκλικός κώδικας.

    Στην περίπτωση, όπου ο $\mathcal{C}_0$ είναι γνήσιο υποσύνολο του $\mathcal{C}$, δείξτε ότι του πολυώνυμο $(x-1)\gamma(x)$ είναι το πολυώνυμο γεννήτορας κώδικα $\mathcal{C}_0$.

Επίσης, δείξτε ότι $\mathcal{C}_0 = \mathcal{C}$, αν και μόνο αν $\gamma(1) = 0$. (Παραβάλατε με το Θεώρημα 3.2.21.)

25. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας φυσικός αριθμός πρώτος προς τον q. Ως συνήθως, συμβολίζουμε με $\mathcal{R}_n$ τον δακτύλιο πηλίκων $\mathbb{F}[x]/\langle x^n - 1\rangle$. Έστω $x^n - 1 = (x-1)\varphi(x)$, όπου $\varphi(x) = x^{n-1} + x^{n-2} + \cdots x + 1$. Αν $\vartheta(x) = (1/n)\varphi(x)$, δείξτε ότι:

    (i) $(\varphi(x))^2 = n\varphi(x)$ ως στοιχεία του δακτυλίου $\mathcal{R}_n$.

    (ii) Το $\vartheta(x)$ είναι αδύναμο στοιχείο του δακτυλίου $\mathcal{R}_n$.

    (iii) Το $\vartheta(x)$ είναι ο αδύναμος γεννήτορας του επαναληπτικού κώδικα μήκους n επί του σώματος $\mathbb{F}$.

    (iv) Το $1 - \vartheta(x)$ είναι ο αδύναμος γεννήτορας του κυκλικού κώδικα $\mathcal{E}_n$, του οποίου τα στοιχεία είναι όλες οι λέξεις με μηδενικό άθροισμα χαρακτήρων.

26. Έστω $\mathcal{C}$ ένας κυκλικός κώδικας επί του πεπερασμένου σώματος $\mathbb{F}$ με αδύναμο γεννήτορα $\epsilon(x)$ και $\mathcal{C}_0$ ο υποκώδικας, ο οποίος αποτελείται από όλες τις (κωδικο)λέξεις μηδενικού αθροίσματος.

    Στην περίπτωση, όπου ο $\mathcal{C}_0$ είναι γνήσιο υποσύνολο του $\mathcal{C}$, δείξτε ότι του πολυώνυμο $\epsilon(x) - \vartheta(x)$ είναι ένας αδύναμος γεννήτορας κώδικα $\mathcal{C}_0$.

27. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας φυσικός αριθμός πρώτος προς τον q. Δείξτε ότι κάθε ελάχιστος κώδικας $\mathcal{D}$ μήκους n περιέχει ένα μόνο μη μηδενικό αδύναμο στοιχείο.

28. Έστω ο δυαδικός κυκλικός κώδικας $\mathcal{C}$ μήκους δεκαπέντε με γεννήτορα πολυώνυμο $\gamma(x) = (x^2+x+1)(x^4+x^3+x^2+x+1)$. Να κωδικοποιήσετε το μήνυμα $\mathbf{a} = 101101001$ με συστηματική κωδικοποίηση με τη βοήθεια ενός πίνακα ελέγχου ισοτιμίας του κώδικα. (Θεωρήστε γνωστή την ανάλυση $x^{15}-1 = (x+1)(x^2+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$.)

29. Έστω $\mathcal{C}$ ο κυκλικός κώδικας, επί του πεπερασμένου σώματος $\mathbb{F}$, με πολυώνυμο γεννήτορα $\gamma(x)$ και P ένας πίνακας ελέγχου ισοτιμίας. Να δείξετε ότι για το στοιχείο $c(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R}_n$ ισχύει

$\sigma(c(x)) = (a_0\, a_1 \cdots a_{n-1})\mathrm{P}^t$, δηλαδή ο ορισμός του συνδρόμου που δώσαμε εδώ (Ορισμός 3.2.42) είναι ο ίδιος με τον ορισμό του συνδρόμου που δώσαμε στη σελίδα 136.

30. Στο Παράδειγμα 3.2.48 Να κάνετε τον έλεγχο των πράξεων.

Βιβλιογραφία

Berlekamp, E. R. *"Algebraic Coding Theory"*. Laguna Hills, CA: Aegean Park Press, 1984.

Hall, J.I. *Notes on Coding Theory*. (σε ηλεκτρονική μορφή). www.math.msu.edu/~jhall.

Hamming, R. *"Coding and Information Theory"*. Prentice-Hall, Englewood Cliffs 2^{nd} Edition, 1986.

Herstein, I. N. *"Abstract Algebra"*. New York: Macmillan, 1990.

Hill, R. *"A First Course in Coding Theory"*. Oxford University Press, Oxford, 1986.

Huffman, C. W. and Pless, V. . *"Fundamentals of Error-Correcting Codes"*. Cambridge University Press, 2003.

Justesen, J. and Hoholdt, T. *"A Course In Error-Correcting Codes"*. European Mathematical Society, 2004.

Lidl, R. and Niederreiter H. . *"Introduction to finite fields and their applications"*. Cambridge University Prees, 2000.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*. Wiley, New York, 1998.

Pretzel, O. *"Error-Correcting Codes and Finite Fields"*. Oxford University Press, Oxford, 1992.

Roman, S. *"Coding and Information Theory"*. Springer-Verlag, 1992.

van Lint, J.H. *"Introduction to Coding Theory"*. Springer-Verlag, 1999.

Walker, J. L. *"Codes and Curves"*, volume 7 of *Student Mathematical Library*. AMS, 2000.

Σ. Ανδρεαδάκης. *Θεωρία Galois*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1992.

Σ. Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1993.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

ΚΕΦΑΛΑΙΟ 4

"Ενδιαφέροντες" Κώδικες

Πολλές φορές προηγουμένως, αναφερθήκαμε στις ιδιότητες που έχει ένας κώδικας, π.χ. ως προς την αποτελεσματικότητά του να ανιχνεύει ή (και) να διορθώνει λάθη, ως προς το πλήθος των πληροφοριών που μπορεί να μεταδοθούν μέσω του κώδικα, ως προς την ευκολία που πραγματοποιείται η κωδικοποίηση και η αποκωδικοποίηση κ.λ.π. Τα κριτήρια επιλογής ενός κώδικα ποικίλλουν από περίπτωση σε περίπτωση και εξαρτώνται τόσο από τη φύση του προς κωδικοποίηση μηνύματος, όσο και από τα διαθέσιμα μέσα για αποθήκευση/αποστολή του μηνύματος. Επιπλέον, ο χαρακτηρισμός ενός κώδικα ως "ενδιαφέροντος" εμπεριέχει και υποκειμενικά κριτήρια και μάλλον θα ήταν προτιμότερο να αναφέρονται ως "βολικοί" κώδικες.

Στις επόμενες παραγράφους θα αναφερθούμε σε ορισμένες κατηγορίες κωδίκων οι οποίοι είναι γραμμικοί. Ο τρόπος που ορίζονται είναι τέτοιος ώστε να μας εξαφαλίζει έναν αποτελεσματικό τρόπο χειρισμού των. Από ιστορικής πλευράς είναι κώδικες οι οποίοι έχουν επινοηθεί και χρησιμοποιηθεί με επιτυχία σε πολλές περιπτώσεις. Μάλιστα, οι περισσότεροι εξακολουθούν να χρησιμοποιούνται μέχρι σήμερα.

4.1 Κώδικες Hamming

Οι κώδικες Hamming είναι από τους πλέον γνωστούς κώδικες που χρησιμοποιούνται. Το πλεονέκτημά τους (αν και δεν μπορούν να διορθώσουν μεγάλο αριθμό λαθών) έγκειται στο γεγονός ότι η αποκωδικοποίηση είναι εύκολη και επιτυγχάνεται με ιδιαίτερα κομψό τρόπο.

Επινοήθηκαν, ανεξάρτητα, από τους Marcel Golay το 1949 και Richard Hamming το 1950 και λόγω των πλεονεκτημάτων τους εξακολουθούν και σήμερα να είναι σε χρήση.

Συμφωνα με την Πρόταση 2.2.25 η ελάχιστη απόσταση ενός $[n,\, k]$ γραμμικού κώδικα, με πίνακα ελέγχου ισοτιμίας H, είναι ο μικρότερος θετικός ακέραιος d για τον οποίο υπάρχουν d το πλήθος γραμμικά εξαρτημένες στήλες στον πίνακα H. Η πιο απλή, ενδιαφέρουσα περίπτωση είναι να μην υπάρχουν δύο γραμμικά εξαρτημένες στήλες, δηλαδή καμία στήλη να μην είναι πολλαπλάσιο κάποιας άλλης. Επομένως, εάν θέλουμε να κατασκευάσουμε έναν $[n,\, k,\, 3]$ γραμμικό κώδικα, πρέπει και αρκεί να κατασκευάσουμε έναν $(n-k)\times n$ πίνακα του οποίου ανά δύο οι στήλες να είναι γραμμικά ανεξάρτητες, αλλά να υπάρχει (τουλάχιστον) ένα σύνολο τριών γραμμικά εξαρτημένων στηλών. Ο πίνακας αυτός θα είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα.

Η διαδικασία κατασκευής ενός τέτοιου πίνακα είναι απλή, μάλιστα δε μπορούμε να κατασκευάσουμε τέτοιους πίνακες με το μεγαλύτερο δυνατό πλήθος στηλών.

Έστω r ένας θετικός ακέραιος διάφορος του 1, $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^m$ το πλήθος στοιχεία, το οποίο θα είναι το αλφάβητο και $V_1 = \mathbb{F}^r$. Επιλέγουμε ένα μη μηδενικό διάνυσμα $\mathbf{c_1} \in V_1$ και θέτουμε $V_2 = V_1 \setminus \{\, \lambda \mathbf{c_1} \mid \lambda \in \mathbb{F},\, \lambda \neq 0 \,\}$. Τώρα επιλέγουμε ένα μη μηδενικό διάνυσμα $\mathbf{c_2} \in V_2$ και θέτουμε $V_3 = V_2 \setminus \{\, \lambda \mathbf{c_2} \mid \lambda \in \mathbb{F},\, \lambda \neq 0 \,\}$. Η διαδικασία αυτή συνεχίζεται έως ότου εξαντληθούν όλα τα μη μηδενικά στοιχεία του $\mathbb{F}^r$. Ας υπολογίσουμε όλα τα στοιχεία του $\mathbb{F}^r$, τα οποία μπορούν να επιλεγούν με αυτή τη διαδικασία. Τα μη μηδενικά στοιχεία του σώματος είναι $q-1$, επομένως σε κάθε βήμα εξαιρούμε $|\, \{\, \lambda \mathbf{c_i} \mid \lambda \in \mathbb{F},\, \lambda \neq 0 \,\} \,| = q-1$ στοιχεία, Το σύνολο $\mathbb{F}^r$ έχει q^r-1 μη μηδενικά στοιχεία. Επομένως, τελικά, μπορούμε να επιλέξουμε $(q^r-1)/(q-1)$

το πλήθος στοιχεία με αυτή τη διαδικασία.

Με άλλα λόγια διαμερίζουμε το σύνολο $\mathbb{F}^r \setminus \{0\}$ σε κλάσεις, όπου κάθε κλάση περιέχει όλα τα μη μηδενικά πολλαπλάσια ενός μη μηδενικού διανύσματος [υπάρχουν $(q^r-1)/(q-1)$ το πλήθος τέτοιες κλάσεις] και από κάθε κλάση επιλέγουμε ένα διάνυσμα.

Κατασκευάζουμε έναν $r \times n$ πίνακα H, όπου $n = (q^r-1)/(q-1)$, του οποίου οι στήλες είναι τα διανύσματα που επιλέξαμε.

Από το Πόρισμα 2.2.14 έπεται ότι υπάρχει μοναδικός γραμμικός κώδικας με πίνακα ελέγχου ισοτιμίας τον πίνακα H, ο οποίος, από τον τρόπο κατασκευής του, έχει ελάχιστη απόσταση ίση με 3 και διάσταση ίση με $k = ((q^r-1)/(q-1)) - r$.

Ορισμός 4.1.1. *Ο γραμμικός κώδικας με παραμέτρους* $[n = (q^r-1)/(q-1), k = ((q^r-1)/(q-1))-r = n-r, 3]$, *που κατασκευάσαμε με την παραπάνω διαδικασία, ονομάζεται* $q-$*αδικός κώδικας* ***Hamming*** *και συμβολίζεται με* $\mathcal{H}(r, q)$. *Ο πίνακας ελέγχου ισοτιμίας* H *ονομάζεται πίνακας* ***Hamming***.

Παραδείγματα 4.1.2. 1. Ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

είναι ένας πίνακας ελέγχου ισοτιμίας για έναν $\mathcal{H}(2, 2)$ κώδικα. Οπότε ο γεννήτορας πίνακας είναι ο $\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$. Δηλαδή ο κώδικας $\mathcal{H}(2, 2)$ είναι ο επαναληπτικός κώδικας $\{000, 111\}$.

2. Ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

είναι ένας πίνακας ελέγχου ισοτιμίας για έναν $\mathcal{H}(3, 2)$ κώδικα.

3. Ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

είναι ένας πίνακας ελέγχου ισοτιμίας για έναν $\mathcal{H}(2,\,11)$ κώδικα.

Ο κώδικας που μελετήσαμε στο Παράδειγμα 2.2.26 προέρχεται από διπλή σύμπτυξη του κώδικα $\mathcal{H}(2,\,11)$, αφού ο πίνακας ελέγχου ισοτιμίας του προέρχεται από τον παραπάνω πίνακα H διαγράφοντας τις δύο πρώτες στήλες.

4. Ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

είναι ένας πίνακας ελέγχου ισοτιμίας για έναν $\mathcal{H}(3,\,3)$ κώδικα.

Θεώρημα 4.1.3. *Ένας $\mathcal{H}(r,\,q)$ κώδικας είναι τέλειος και διορθώνει μόνο ένα λάθος.*

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια της Πρότασης 1.5.12 και για τον λόγο αυτό αφίεται ως άσκηση. ό.έ.δ.

Παρατηρήσεις 4.1.4. 1. Ο τρόπος κατασκευής ενός κώδικα Hamming δίνει πολλές δυνατότητες για την επιλογή των διανυσμάτων που θα αποτελέσουν τις στήλες του πίνακα ελέγχου ισοτιμίας, επομένως μπορούμε να κατασκευάσουμε πολλούς $\mathcal{H}(r,\,q)$ κώδικες, οι οποίοι όμως είναι ισοδύναμοι. Όπως έχουμε επισημάνει ισοδύναμοι κώδικες ταυτίζονται, για τον λόγο αυτό στα επόμενα θα λέμε ο $\mathcal{H}(r,\,q)$ κώδικας.

Ένας εύκολος τρόπος κατασκευής ενός πίνακα ελέγχου ισοτιμίας για έναν $\mathcal{H}(r,\,q)$ κώδικα είναι ο ακόλουθος.

Ως στήλες λαμβάνουμε κατά (αύξουσα) σειρά όλους τους αριθμούς που έχουν r το πλήθος ψηφία, όταν γραφούν σε $q-$αδική μορφή, των οποίων το πρώτο μη μηδενικό ψηφίο είναι ίσο με 1 (μεταξύ των πολλαπλασίων ενός μη μηδενικού διανύσματος υπάρχει μόνο ένα, του οποίου η πρώτη μη μηδενική συντεταγμένη ισούται με 1). Σε όλα τα προηγούμενα παραδείγματα, εκτός του πρώτου, οι πίνακες ελέγχου ισοτιμίας έχουν κατασκευασθεί με αυτόν τον τρόπο.

2. Σε έναν πίνακα ελέγχου ισοτιμίας που κατασκευάζεται σύμφωνα με τον προηγούμενο τρόπο, υπάρχουν r το πλήθος διαφορετικές στήλες των οποίων τα στοιχεία είναι όλα 0 εκτός ενός το οποίο είναι το 1 (γιατί;). Επομένως, μπορούμε να πάρουμε έναν ισοδύναμο κώδικα με πίνακα ελέγχου ισοτιμίας της μορφής $\mathrm{H} = [B\, I_r]$. Σύμφωνα με το Θεώρημα 2.2.17 ένας γεννήτορας πίνακας του κώδικα είναι ο $\mathrm{G} = [I_{n-r} \; -B^t]$, όπου $n = (q^r - 1)/(q - 1)$. Στην περίπτωση αυτή έχουμε έναν συστηματικό κώδικα (βλέπε σελίδα 80) με όλα τα πλεονεκτήματα αποκωδικοποίησης.

   Στο προηγούμενο Παράδειγμα 2 ένας ισοδύναμος πίνακας του πίνακα H είναι ο πίνακας:

$$\overline{\mathrm{H}} = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

   (ιδέ Άσκηση 3 στο τέλος της παραγράφου). Οπότε έχουμε τον συστηματικό $\mathcal{H}(3,\, 2)$ κώδικα Hamming με γεννήτορα πίνακα:

$$\overline{\mathrm{G}} = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right).$$

   Ο κώδικας αυτός δεν είναι κώδικας μέγιστης απόστασης (ιδέ Θεώρημα 2.6.6). Επομένως και ο δυϊκός του δεν είναι κώδικας μέγιστης απόστασης.

3. Οι πλέον συνηθισμένοι κώδικες Hamming είναι οι δυαδικοί. Εδώ οι στήλες ενός πίνακα ελέγχου ισοτιμίας είναι οι ακέραιοι από το 1 έως το $2^r - 1$ εκφρασμένοι σε δυαδική μορφή.

4. Από τον τρόπο ορισμού οι κώδικες Hamming είναι γραμμικοί. Υπάρχουν όμως και μη γραμμικοί κώδικες, οι οποίοι έχουν τις ίδιες παραμέτρους με έναν κώδικα Hamming.

Έστω ο κώδικας $\mathcal{H}(r, 2)$ και $\vartheta : \mathcal{H}(r, 2) \longrightarrow \mathbb{Z}_2$ μια μη γραμμική απεικόνιση με $\vartheta(0) = 0$. Επομένως, υπάρχουν $\mathbf{c}, \mathbf{d} \in \mathcal{H}(r, 2)$, έτσι ώστε $\vartheta(\mathbf{c} + \mathbf{d}) \neq \vartheta(\mathbf{c}) + \vartheta(\mathbf{d})$. Για $\mathbf{x} \in \mathbb{Z}_2^n$ ορίζουμε $\pi(\mathbf{x}) = 0$, αν το $\mathbf{x}$ έχει άρτιο βάρος και $\pi(\mathbf{x}) = 1$, αν το $\mathbf{x}$ έχει περιττό βάρος.

Θεωρούμε τον κώδικα:

$$\mathcal{D} = \{ (\mathbf{x}\,(\mathbf{x} + \mathbf{c})\,(\pi(\mathbf{x}) + \vartheta(\mathbf{c}))) \mid \mathbf{x} \in \mathbb{Z}_2^n,\ \mathbf{c} \in \mathcal{H}(r, 2) \}$$

με $n = 2^r - 1$. Το μήκος του κώδικα $\mathcal{D}$ προφανώς είναι ίσο με $n+n+1 = 2^{r+1}-1$. Το μέγεθός του είναι ίσο με $2^{2n+1-(r+1)}$ (γιατί;) και η απόστασή του ίση με τρία. Επομένως, έχουμε έναν κώδικα με παραμέτρους όπως οι παράμετροι ενός κώδικα Hamming, ο οποίος προφανώς δεν είναι γραμμικός.

5. Από το προηγούμενο Θεώρημα έπεται άμεσα ότι για $n = (q^r - 1)/(q-1)$ ισχύει ότι $A_q(n, 3) = q^{n-r}$, δηλαδή έχουμε απαντήσει στο πρόβλημα του προσδιορισμού του $A_q(n, 3)$ (βλέπε Παράγραφο 1.5.2) για άπειρες τιμές του n (αλλά της παραπάνω μορφής).

4.1.1 Αποκωδικοποίηση με κώδικες Hamming

Στη δεύτερη από τις προηγούμενες παρατηρήσεις είδαμε ότι ένας κώδικας Hamming είναι ισοδύναμος με έναν συστηματικό κώδικα. Αν όμως έχουμε έναν πίνακα ελέγχου ισοτιμίας στη μορφή που περιγράφεται στην πρώτη παρατήρηση, τότε η αποκωδικοποίηση γίνεται ευκολότερα επιτυγχάνοντας όχι μόνο τη διόρθωση ενός λάθους, αλλά εντοπίζοντας και τη θέση στην οποία επήλθε η αλλοίωση του χαρακτήρα.

Έστω ότι έχουμε τον κώδικα $\mathcal{H}(r, q)$ με πίνακα ελέγχου ισοτιμίας H, στη μορφή που περιγράφεται παραπάνω, και ότι κατά την μετάδοση υπεισήλθε το διάνυσμα λάθους $(0, 0, \ldots, a, \ldots, 0)$, όπου το a βρίσκεται στην i θέση. Το σύνδρομό του (βλέπε Παράγραφο 2.4.4) είναι ίσο με $(0, 0, \ldots, a, \ldots, 0) \cdot \mathrm{H}^{\perp}$, δηλαδή η i στήλη του πίνακα H πολλαπλασιασμένη με a. Από τον τρόπο κατασκευής του πίνακα το a είναι το πρώτο μη μηδενικό ψηφίο του συνδρόμου. Επιπλέον, πολλαπλασιάζοντας το σύνδρομο με a^{-1} μπορούμε να εντοπίσουμε τη θέση του λάθους.

Για παράδειγμα, ας πάρουμε τον πίνακα ελέγχου ισοτιμίας:

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

για τον κώδικα $\mathcal{H}(3,\,3)$. Υποθέτουμε ότι λάβαμε τη λέξη $\mathbf{x} = 1101112211201$. Το σύνδρομό της είναι το:

$$(1101112211201) \cdot \mathrm{H}^{\perp} = (201) = 2(102).$$

Η στήλη $(1\,0\,2)^t$ είναι η εβδόμη στήλη του πίνακα Η, επομένως αφαιρώντας το λάθος 2 από την εβδόμη θέση της λέξης $\mathbf{x}$, έχουμε την (κωδικο)λέξη $\mathbf{c} = 1\,1\,0\,1\,1\,1\,0\,2\,1\,1\,2\,0\,1$ που εστάλη.

Στην περίπτωση όπου ο κώδικας είναι δυαδικός, η όλη διαδικασία είναι ευκολότερη, καθότι αν ένα λάθος έχει υπεισέλθει στην i θέση, τότε η i στήλη του πίνακα ελέγχου ισοτιμίας είναι το σύνδρομο της λέξης που ελήφθη. Επιπλέον δε, η στήλη i δεν είναι τίποτε άλλο παρά ο αριθμός i εκφρασμένος σε δυαδική μορφή. Οπότε, κατευθείαν από το σύνδρομο μιας λέξης που λάβαμε έχουμε τη θέση του λάθους που υπεισήλθε.

4.1.2 Ο δυϊκός ενός κώδικα Hamming

Ο δυϊκός κώδικας $\mathcal{H}(r,\,q)^{\perp}$ ενός κώδικα Hamming $\mathcal{H}(r,\,q)$ έχει παραμέτρους $[n = (q^r - 1)/(q - 1),\, r,\, d]$. Σε αντίθεση με τον κώδικα $\mathcal{H}(r,\,q)$, όπως θα δούμε, ο δυϊκός κώδικας έχει συγκριτικά μεγάλη ελάχιστη απόσταση.

Ας εξετάσουμε πρώτα την περίπτωση που ο κώδικας είναι δυαδικός.

Έστω $\mathcal{H}(r,\,2)$ ο δυαδικός κώδικας Hamming με παραμέτρους $[2^r - 1,\, 2^r - 1 - r,\, 3]$. Ένας πίνακας Hamming H_r αποτελεί τον πίνακα ελέγχου ισοτιμίας του. Επομένως, επειδή οι γραμμές του είναι γραμμικά ανεξάρτητες, αποτελεί έναν γεννήτορα πίνακα του δυϊκού κώδικα $\mathcal{H}(r,\,2)^{\perp}$. Ο κώδικας $\mathcal{H}(r,\,2)^{\perp}$ έχει μήκος ίσο με $2^r - 1$ και διάσταση ίση με r. Πριν υπολογίσουμε την ελάχιστη απόσταση του $\mathcal{H}(r,\,2)^{\perp}$, θα δούμε πώς υπολογίζουμε επαγωγικά τους πίνακες H_r για $r \geq 1$.

Πρόταση 4.1.5. *Ο πίνακας* H_1 *είναι ο* 1×1 *πίνακας 1 και για* $r \geq 1$ *ισχύει:*

$$\mathrm{H}_{r+1} = \left(\begin{array}{ccc|c|ccc} 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline & & & 0 & & & \\ & \mathrm{H}_r & & \vdots & & \mathrm{H}_r & \\ & & & 0 & & & \end{array}\right).$$

Απόδειξη. Η απόδειξη είναι απλή αρκεί να δούμε τον τρόπο κατασκευής των πινάκων Hamming που αναφέρουμε στην Παρατήρηση $4.1.4_1$. ό.έ.δ.

Αυτός ο τρόπος κατασκευής των πινάκων μας επιτρέπει να περιγράψουμε (επαγωγικά) τα στοιχεία του κώδικα $\mathcal{H}(r+1,\,2)^{\perp}$ με τη βοήθεια των στοιχείων του $\mathcal{H}(r,\,2)^{\perp}$.

Ως γνωστόν, $\mathcal{H}(r+1,\,2)^{\perp} = \{\,\mathbf{c}\cdot\mathrm{H}_{r+1} \mid \mathbf{r} \in \mathbb{Z}_2^{r+1}\,\}$. Αν δούμε το στοιχείο $\mathbf{r} \in \mathbb{Z}_2^{r+1}$ ως $a\mathbf{s}$ με $a = 0,\,1$ και $\mathbf{s} \in \mathbb{Z}_2^{r}$, τότε από τη μορφή του πίνακα H_{r+1} έχουμε ότι $\mathbf{r}\cdot\mathrm{H}_{r+1} = (a\mathbf{s})\cdot\mathrm{H}_{r+1} = (\mathbf{s}\cdot\mathrm{H}_r)\,a\,(a\mathbf{1}+\mathbf{s}\cdot\mathrm{H}_r)$. Από την τελευταία σχέση βλέπουμε ότι το τυχαίο στοιχείο $\mathbf{c} \in \mathcal{H}(r+1,\,2)^{\perp}$ γράφεται στη μορφή $\mathbf{d}a(a\mathbf{1}+\mathbf{d})$ με $\mathbf{d} \in \mathcal{H}(r,\,2)^{\perp}$ και $a = 0$ ή 1.

Στην πραγματικότητα έχουμε αποδείξει την επόμενη πρόταση.

Πρόταση 4.1.6. *Για τον κώδικα* $\mathcal{H}(r,\,2)^{\perp}$ *ισχύει:*

1. $\mathcal{H}(1,\,2)^{\perp} = \mathbb{Z}_2$.
2. *Για* $r \geq 1$ $\mathcal{H}(r+1,\,2)^{\perp} = \{\,\mathbf{d}0\mathbf{d}$ *με* $\mathbf{d} \in \mathcal{H}(r,\,2)^{\perp}\,\} \cup \{\,\mathbf{d}1\mathbf{d}^{c}$ *με* $\mathbf{d} \in \mathcal{H}(r,\,2)^{\perp}\,\}$.
3. *Η ελάχιστη απόσταση του* $\mathcal{H}(r,\,2)^{\perp}$ *είναι ίση με* 2^{r-1}. *Επιπλέον, η απόσταση μεταξύ δύο (οποιωνδήποτε) στοιχείων του* $\mathcal{H}(r,\,2)^{\perp}$ *είναι ίση με* 2^{r-1}.

Απόδειξη. Το μεγαλύτερο μέρος της απόδειξης έχει προηγηθεί. Όσον αφορά την απόσταση μεταξύ δύο (κωδικο)λέξεων μπορούμε επαγωγικά να την υπολογίσουμε αν παρατηρήσουμε τη μορφή των στοιχείων του κώδικα $\mathcal{H}(r,\,2)^{\perp}$. ό.έ.δ.

Στην γενική περίπτωση όπου έχουμε έναν Hamming κώδικα $\mathcal{H}(r,\, q)$, αν και δεν είναι εύκολο να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας του κώδικα $\mathcal{H}(r{+}1,\, q)$ από έναν πίνακα ελέγχου ισοτιμίας του $\mathcal{H}(r,\, q)$, μπορούμε πάλι να αποδείξουμε ότι η ελάχιστη απόσταση του δυϊκού του είναι ίση με q^{r-1}.

Πρόταση 4.1.7. *Το βάρος κάθε (κωδικο)λέξης του δυϊκού κώδικα $\mathcal{H}(r,\, q)^{\perp}$ είναι ίσον με q^{r-1}.*

Απόδειξη. Στην αρχή της παραγράφου (ιδέ σελίδα 222) είχαμε περιγράψει πώς κατασκευάζουμε έναν πίνακα H ελέγχου ισοτιμίας του κώδικα $\mathcal{H}(r,\, q)$. Συγκεκριμένα, κάθε στήλη του πίνακα H είναι ένα μη μηδενικό διάνυσμα, το οποίο έχει επιλεγεί από κάθε (διαφορετικό) μονοδιάστατο υπόχωρο του $\mathbb{F}^r$. Ο $r \times n$ πίνακας H είναι ένας γεννήτορας πίνακας του δυϊκού κώδικα $\mathcal{H}(r,\, q)^{\perp}$. Δηλαδή $\mathcal{H}(r,\, q)^{\perp} = \{\, \mathbf{x} \cdot \mathrm{H} \mid \mathbf{x} \in \mathbb{F}^r \,\}$.

Το στοιχείο $\mathbf{x} \cdot \mathrm{H}$ έχει μηδενική μία συντεταγμένη του, αν η αντίστοιχη στήλη $\mathbf{y}^t$ του πίνακα H έχει την ιδιότητα $\mathbf{x} \cdot \mathbf{y}^t = \mathbf{0}$. Το σύνολο όμως των ορθογωνίων, προς το $\mathbf{x}$, διανυσμάτων του $\mathbb{F}^r$ αποτελεί έναν υπόχωρο του $\mathbb{F}^r$ διάστασης ίσης με $r-1$. Δηλαδή υπάρχουν $(q^{r-1}-1)/(q-1)$ το πλήθος στήλες του πίνακα H με την ιδιότητα $\mathbf{x} \cdot \mathbf{y}^t = \mathbf{0}$. Συνεπώς το πλήθος των μη μηδενικών χαρακτήρων στην (κωδικο)λέξη $\mathbf{x} \cdot \mathrm{H}$ (δηλαδή το βάρος της) ισούται με $w(\mathbf{x} \cdot \mathrm{H}) = (q^r-1)/(q-1) - (q^{r-1}-1)/(q-1) = q^{r-1}$. ό.έ.δ.

Παρατηρήσεις 4.1.8.

1. Στην προηγούμενη πρόταση αποδείξαμε ότι όλες οι μη μηδενικές (κωδικο)λέξεις του δυϊκού κώδικα $\mathcal{H}(r,\, q)^{\perp}$ είναι ισοβαρείς. Αυτό συνεπάγεται ότι όλες οι (κωδικο)λέξεις, ανά δύο, ισαπέχουν. Για τον λόγο αυτό, έχει επικρατήσει οι κώδικες αυτοί να ονομάζονται κώδικες **Simplex** και να συμβολίζονται με $\mathcal{S}(r,\, q) =: \mathcal{H}(r,\, q)^{\perp}$, καθότι μπορούμε να φαντασθούμε ότι τα στοιχεία τους καταλαμβάνουν τις κορυφές ενός (πολυδιάστατου) simplex. Στην περίπτωση όπου $r = 2$, είναι εύκολο να δούμε τα στοιχεία του $\mathcal{S}(2,\, 2)$ ως τις κορυφές ενός κανονικού τετραέδρου.

2. Η ελάχιστη απόσταση του κώδικα $\mathcal{H}(r,\, q)$ είναι ίση με τρία, ενώ το μέγεθος του είναι πολύ μεγάλο. Επομένως, το επιτρεπόμενο μέγεθος

της μεταδιδόμενης πληροφορίας είναι μεγάλο σε αντίθεση με το πλήθος των λαθών τα οποία μπορούν να διορθωθούν.

Από την άλλη πλευρά ο δυϊκός κώδικας $\mathcal{S}(r,\, q)$ έχει μικρό μέγεθος, άρα περιορισμένη δυνατότητα στη μετάδοση μεγάλου όγκου πληροφοριών, αλλά η ελάχιστη απόστασή του επιτρέπει να διορθώνονται συγκριτικά πολλά λάθη σε σχέση με το μήκος της μεταδιδόμενης (κωδικο)λέξης.

Για παράδειγμα, αν έχουμε τον δυαδικό κώδικα Hamming $\mathcal{H}(4,\, 2)$, τότε αυτός έχει μήκος $n = 15$, πλήθος στοιχείων $M = 2^{11}$ και διορθώνει ένα λάθος. Σε αντιδιαστολή, ο δυϊκός του κώδικας $\mathcal{S}(4,\, 2)$ έχει πλήθος στοιχείων $N = 2^4$, αλλά διορθώνει 3 λάθη.

3. Όπως έχουμε προαναφέρει στον δυϊκό ενός κώδικα Hamming $\mathcal{H}(r,\, q)$ όλα τα μη μηδενικά στοιχεία έχουν βάρος ίσον με q^{r-1}, επομένως ο απαριθμητής βάρους για τον κώδικα $\mathcal{C} = \mathcal{H}(r,\, q)^{\perp}$ ισούται με $W_{\mathcal{C}}(z) = 1 + (q^{r-1}) \cdot z^{q^{r-1}}$ (γιατί;).

   Οπότε από την ταυτότητα του MacWilliams (ιδέ Παρατηρήσεις 2.5.6) μπορούμε να υπολογίσουμε την διασπορά βαρών του κώδικα $\mathcal{H}(r,\, q)$.

4.1.3 Οι κώδικες Hamming ως κυκλικοί κώδικες

Η παρουσίαση των κυκλικών κωδίκων με τη βοήθεια των $n-$οστών ριζών της μονάδας (βλέπε σελίδα 189) μας επιτρέπει να δούμε ότι μερικοί από τους κώδικες Hamming είναι ισοδύναμοι με κυκλικούς κώδικες.

Στην αρχή θα δούμε δύο παραδείγματα:

1. Έστω ότι έχουμε το πολυώνυμο $x^7 - 1$ επί του $\mathbb{Z}_2$. Με απλή επαλήθευση βλέπουμε ότι η ανάλυσή του σε γινόμενο αναγώγων παραγόντων είναι η εξής: $x^7 - 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$. Έστω $\mathcal{C} = \langle x^3 + x + 1 \rangle$ ο κυκλικός κώδικας με πολυώνυμο γεννήτορα $x^3 + x + 1$. Τότε ένας γεννήτορας πίνακας είναι ο:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

και ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$ είναι ο πίνακας:

$$\mathrm{P} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

καθότι ισχύει $\mathrm{GP}^t = \mathbf{0}$.

Όπως παρατηρούμε οι στήλες του πίνακα ελέγχου ισοτιμίας αναπαριστούν όλους τους αριθμούς από το 1 έως το $7 = 2^3 - 1$ σε δυαδική μορφή. Επομένως, ο κώδικας $\mathcal{C}$ είναι ισοδύναμος με τον κώδικα Hamming $\mathcal{H}(3, 2)$, ο οποίος έχει πίνακα ελέγχου ισοτιμίας τον πίνακα

$$\mathrm{H} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(βλέπε Παράδειγμα $4.1.2_2$).

Εδώ πρέπει να επισημάνουμε ότι ο κώδικας $\mathcal{H}(3, 2)$ δεν είναι κυκλικός (μπορείτε να ελέγξετε ότι το διάνυσμα $\mathbf{c} = 1000011$ είναι μια (κωδικο)λέξη του $\mathcal{H}(3, 2)$, ενώ η λέξη 1100001 δεν ανήκει στον $\mathcal{H}(3, 2)$.

Ας δούμε το προηγούμενο παράδειγμα με τον τρόπο που αναφέρεται στη σελίδα 191. Έστω ω μια πρωταρχική $7^η$ εβδόμη ρίζα της μονάδας επί του $\mathbb{Z}_2$, η οποία μηδενίζει το πολυώνυμο x^3+x+1. Η ω βρίσκεται στο σώμα ριζών του $x^3 + x + 1$, έστω $\mathbb{E}$. Το σώμα $\mathbb{E}$ περιέχει $2^3 = 8$ το πλήθος στοιχεία (γιατί;). Επίσης, επειδή η ω είναι πρωταρχική ρίζα της μονάδας όλες οι δυνάμεις $\omega, \omega^2, \ldots, \omega^7 = \omega^0 = 1$, είναι διακεκριμένες και ανήκουν στο $\mathbb{E}$. Επομένως, τα μη μηδενικά στοιχεία του $\mathbb{E}$ είναι οι δυνάμεις του ω. Αν επιλέξουμε μια βάση του $\mathbb{E}$ ως προς το $\mathbb{Z}_2$, τότε αυτή θα περιέχει τρία στοιχεία. Έστω $[\omega^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση του ω^j ως γραμμικού συνδυασμού των στοιχείων αυτής της βάσης με συντελεστές από το σώμα $\mathbb{Z}_2$. Τότε ο πίνακας $\mathrm{H} = \begin{pmatrix} [\omega^0] & [\omega^1] & \cdots & [\omega^6] \end{pmatrix}$ είναι ένας 3×7 πίνακας και οι στήλες του παριστούν όλους τους αριθμούς από το 1 έως το 7 σε δυαδική μορφή, άρα αποτελεί τον πίνακα ελέγχου ισοτιμίας ενός κώδικα Hamming, ο οποίος είναι ο κυκλικός κώδικας $\mathcal{C} = \langle x^3 + x + 1 \rangle$.

2. Στο Παράδειγμα 3.2.13 είχαμε κατασκευάσει όλους τους κυκλικούς κώδικες επί του $\mathbb{Z}_3$ μήκους τέσσερα. Από αυτούς οι κώδικες με γεννήτορες πίνακες:

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{και} \quad \begin{pmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$$

έχουν διάσταση ίση με 2 και ελάχιστη απόσταση το πολύ ίση με 2 (γιατί;).

Ένας τριαδικός κώδικας Hamming μήκους 4 έχει παραμέτρους $[n = (3^2-1)/(3-1) = 4, k = 4-2 = 2, d = 3]$. Επομένως, δεν μπορεί να είναι κυκλικός.

Μετά από τα παραδείγματα αυτά είμαστε σε θέση να δούμε τη γενική περίπτωση.

Θεώρημα 4.1.9. *Οι δυαδικοί κώδικες Hamming $\mathcal{H}(r, 2)$ είναι ισοδύναμοι με κυκλικούς κώδικες.*

Απόδειξη. Ως γνωστόν, ένας κώδικας Hamming $\mathcal{H}(r, 2)$ έχει παραμέτρους:

$$[n = 2^r - 1, k = 2^r - 1 - r, d = 3]$$

και πίνακα ελέγχου ισοτιμίας του οποίου οι στήλες αναπαριστούν όλους τους αριθμούς από το 1 έως το $2^r - 1$. Έστω τώρα ω μια $n-$οστή πρωταρχική ρίζα της μονάδας ($n = 2^r - 1$) επί του $\mathbb{Z}_2$. Το σώμα ριζών του πολυωνύμου $x^n - 1 \in \mathbb{Z}_2[x]$, έστω $\mathbb{E}$, αποτελείται από $n + 1 = 2^r$ το πλήθος στοιχεία και είναι διάστασης r ως διανυσματικός χώρος επί του $\mathbb{Z}_2$. Έστω $m_\omega(x)$ το ελάχιστο πολυώνυμο της ω. Το σώμα $\mathbb{E}$ είναι, επίσης, το σώμα ριζών του πολυωνύμου $m_\omega(x)$. Επειδή η ω είναι πρωταρχική ρίζα της μονάδας τα μη μηδενικά στοιχεία του $\mathbb{E}$ είναι οι δυνάμεις της ω. Αν συμβολίζουμε με $[\omega^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση της ω^j για $j = 0, \dots, n-1$ ως γραμμικού συνδυασμού των στοιχείων μιας βάσης με συντελεστές από το σώμα $\mathbb{Z}_2$, τότε ο πίνακας $\mathrm{H} = \begin{pmatrix} [\omega^0] & [\omega^1] & \cdots & [\omega^{n-1}] \end{pmatrix}$ είναι ένας $r \times n$ πίνακας και οι στήλες του παριστούν όλους τους αριθμούς από το 1 έως το n σε δυαδική μορφή, άρα αποτελεί τον πίνακα ελέγχου ισοτιμίας ενός κώδικα Hamming, ο οποίος είναι ο κυκλικός κώδικας $\mathcal{C} = \langle m_\omega(x) \rangle$. (Ιδέ τη σχετική συζήτηση στη σελίδα 191.) ό.έ.δ.

Παράδειγμα 4.1.10. Θεωρούμε τον κώδικα $\mathcal{H}(4,\,2)$. Στην περίπτωση αυτή το μήκος του κώδικα είναι ίσον με $n = 2^4 - 1 = 15$ και το σώμα ριζών του πολυωνύμου $x^{15} - 1 \in \mathbb{Z}_2[x]$ είναι το σώμα $\mathbb{E}$ με 2^4 το πλήθος στοιχεία. Έστω ω ένα πρωταρχικό στοιχείο του σώματος $\mathbb{E}$. Το στοιχείο αυτό είναι και 15^η πρωταρχική ρίζα της μονάδος, οι δυνάμεις $\omega,\, \omega^2,\, \omega^4,\, \omega^8$ είναι οι ρίζες του ελαχίστου πολυωνύμου $m_\omega(x) \in \mathbb{Z}_2[x]$. Δηλαδή:

$$m_\omega(x) = (x-\omega)(x-\omega^2)(x-\omega^4)(x-\omega^8) = x^4 - x + 1$$

(ίδέ Παράδειγμα Α΄.3.23).

Επομένως, το πολυώνυμο $x^4 - x + 1$ είναι το πολυώνυμο γεννήτορας του κώδικα $\mathcal{H}(4,\,2)$.

Στην περίπτωση που έχουμε έναν $q-$αδικό κώδικα Hamming $\mathcal{H}(r,\,q)$ με $q \neq 2$, όπως είδαμε και στο παράδειγμα προηγουμένως, ο κώδικας δεν είναι κατ' ανάγκην ισοδύναμος με έναν κυκλικό κώδικα. Το επόμενο θεώρημα δίνει μια ικανή συνθήκη για να είναι ένας κώδικας Hamming ισοδύναμος με έναν κυκλικό κώδικα.

Θεώρημα 4.1.11. *Έστω ο $q-$αδικός κώδικας Hamming $\mathcal{H}(r,\,q)$. Υποθέτουμε ότι $\text{μκδ}\,(r,\,q-1) = 1$. Τότε ο $\mathcal{H}(r,\,q)$ είναι ισοδύναμος με έναν κυκλικό κώδικα.*

Απόδειξη. Ο κώδικας $\mathcal{H}(r,\,q)$ έχει παραμέτρους:

$$[n = (q^r-1)/(q-1),\, k = (q^r-1)/(q-1) - r,\, d = 3].$$

Έστω $\mathbb{E}$ το σώμα ριζών του πολυωνύμου $x^n - 1$ επί του $\mathbb{F}$. Υποθέτουμε ότι το $\mathbb{E}$ έχει q^s το πλήθος στοιχεία. Έστω ω μια $n-$οστή πρωταρχική ρίζα της μονάδας. Τότε, αφενός η τάξη της ως στοιχείο της πολλαπλασιαστικής ομάδας του $\mathbb{E}$ είναι ίση με n και ο n διαιρεί τον $q^s - 1$, αφετέρου ο s είναι ο μικρότερος θετικός ακέραιος, ώστε η ω να ανήκει σε ένα σώμα με q^s το πλήθος στοιχεία. Δηλαδή έχουμε ότι ο $n = (q^r-1)/(q-1)$ διαιρεί τον $q^s - 1$ και ο s είναι ο μικρότερος θετικός ακέραιος με αυτή την ιδιότητα. Επειδή $(q^r-1)/(q-1) > q^{r-1} - 1$ και ο $(q^r-1)/(q-1)$ διαιρεί τον $q^r - 1$ έχουμε ότι αναγκαστικά $s = r$. Δηλαδή το σώμα ριζών $\mathbb{E}$ του πολυωνύμου $x^n - 1$ έχει q^r το πλήθος

στοιχεία. Αν, όπως προηγουμένως, συμβολίζουμε με $[\omega^j]$ το διάνυσμα στήλη των συντελεστών στην έκφραση της ω^j για $j = 0, \dots, n-1$ ως γραμμικού συνδυασμού των στοιχείων μιας βάσης με συντελεστές από το σώμα $\mathbb{F}$, τότε ο πίνακας $\mathrm{H} = \begin{pmatrix} [\omega^0] & [\omega^1] & \cdots & [\omega^{n-1}] \end{pmatrix}$ είναι ένας $r \times n$ πίνακας. Σκοπός μας είναι να δείξουμε ότι ο κυκλικός κώδικας $\mathcal{C}$, που έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα H, έχει τις ίδιες παραμέτρους με τον κώδικα $\mathcal{H}(r, q)$.

Ανά δύο οι στήλες του πίνακα H είναι γραμμικά ανεξάρτητες. Πράγματι, οι στήλες $[\omega^i]$ και $[\omega^j]$ είναι γραμμικά εξαρτημένες, αν και μόνο αν η μια είναι πολλαπλάσιο της άλλης με ένα στοιχείο από το $\mathbb{F}$. Αν και μόνο αν $\omega^i \cdot \omega^j = \omega^{i-j} \in \mathbb{F}$. Αλλά ένα μη μηδενικό στοιχείο a του $\mathbb{E}$ ανήκει στο $\mathbb{F}$, αν και μόνο αν $a^{q-1} = 1$. Επομένως, οι δύο στήλες $[\omega^i]$ και $[\omega^j]$ είναι γραμμικά εξαρτημένες, αν και μόνο αν $\omega^{(i-j)(q-1)} = 1$. Η ω είναι μια πρωταρχική $n-$οστη ρίζα της μονάδος, άρα $\omega^{(i-j)(q-1)} = 1$, αν και μόνο αν $(i-j)(q-1) \equiv 0 \mod n$. Η τελευταία σχέση με την προϋπόθεση ότι $\mathrm{μκδ}\,(r, q-1) = 1$ ισχύει (ιδέ την παρατήρηση μετά το τέλος της απόδειξης), μόνο αν $i = j$. Άρα αποδείξαμε ότι ανά δύο οι στήλες του πίνακα H είναι γραμμικά ανεξάρτητες. Επομένως, ο κυκλικός κώδικας $\mathcal{C}$ έχει μήκος ίσο με $n = (q^r - 1)/(q-1)$, διάσταση $k \geq (q^r-1)/(q-1) - r$ και ελάχιστη απόσταση $d \geq 3$ (ιδέ Πρόταση 2.2.25). Τώρα από το Θεώρημα 1.5.8 έπεται εύκολα ότι $k = (q^r-1)/(q-1) - r$ και $d = 3$, οπότε η απόδειξη τελείωσε. ό.έ.δ.

Παρατηρήσεις 4.1.12. 1. Στην προηγούμενη απόδειξη ισχυριστήκαμε ότι ισχύει $(i-j)(q-1) \equiv 0 \mod n$ με την προϋπόθεση ότι $\mathrm{μκδ}\,(r, q-1) = 1$, μόνο αν $i = j$.

Πράγματι, θα αποδείξουμε την εξής απλή άσκηση στη Θεωρία αριθμών. Έστω q δύναμη πρώτου αριθμού, r θετικός ακέραιος και $n = (q^r - 1)/(q-1)$, τότε ισχύει $\mathrm{μκδ}\,(r, q-1) = 1$, αν και μόνο αν $\mathrm{μκδ}\,(n, q-1) = 1$.

Έχουμε ότι $n = (q^r-1)/(q-1) = 1+q+q^2+\cdots+q^{r-1}$ και ο $q-1$ διαιρεί τον $q^i - 1$ για κάθε $i = 0, 1, \dots, r-1$, δηλαδή υπάρχουν ακέραιοι s_i, έτσι ώστε $q^i = (q-1)s_i + 1$. Επομένως, έχουμε ότι $n = ((q-1)s_0+1) + ((q-1)s_1+1) + \cdots + ((q-1)s_{r-1}+1) = (q-1)s + r$. Άρα, $\mathrm{μκδ}\,(r, q-1) = 1$, αν και μόνο αν $\mathrm{μκδ}\,(n, q-1) = 1$.

Επανερχόμενοι στα προηγούμενα, με την προϋπόθεση ότι $\mu\kappa\delta(r, q-1) = 1$ (δηλαδή ότι $\mu\kappa\delta(n,\, q-1) = 1$), έχουμε ότι $(i-j)(q-1) \equiv 0 \mod n$. Αυτό συνεπάγεται ότι $i = j$, δεδομένου ότι το n είναι η τάξη της ρίζας ω.

2. Στο προηγούμενο Παράδειγμα 2 είχαμε δει ότι ο τριαδικός κώδικας Hamming $\mathcal{H}(2,\, 3)$ δεν είναι ισοδύναμος με έναν κυκλικό κώδικα. Το αποτέλεσμα αυτό συνάδει με το προηγούμενο θεώρημα, καθότι $\mu\kappa\delta(r = 2,\, q-1 = 2) \neq 1$, αλλά δεν απορρέει ως αποτέλεσμα από το θεώρημα, διότι στο θεώρημα διατυπώνεται (μόνο) μια ικανή συνθήκη για να είναι ένας κώδικας Hamming κυκλικός.

4.1.4 Ασκήσεις

1. Με τη βοήθεια του κώδικα Hamming $\mathcal{H}(3,\, 2)$ να αποκωδικοποιήσετε τις λέξεις 1111000 και 1111111.

2. Με τη βοήθεια του κώδικα Hamming $\mathcal{H}(3,\, 3)$ να αποκωδικοποιήσετε τις λέξεις 1111001122201 και 0012200112202.

3. Εφαρμόζοντας στοιχειώδεις μετασχηματισμούς στον πίνακα ελέγχου ισοτιμίας του κώδικα $\mathcal{H}(3,\, 2)$ να τον φέρετε στη μορφή $[\mathrm{A}\ \mathrm{I}_3]$. Κατόπιν υπολογίστε έναν γεννήτορα πίνακα του $\mathcal{H}(3,\, 2)$.

4. Έστω $\widehat{\mathcal{H}(r,\, 2)}$ ο κώδικας που προκύπτει από την προσθήκη ενός ψηφίου ελέγχου ισοτιμίας στον κώδικα Hamming $\mathcal{H}(r,\, 2)$. Εξετάστε αν η δυνατότητα διόρθωσης λαθών αυξάνει με τον νέο κώδικα. Τι συμβαίνει με τη δυνατότητα ανίχνευσης λαθών;

5. Υποθέτουμε ότι έχουμε έναν συμμετρικό δυαδικό δίαυλο επικοινωνίας. Να δείξετε ότι η πιθανότητα σωστής αποκωδικοποίησης με τη βοήθεια του συνδρόμου, είναι ίδια είτε χρησιμοποιήσουμε τον κώδικα Hamming $\mathcal{H}(r,\, 2)$ είτε χρησιμοποιήσουμε τον κώδικα $\widehat{\mathcal{H}(r,\, 2)}$ που προκύπτει από την προσθήκη ενός ψηφίου ελέγχου ισοτιμίας στον κώδικα Hamming $\mathcal{H}(r,\, 2)$.

6. Να γενικεύσετε την προηγούμενη άσκηση στην περίπτωση ενός (τυχαίου) δυαδικού τέλειου κώδικα.

7. Δείξτε ότι αν q είναι μια δύναμη ενός πρώτου αριθμού και $3 \leq n \leq q+1$, τότε $A_q(n, 3) = q^{n-2}$.

8. Έχοντας υπόψη ότι οι κώδικεςHamming είναι τέλειοι, υπολογίστε τον αριθμό των (κωδικο)λέξεων βάρους 3 στον κώδικα $\mathcal{H}(r, 2)$. (Συγκεκριμένα δείξτε ότι ο αριθμός αυτός είναι ίσος με $(2^r - 1)(2^{r-1} - 1)/3$.)

9. Να υπολογίσετε τον απαριθμητή βάρους του κώδικα $\mathcal{H}(3, 2)$.

10. Να υπολογίσετε το πολυώνυμο γεννήτορα του (ισοδυνάμου) κυκλικού κώδικα Hamming $\mathcal{H}(3, 2)$, καθώς και τον αδύναμο γεννήτορα του.

11. Έστω ο κώδικας Hamming $\mathcal{H}(r, q)$ και $\mathcal{S}(r, q) = \mathcal{H}(r, q)^{\perp}$. Δείξτε ότι ο κώδικας $\mathcal{S}(r, q)$ *επιτυγχάνει* το φράγμα Plotkin.

    (Ιδέ Πόρισμα 1.5.24).

12. Έστω $\mathcal{H}(r, 2)$ ο δυαδικός κώδικας Hamming και H ένας πίνακας ελέγχου ισοτιμίας του.

    i) Δείξτε ότι, για κάθε δύο στήλες $\mathbf{h_1}$ και $\mathbf{h_2}$ του πίνακα H, υπάρχει μία άλλη (μοναδική) στήλη $\mathbf{h_3}$ με $\mathbf{h_1} + \mathbf{h_2} = \mathbf{h_3}$.

    ii) Με τη βοήθεια του προηγουμένου ερωτήματος, δείξτε ότι το πλήθος των (κωδικο)λέξεων βάρους 3 ισούται με $n(n-1)/6$, όπου n είναι το μήκος του κώδικα. (Συγκρίνατε με την ανωτέρω Άσκηση 8.)

    iii) Δείξτε ότι ο κώδικας $\mathcal{H}(r, 2)$ περιέχει την λέξη $1\,1 \cdots 1$.

    iv) Να υπολογίσετε το πλήθος των (κωδικο)λέξεων με βάρη $n-1$, $n-2$ και $n-3$.

13. Να αποδείξετε ότι ο απαριθμητής βάρους για τον κώδικα Hamming $\mathcal{C} = \mathcal{H}(r, 2)$ είναι ο:

$$W_{\mathcal{C}}(z) = \frac{1}{n+1} \cdot (1+z)^{(n-1)/2}((1+z)^{(n+1)/2} + n \cdot (1-z)^{(n+1)/2}).$$

Υπόδειξη: Ανατρέξτε στις Παρατηρήσεις 4.1.8$_3$ και 2.5.6.

14. Ένα δελτίο προγνωστικών αγώνων ποδοσφαίρου περιέχει έναν κατάλογο με 13 προγραμματισμένους αγώνες. Δίπλα σε κάθε προγραμματισμένο αγώνα ο *παίκτης* μπορεί να σημειώσει (μόνο) μια από τις προβλέψεις **1**, **x**, **2**.

    Να περιγράψετε τη *στρατηγική* που πρέπει να ακολουθήσει, κατά τη συμπλήρωση, ώστε να να απαιτηθεί ο ελάχιστος δυνατός αριθμός δελτίων που πρέπει να συμπληρωθούν, ώστε τουλάχιστον ένα από αυτά να περιέχει τουλάχιστον 12 σωστές προβλέψεις.

    Ποίος είναι ο ελάχιστος αριθμός των απαιτουμένων δελτίων;

    Υπόδειξη: Θεωρήστε τον $\mathcal{H}(3,\,3)$ κώδικα Hamming.

15. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

4.2 Κώδικες Golay

Οι κώδικες Golay αποτελούν μια πολύ ειδική κατηγορία κωδίκων, η οποία είναι από τις πλέον σημαντικές κατηγορίες κωδίκων που έχουν επινοηθεί. Υπάρχουν τέσσερεις κώδικες Golay, δύο από αυτούς είναι δυαδικοί και δύο τριαδικοί. Όλοι είναι γραμμικοί κώδικες. Δύο από αυτούς είναι κυκλικοί και τέλειοι, ενώ οι άλλοι δύο μπορούν να προκύψουν ως επεκτάσεις αυτών.

Οι κώδικες αυτοί επινοήθηκαν το 1948 από τον Golay και χρησιμοποιήθηκαν την περίοδο 1979 - 1981 από το διαστημόπλοιο Voyager για την αποστολή εγχρώμων φωτογραφιών στη Γη από τους πλανήτες Δία και Κρόνο.

Η εισαγωγή αυτών των κωδίκων έγινε από τον Golay παρουσιάζοντας τους αντίστοιχους γεννήτορες πίνακες. Ο τρόπος αυτός ορισμού των δεν δίνει καμία ένδειξη για τον λόγο που χρησιμοποιήθηκαν αυτοί οι συγκεκριμένοι πίνακες. Κατόπιν, λόγω του μεγάλου ενδιαφέροντος που παρουσιάζουν, επινοήθηκαν διάφοροι άλλοι τρόποι ορισμού των οι οποίοι όχι μόνο αποδεικνύουν με σύντομο και κομψό τρόπο τις ιδιότητες των κωδίκων Golay, αλλά και την μοναδικότητά τους.

Στην παράγραφο αυτή θα επιχειρήσουμε μια πρώτη παρουσίαση των κωδίκων Golay ορίζοντάς τους με την βοήθεια των αντιστοίχων γεννητόρων πινάκων χρησιμοποιώντας στοιχειώδη επιχειρήματα. Αργότερα θα επανέλθουμε (στην παράγραφο, όπου μελετώνται οι κώδικες τετραγωνικών υπολοίπων) και θα δούμε ότι οι κώδικες αυτοί αποτελούν μια πολύ ειδική περίπτωση μιας ευρύτερης κατηγορίας κωδίκων.

4.2.1 Δυαδικοί κώδικες Golay

Έστω ο 12×12 πίνακας με στοιχεία από το $\mathbb{Z}_2$:

$$\mathrm{A} = \begin{pmatrix} \cdot & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot \\ 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 \\ 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot \\ 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 \\ 1 & 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 \\ 1 & \cdot & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot \\ 1 & \cdot & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & 1 & 1 & \cdot & 1 & 1 & 1 & \cdot & \cdot & \cdot & 1 \end{pmatrix},$$

όπου στη θέση των $\cdot$ είναι μηδενικά.

Ορισμός 4.2.1. *Ο γραμμικός κώδικας με γεννήτορα πίνακα τον πίνακα* $\mathrm{G} = [\mathrm{I}_{12}\, \mathrm{A}]$ *λέγεται (επεκταμένος) κώδικας Golay και συμβολίζεται* $\mathcal{G}_{24}$.

Πρόταση 4.2.2. *1. Ο κώδικας* $\mathcal{G}_{24}$ *είναι αυτοδυϊκός.*

2. Ο πίνακας $[\mathrm{A}\, \mathrm{I}_{12}]$ *είναι, επίσης, ένας γεννήτορας πίνακας του* $\mathcal{G}_{24}$.

Απόδειξη. Δεν είναι δύσκολο να δούμε ότι ανά δύο οι γραμμές του γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_{12}\, \mathrm{A}]$ είναι κάθετες μεταξύ τους. Δηλαδή $\mathrm{G} \cdot \mathrm{G}^t = \mathbf{0}$. Από την Πρόταση 2.2.12 και το Θεώρημα 2.2.13 έπεται ότι $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

Παρατηρούμε ότι ο πίνακας A είναι συμμετρικός, οπότε από το Θεώρημα 2.2.17 έπεται ότι ο πίνακας $[\mathrm{A}\,\mathrm{I}_{12}]$ είναι, επίσης, ένας γεννήτορας πίνακας του $\mathcal{G}_{24}$. ό.έ.δ.

Λήμμα 4.2.3. *Το βάρος κάθε (κωδικο)λέξης στον κώδικα $\mathcal{G}_{24}$ είναι πολλαπλάσιο του 4, αλλά δεν ισούται με 4.*

Απόδειξη. Παρατηρούμε ότι το βάρος κάθε γραμμής του γεννήτορα πίνακα G είναι πολλαπλάσιο του 4. Έστω $\mathbf{r}$ και $\mathbf{s}$ δύο γραμμές του G. Από την Πρόταση 1.2.11 έχουμε ότι $w(\mathbf{r}+\mathbf{s}) = w(\mathbf{r}) + w(\mathbf{s}) - 2w(\mathbf{r}\cap\mathbf{s})$. Αλλά προηγουμένως έχουμε αποδείξει ότι οι γραμμές του πίνακα G είναι ανά δύο κάθετες, δηλαδή $w(\mathbf{r}\cap\mathbf{s}) = 0 \bmod 2$. Επομένως και το $w(\mathbf{r}+\mathbf{s})$ είναι πολλαπλάσιο του 4.

Επειδή ο κώδικας είναι δυαδικός, ισχύει ότι κάθε (κωδικο)λέξη είναι άθροισμα γραμμών του πίνακα G. Άρα, έχει βάρος πολλαπλάσιο του 4.

Υποθέτουμε τώρα ότι υπάρχει μια (κωδικο)λέξη $\mathbf{c} = c_1\,c_2\cdots c_{12}\,c_{13}\cdots c_{24}$ με βάρος ίσο με 4. Αν χωρίσουμε τη $\mathbf{c}$ σε δύο τμήματα $\mathbf{a} = c_1\,c_2\cdots c_{12}$ και $\mathbf{b} = c_{13}\cdots c_{24}$, τότε διακρίνουμε τις εξής περιπτώσεις.

1. $w(\mathbf{a}) = 0$ και $w(\mathbf{b}) = 4$. Η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{I}_{12}\,\mathrm{A}]$ έπεται ότι μόνο η μηδενική λέξη έχει τους πρώτους 12 χαρακτήρες όλους ίσους με 0.

2. $w(\mathbf{a}) = 4$ και $w(\mathbf{b}) = 0$. Όμοια η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{A}\,\mathrm{I}_{12}]$ έπεται ότι μόνο η μηδενική λέξη έχει τους 12 τελευταίους χαρακτήρες όλους ίσους με 0.

3. $w(\mathbf{a}) = 1$ και $w(\mathbf{b}) = 3$. Η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{I}_{12}\,\mathrm{A}]$ έπεται ότι η λέξη $\mathbf{c}$ πρέπει να είναι μια γραμμή του, αλλά καμία γραμμή του γεννήτορα πίνακα δεν έχει βάρος ίσο με 4.

4. $w(\mathbf{a}) = 3$ και $w(\mathbf{b}) = 1$. Όμοια η περίπτωση αυτή είναι αδύνατη, καθότι από τον γεννήτορα πίνακα $[\mathrm{A}\,\mathrm{I}_{12}]$ έπεται ότι η λέξη $\mathbf{c}$ πρέπει να είναι μια γραμμή του, αλλά καμία γραμμή του γεννήτορα πίνακα δεν έχει βάρος ίσο με 4.

   Απομένει μόνο η περίπτωση

5. $w(\mathbf{a}) = 2$ και $w(\mathbf{b}) = 2$. Στην περίπτωση αυτή έπεται ότι η λέξη $\mathbf{c}$ πρέπει να είναι το άθροισμα δύο γραμμών του πίνακα $[\mathrm{I}_{12}\,\mathrm{A}]$. Αλλά το άθροισμα δύο οποιωνδήποτε γραμμών του πίνακα A δεν έχει βάρος ίσον με 2.

   Άρα, τελικά, δεν υπάρχει $\mathbf{c} \in \mathcal{G}_{24}$ με βάρος ίσο με 4.

ό.έ.δ.

Από τα προηγούμενα έπεται το ακόλουθο θεώρημα.

Θεώρημα 4.2.4. *Ο κώδικας $\mathcal{G}_{24}$ είναι ένας $[24, 12, 8]$ γραμμικός κώδικας.*

Απόδειξη. Η απόδειξη είναι άμεση από τα προηγούμενα αρκεί να παρατηρήσουμε ότι η δεύτερη γραμμή του γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ έχει βάρος ίσο με 8. ό.έ.δ.

Παρατηρήσεις 4.2.5.

1. Στην Πρόταση 4.2.2 ο έλεγχος καθετότητας ανά δύο των γραμμών του γεννήτορα πίνακα $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ δεν είναι δύσκολος, αλλά είναι χρονοβόρος. Παρατηρούμε ότι το δεύτερο ήμισυ κάθε γραμμής, από την τρίτη έως και τη δωδέκατη, προέρχεται από μια κυκλική μετάθεση των στοιχείων του δεύτερου ήμισυ της δεύτερης γραμμής. Επομένως, για τον έλεγχο της καθετότητας δύο γραμμών του πίνακα είναι αρκετό να ελέγξουμε την καθετότητα μόνο της πρώτης και δεύτερης γραμμής ως προς τις γραμμές του πίνακα.

2. Ο γεννήτορας πίνακας $\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}]$ δεν είναι ο πίνακας που αρχικά επινοήθηκε από τον Golay, αλλά ένας πίνακας που δίνει έναν (ισοδύναμο) $[24, 12, 8]$ κώδικα Golay.

Αν από κάθε στοιχείο του κώδικα $\mathcal{G}_{24}$ διαγράψουμε τον τελευταίο χαρακτήρα, τότε επιτυγχάνουμε μια σύμπτυξη του κώδικα σε έναν άλλο κώδικα $\mathcal{G}_{23}$ με παραμέτρους $(23, 2^{12}, 7)$, (ο οποίος προς το παρόν δεν γνωρίζουμε αν είναι γραμμικός). Ο κώδικας $\mathcal{G}_{23}$ είναι ο δεύτερος δυαδικός κώδικας Golay και είναι τέλειος. Πράγματι, έχουμε ότι $2^{12}[1 + 23 + \binom{23}{2} + \binom{23}{3}] = 2^{23}$, οπότε από την Πρόταση 1.5.12 έχουμε ότι ο $\mathcal{G}_{23}$ είναι τέλειος.

Παρατήρηση 4.2.6. Αντί να διαγράψουμε τον τελευταίο χαρακτήρα κάθε (κωδικο)λέξης του $\mathcal{G}_{24}$ για να πάρουμε τον $\mathcal{G}_{23}$, θα μπορούσαμε να διαγράψουμε τον χαρακτήρα από μια συγκεκριμένη θέση σε όλες τις (κωδικο)λέξεις του $\mathcal{G}_{24}$ και να πάρουμε έναν ισοδύναμο κώδικα προς τον $\mathcal{G}_{23}$ (γιατί;).

Επίσης, θα μπορούσαμε να πάρουμε τον $\mathcal{G}_{24}$ ως επέκταση του $\mathcal{G}_{23}$ προσθέτοντας ένα στοιχείο ελέγχου ισοτιμίας οπότε από το Θεώρημα 1.4.10 δεν έχει σημασία ποιον από τους $\mathcal{G}_{24}$ ή $\mathcal{G}_{23}$ θα ορίσουμε πρώτα.

Ο κώδικας $\mathcal{G}_{24}$ διορθώνει τρία λάθη. Αν θελήσουμε να πραγματοποιήσουμε αποκωδικοποίηση με την βοήθεια των συνδρόμων, τότε πρέπει να υπολογίσουμε $\frac{2^{24}}{2^{12}} = 2^{12} = 4096$ το πλήθος σύνδρομα. Εκμεταλευόμενοι τη δομή του κώδικα μπορούμε να περιορίσουμε κατά πολύ τον αριθμό των απαιτουμένων συνδρόμων για την αποκωδικοποίηση μιας λέξης.

Έστω ότι ελήφθη η λέξη $\mathbf{x}$ και ότι κατά την αποστολή υπεισήλθαν 3 το πολύ λάθη, δηλαδή το διάνυσμα λάθους $\mathbf{e}$ έχει βάρος $w(\mathbf{e}) \leq 3$.

Ο κώδικας $\mathcal{G}_{24}$ είναι αυτοδυϊκός, επομένως οι πίνακες:

$$\mathrm{G} = [\mathrm{I}_{12}\,\mathrm{A}] \text{ και } \mathrm{C} = [\mathrm{A}\,\mathrm{I}_{12}]$$

είναι ταυτόχρονα και γεννήτορες και πίνακες ελέγχου ισοτιμίας. Ο υπολογισμός του συνδρόμου της λέξης $\mathbf{x}$ τόσο με την βοήθεια του πίνακα G όσο και με την βοήθεια του πίνακα C μας επιτρέπει να υπολογίσουμε το διάνυσμα λάθους σχετικά εύκολα.

Καταρχήν παρατηρούμε ότι το άθροισμα τρίων ή λιγότερο το πλήθος γραμμών του πίνακα A έχει βάρος τουλάχιστον ίσο με 5 (ιδέ τη μορφή του πίνακα A).

Θεωρούμε ότι το $\mathbf{e}$ αποτελείται από δύο τμήματα, δηλαδή $\mathbf{e} = \mathbf{e}_1\mathbf{e}_2$, όπου το κάθε ένα από τα $\mathbf{e}_i$ είναι μήκους 12. Τότε έχουμε:

$$\mathbf{x}\mathrm{G}^{\perp} = \mathbf{e}\mathrm{G}^{\perp} = \mathbf{e}_1 + \mathbf{e}_2\mathrm{A} \quad \text{και} \quad \mathbf{x}\mathrm{C}^{\perp} = \mathbf{e}\mathrm{C}^{\perp} = \mathbf{e}_1\mathrm{A} + \mathbf{e}_2.$$

Από τις προηγούμενες σχέσεις υπολογίζουμε τα βάρη των συνδρόμων:

$$\mathbf{x}\mathrm{G}^{\perp} = \mathbf{e}\mathrm{G}^{\perp} \quad \text{και} \quad \mathbf{x}\mathrm{C}^{\perp} = \mathbf{e}\mathrm{C}^{\perp}.$$

Διακρίνουμε περιπτώσεις:

(i) $w(\mathbf{e}\mathrm{G}^{\perp}) \geq 5$ και $w(\mathbf{e}\mathrm{C}^{\perp}) \leq 3$.

(ii) $w(\mathbf{e}\mathrm{G}^{\perp}) \leq 3$ και $w(\mathbf{e}\mathrm{C}^{\perp}) \geq 5$.

(iii) $w(\mathbf{e}\mathrm{G}^{\perp}) \geq 5$ και $w(\mathbf{e}\mathrm{C}^{\perp}) \geq 5$.

Αν έχουμε την πρώτη περίπτωση, τότε από τις προηγούμενες σχέσεις έπεται ότι αναγκαστικά το πρώτο τμήμα $\mathbf{e}_1$ στο διάνυσμα λάθους $\mathbf{e}$ είναι ίσο με το μηδενικό διάνυσμα ($\mathbf{e}_1 = \mathbf{0}$), οπότε από τη σχέση $\mathbf{x}\mathrm{C}^{\perp} = \mathbf{e}\mathrm{C}^{\perp} = \mathbf{e}_1\mathrm{A} + \mathbf{e}_2$ εύκολα έπεται ότι $\mathbf{e} = \mathbf{0}\mathbf{e}_2 = \mathbf{0}(\mathbf{x}\mathrm{C}^{\perp})$.

Όμοια, αν έχουμε τη δεύτερη περίπτωση, τότε έπεται ότι $\mathbf{e} = \mathbf{e}_1\mathbf{0} = (\mathbf{x}\mathrm{G}^{\perp})\mathbf{0}$.

Αν έχουμε την τρίτη περίπτωση, τότε έπεται ότι τόσο το τμήμα $\mathbf{e}_1$, όσο και το τμήμα $\mathbf{e}_2$ είναι μη μηδενικά. Αυτό σημαίνει ότι έχουν υπεισέλθει λάθη τόσο στις πρώτες 12 θέσεις, όσο και στις υπόλοιπες 12 θέσεις. Μάλιστα δε, αν έχει υπεισέλθει ένα λάθος στο πρώτο τμήμα, τότε στο δεύτερο έχουν υπεισέλθει το πολύ δύο και αντίστροφα.

Έστω ότι ένα λάθος εμφανίζεται στο πρώτο τμήμα στη θέση i, $i = 1, 2, \ldots, 12$. Τότε το $\mathbf{e}_1$ θα ισούται με ένα από τα $\epsilon_i = 0\,0 \cdots 1 \cdots 0$, οπότε υπολογίζοντας τα 12 σύνδρομα:

$$(\mathbf{x} + \boldsymbol{\epsilon}_j\mathbf{0})\mathrm{C}^{\perp} = (\mathbf{e} + \epsilon_j\mathbf{0})\mathrm{C}^{\perp} = (\epsilon_i\mathbf{e}_2 + \epsilon_j\mathbf{0})\mathrm{C}^{\perp} = \epsilon_i\mathrm{A} + \mathbf{e}_2 + \epsilon_j\mathrm{A}$$

για $j = 1, 2 \ldots, 12$ εντοπίζουμε τη θέση i του λάθους ως εξής:

Όλα τα παραπάνω σύνδρομα έχουν βάρος τουλάχιστον ίσο με 4 (γιατί;) εκτός από την περίπτωση όπου $i = j$, όπου έχουμε $\epsilon_i\mathrm{A} + \mathbf{e}_2 + \epsilon_i\mathrm{A} = \mathbf{e}_2$ και συνεπώς προσδιορίζουμε τόσο τη θέση του ενός λάθους στο πρώτο τμήμα $\mathbf{e}_1$, όσο και το δεύτερο τμήμα $\mathbf{e}_2$.

Παρόμοια αντιμετωπίζεται η περίπτωση, όπου στο πρώτο τμήμα εμφανίζονται δύο λάθη (οπότε στο δεύτερο εμφανίζεται ακριβώς ένα λάθος).

Ανακεφαλαιώνοντας, βλέπουμε ότι είναι αρκετός ο υπολογισμός 26 (το πολύ) συνδρόμων για να εντοπίσουμε και να διορθώσουμε μέχρι τρία λάθη με τον κώδικα $\mathcal{G}_{24}$.

4.2.2 Τριαδικοί κώδικες Golay

Έστω ο 6×6 πίνακας με στοιχεία από το $\mathbb{Z}_3$:

$$\mathrm{B} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}.$$

Ορισμός 4.2.7. *Ο γραμμικός κώδικας με γεννήτορα πίνακα τον πίνακα* $\mathrm{G} = [\mathrm{I}_6\, \mathrm{B}]$ *λέγεται (επεκταμένος) τριαδικός κώδικας Golay και θα συμβολίζεται με* $\mathcal{G}_{12}$.

Όπως και στην περίπτωση του δυαδικού κώδικα Golay $\mathcal{G}_{24}$, μπορούμε να αποδείξουμε το ακόλουθο θεώρημα.

Θεώρημα 4.2.8. *1. Ο τριαδικός κώδικας Golay* $\mathcal{G}_{12}$ *είναι αυτοδυϊκός.*

2. Ο πίνακας $[-\mathrm{B}\, \mathrm{I}_6]$ *είναι, επίσης, ένας γεννήτορας πίνακας του* $\mathcal{G}_{12}$.

3. Ο κώδικας $\mathcal{G}_{12}$ *είναι ένας* $[12, 6, 6]$ *κώδικας.*

4. Ο τριαδικός κώδικας $\mathcal{G}_{11}$ *που προέρχεται από τον* $\mathcal{G}_{12}$, *όταν διαγράψουμε τον τελευταίο χαρακτήρα από κάθε στοιχείο του* $\mathcal{G}_{12}$, *είναι ένας* $[11, 6, 5]$ *τέλειος κώδικας.*

Απόδειξη. Η απόδειξη είναι παρόμοια με την περίπτωση του δυαδικού κώδικα Golay $\mathcal{G}_{24}$ και αφίεται ως άσκηση. ό.έ.δ.

Επίσης, ο κώδικας $\mathcal{G}_{12}$ προέρχεται από τον κώδικα $\mathcal{G}_{11}$ προσθέτοντας ένα ψηφίο ελέγχου ισοτιμίας.

4.2.3 Οι κώδικες Golay ως κυκλικοί κώδικες

Εδώ θα δούμε ότι οι κώδικες $\mathcal{G}_{23}$ και $\mathcal{G}_{11}$ μπορούν να θεωρηθούν κατά ένα φυσιολογικό τρόπο ως κυκλικοί κώδικες.

Πρώτα θα εξετάσουμε την περίπτωση του δυαδικού κώδικα $\mathcal{G}_{23}$. Το μόνο που θα θεωρήσουμε ως δεδομένο είναι η ανάλυση του πολυωνύμου $x^{23}-1 = (x-1)\cdot(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)\cdot(x^{11}+x^9+x^7+x^6+x^5+x+1) \in \mathbb{Z}_2[x]$ σε γινόμενο αναγώγων πολυωνύμων. Έστω $g_1(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$ και $g_2(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$. Όπως βλέπουμε τα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία πολυώνυμα (βλέπε Παρατήρηση 3.2.17). Επομένως, αν $\mathcal{C}_1 = \langle g_1(x)\rangle$ και $\mathcal{C}_2 = \langle g_2(x)\rangle$, τότε οι $\mathcal{C}_1$ και $\mathcal{C}_2$ είναι ισοδύναμοι κώδικες. Από την Πρόταση 3.2.11 έχουμε ότι ο κυκλικός κώδικας $\mathcal{C}_1 = \langle g_1(x)\rangle$ έχει παραμέτρους $[23, 12, ?]$. Ο σκοπός μας τώρα είναι να υπολογίσουμε την ελάχιστη απόστασή του.

Λήμμα 4.2.9. *Έστω $x^p-1 = (x-1)\cdot g_1(x)\cdot g_2(x) \in \mathbb{Z}_2[x]$, όπου p είναι ένας περιττός πρώτος. Υποθέτουμε ότι οι κυκλικοί κώδικες $\mathcal{C}_1 = \langle g_1(x)\rangle$ και $\mathcal{C}_2 = \langle g_2(x)\rangle$ είναι ισοδύναμοι. Αν $a(x)$ είναι μια (κωδικο)λέξη του $\mathcal{C}_1$ περιττού βάρους, έστω w, τότε $w^2 \geq p$. Αν επιπλέον τα δύο πολυώνυμα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία πολυώνυμα, τότε $w^2 - w + 1 \geq p$.*

Απόδειξη. Επειδή οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ είναι ισοδύναμοι, υπάρχει μια (κωδικο)λέξη $b(x) \in \mathcal{C}_2$, η οποία έχει και αυτή βάρος ίσο με w. Το πολυώνυμο $a(x)$ είναι πολλαπλάσιο του $g_1(x)$, όμοια το πολυώνυμο $b(x)$ είναι πολλαπλάσιο του $g_2(x)$, επομένως το πολυώνυμο $a(x)\cdot b(x)$ είναι πολλαπλάσιο του $g_1(x)\cdot g_2(x)$. Άρα, το $a(x)\cdot b(x)$ θα είναι ίσο με $\mathbf{0}$ ή ίσο με $g_1(x)\cdot g_2(x)$. (Υπενθυμίζουμε ότι ο πολλαπλασιασμός γίνεται $\mod (x^p-1)$.)

Επειδή το βάρος w είναι περιττό, έχουμε ότι $w\cdot w = a(1)\cdot b(1) \equiv 1 \mod 2$. Επομένως αναγκαστικά $a(x)\cdot b(x) = g_1(x)\cdot g_2(x) = 1+x+x^2+\cdots+x^{p-1}$. Αλλά το γινόμενο $a(x)\cdot b(x)$ έχει το πολύ w^2 το πλήθος μη μηδενικούς συντελεστές, επομένως $w^2 \geq p$.

Στην περίπτωση που τα $g_1(x)$ και $g_2(x)$ είναι αμοιβαία πολυώνυμα, τότε τα στοιχεία του κώδικα $\mathcal{C}_2 = \langle g_2(x)\rangle$ είναι τα αμοιβαία στοιχεία των στοιχείων του κώδικα $\mathcal{C}_1 = \langle g_1(x)\rangle$ (ιδέ Παρατήρηση $3.2.17_3$). Επομένως, αν στη θέση του $b(x)$ παραπάνω πάρουμε το $a(x^{-1})$, τότε έχουμε $a(x)\cdot a(x^{-1}) = 1+x+x^2+\cdots+x^{p-1}$. Από τους w^2 το πλήθος όρους του γινομένου $a(x)\cdot a(x^{-1})$ οι w είναι ίσοι με 1 επομένως το μέγιστο βάρος του $a(x)\cdot a(x^{-1})$ ισουται με w^2-w+1, δηλαδή $w^2-w+1 \geq p$. ό.έ.δ.

Λήμμα 4.2.10. *Έστω* $x^p - 1 = (x-1) \cdot g_1(x) \cdot g_2(x) \in \mathbb{Z}_2[x]$, *όπου* p *είναι ένας περιττός πρώτος. Υποθέτουμε ότι τα πολυώνυμα* $g_1(x)$ *και* $g_2(x)$ *είναι αμοιβαία. Αν* $a(x)$ *είναι μια (κωδικο)λέξη του* $\mathcal{C} = \langle g_1(x) \rangle$ *αρτίου βάρους, έστω* w, *τότε* $w \equiv 0 \mod 4$. *Επιπλέον αν* $p \neq 7$, *τότε* $w \neq 4$.

Απόδειξη. Όπως και στην απόδειξη του προηγουμένου λήμματος, έχουμε ότι $a(x) \cdot a(x^{-1}) = 0$ ή $a(x) \cdot a(x^{-1}) = 1 + x + x^2 + \cdots + x^{p-1}$. Το $a(x)$ είναι αρτίου βάρους, επομένως $a(1) = 0$ και συνεπώς $a(x) \cdot a(x^{-1}) = 0$. Υποθέτουμε ότι $a(x) = x^{e_1} + x^{e_2} + \cdots + x^{e_w}$. Τότε $a(x) \cdot a(x^{-1}) = \sum_{i=1}^{w} \sum_{j=1}^{w} x^{e_i - e_j} = 0$ (οι πράξεις γίνονται $\mod (x^p - 1)$). Στο προηγούμενο άθροισμα έχουμε w^2 το πλήθος προσθεταίους. Στην περίπτωση όπου $i = j$ ο αντίστοιχος προσθεταίος είναι ίσος με 1, υπάρχουν w το πλήθος τέτοιοι προσθεταίοι, και επειδή το w είναι άρτιος το αθροισμά τους είναι ίσο με $0 \mod 2$. Οι υπόλοιποι $w^2 - w$ το πλήθος προσθεταίοι είναι της μορφής $x^{e_i - e_j}$ με $i \neq j$ και πρέπει να διαγράφονται ανά ζεύγη. Αλλά, αν $x^{e_i - e_j} = x^{e_k - e_r}$, τότε και $x^{e_j - e_i} = x^{e_r - e_k}$. Αυτό σημαίνει ότι οι προσθεταίοι αυτοί στο παραπάνω άθροισμα διαγράφονται ανά τετράδες. Δηλαδή $w^2 - w \equiv 0 \mod 4$, από όπου έπεται ότι $w \equiv 0 \mod 4$.

Υποθέτουμε τώρα ότι $w = 4$. Άνευ βλάβης της γενικότητας (επειδή ο κώδικας είναι κυκλικός) μπορούμε να υποθέσουμε ότι $a(x) = x^k + x^j + x^i + 1$ με $1 < k, j, i < p$. Από τη σχέση $a(x) \cdot a(x^{-1}) = (x^k + x^j + x^i + 1)(x^{-k} + x^{-j} + x^{-i} + 1) = 0$ έπεται ότι οι εκθέτες του γινομένου $(x^k + x^j + x^i + 1)(x^{-k} + x^{-j} + x^{-i} + 1)$ πρέπει να σχηματίζουν ζεύγη των οποίων τα μέλη να είναι ισότιμα $\mod p$. Εκτελώντας τις πράξεις, λόγω συμμετρίας, είναι αρκετό να εξετάσουμε κατά πόσο το i είναι ισότιμο $\mod p$ με το $j-k$ ή με το $-j$ ή με το $j-i$.

i) Υποθέτουμε ότι $i \equiv (j-k) \mod p$. Τότε όμως έχουμε $k \equiv (j-i) \mod p$, οπότε αναγκαστικά $j \equiv \pm(i-k) \mod p$. Από την πρώτη και τρίτη σχέση έπεται ότι $2k \equiv 0 \mod p$ ή $2i \equiv 0 \mod p$. Αυτό είναι αδύνατον, διότι έχει υποτεθεί ότι ο p είναι περιττός πρώτος.

ii) Υποθέτουμε ότι $i \equiv -j \mod p$. Έχοντας αποκλείσει δυνατότητες που εμφανίζονται στην πρώτη περίπτωση, έπεται ότι $k \equiv i - k \mod p$ ή $k \equiv j - k \mod p$. Υποθέτουμε ότι ισχύει η πρώτη σχέση (όμοια εξετάζεται και

η δεύτερη), οπότε έχουμε $2k \equiv i \mod p$. Τότε όμως αναγκαστικά θα ισχύει και $(i-j) \equiv (j-k) \mod p$. Συνδυάζοντας την τελευταία σχέση με τις σχέσεις $i \equiv -j \mod p$ και $2k \equiv i \mod p$, έχουμε ότι $7k \equiv 0 \mod p$, δηλαδή $p = 7$.

iii) Υποθέτουμε ότι $i \equiv (j-i) \mod p$. Έχοντας αποκλείσει δυνατότητες που εμφανίζονται στις προηγούμενες περιπτώσεις, έπεται ότι $j \equiv (k-j) \mod p$ και $k \equiv (i-k) \mod p$. Οπότε έπεται ότι $8j \equiv j \mod p$, δηλαδή πάλι $p = 7$ και η απόδειξη τελείωσε. ό.έ.δ.

Θεώρημα 4.2.11. *Έστω $\overline{\mathcal{G}_{23}} \subseteq \mathcal{R}_{23}$ ένας δυαδικός κυκλικός κώδικας με γεννήτορα πολυώνυμο $\gamma(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$. Ο κώδικας $\overline{\mathcal{G}_{23}}$ είναι ένας τέλειος κώδικας με παραμέτρους* $[23, 12, 7]$.

Απόδειξη. Από το Λήμμα 4.2.9 έχουμε ότι για κάθε (κωδικο)λέξη περιτού βάρους, έστω w, ισχύει $w^2 - w + 1 \geq 23$, δηλαδή $w \geq 7$. Από το Λήμμα 4.2.10 έχουμε ότι οι (κωδικο)λέξεις αρτίου βάρους έχουν βάρος μεγαλύτερο του 8. Αλλά η (κωδικο)λέξη $\gamma(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$ έχει βάρος 7, άρα ο κώδικας έχει παραμέτρους $[23, 12, 7]$. Επιπλέον, επειδή ισχύει $2^{12}\left[1 + 23 + \binom{23}{2} + \binom{23}{3}\right] = 2^{23}$, ο κώδικας είναι τέλειος. ό.έ.δ.

Παρατηρήσεις 4.2.12.

1. Ο κώδικας $\overline{\mathcal{G}_{23}}$ έχει τις ίδιες παραμέτρους με τον κώδικα Golay $\mathcal{G}_{23}$. Όπως θα δούμε στην επόμενη παράγραφο (Θεώρημα 4.3.3) οι δύο κώδικες είναι ισοδύναμοι, άρα ο κώδικας Golay $\mathcal{G}_{23}$ είναι κυκλικός.

2. Αξίζει να σημειωθεί ότι τα δύο προηγούμενα λήμματα ισχύουν γενικά για οποιονδήποτε περιττό πρώτο p και όχι συγκεκριμένα για τον $p = 23$.

3. Στην περίπτωση όπου $p = 7$ έχουμε ότι:

$$x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Το πολυώνυμο $x^3 + x^2 + 1$ είναι αμοιβαίο με το πολυώνυμο $x^3 + x + 1$ και ο κυκλικός κώδικας $\langle x^3 + x + 1 \rangle$ περιέχει (κωδικο)λέξεις βάρους 4 (υπολογίστε μια τουλάχιστον (κωδιο)λέξη βάρους 4). Άρα πράγματι η εξαίρεση του $p = 7$ στο Λήμμα 4.2.10 είναι αναγκαία.

4. Με τις υποθέσεις του Λήμματος 4.2.9, αν έχουμε εξασφαλίσει ότι η ελάχιστη απόσταση, έστω d, του κώδικα $\langle g_1(x)\rangle$ είναι περιττή, τότε ισχύει $d \geq \sqrt{p}$. Η τελευταία σχέση είναι γνωστή ως *φράγμα της τετραγωνικής ρίζας*.

   Υπάρχει μια ενδιαφέρουσα οικογένεια κωδίκων, οι κώδικες *τετραγωνικών υπολοίπων*, στην οποία ανήκει και ο κωδικας Golay $\mathcal{G}_{23}$, όπου η ελάχιστη απόσταση πληροί το φράγμα της τετραγωνικής ρίζας. Θα επανέλθουμε αργότερα, όταν θα ασχοληθούμε διεξοδικά με κώδικες τετραγωνικών υπολοίπων (ιδέ Παράγραφο 4.6).

Τώρα θα εξετάσουμε την περίπτωση του τριαδικού κώδικα $\mathcal{G}_{11}$. Θεωρούμε δεδομένη την ανάλυση του πολυωνύμου $x^{11}-1$ σε γινόμενο αναγώγων πολυωνύμων επί του $\mathbb{Z}_3$. Δηλαδή $x^{11}-1 = (x-1)\cdot g_1(x)\cdot g_2(x)$, όπου $g_1(x) = x^5+x^4-x^3+x^2-1$ και $g_2(x) = x^5-x^3+x^2-x-1$. Παρατηρούμε ότι $g_2(x) = (-x^5)(g_1(x)$, επομένως οι κυκλικοί κώδικες $\langle g_1(x)\rangle$ και $\langle g_2(x)\rangle$ είναι ισοδύναμοι με παραμέτρους $[11, 6, ?]$. Θα υπολογίσουμε την ελάχιστη απόσταση του κώδικα $\mathcal{C} = \langle g_1(x)\rangle \subseteq \mathcal{R}_{11}$.

Έστω ο κυκλικός κώδικας $\mathcal{D} = \langle (x-1)g_1(x)\rangle$. Προφανώς ο $\mathcal{D}$ περιέχεται στον κώδικα $\mathcal{C}$ και είναι διάστασης 5. Επίσης, από το Θεώρημα 3.2.21, έχουμε ότι ο κώδικας $\mathcal{D}$ είναι μηδενικού αθροίσματος, δηλαδή:

$$\text{αν } d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}, \text{ τότε } \textstyle\sum_{i=0}^{10} d_i = 0.$$

Ο δυϊκός κώδικας $\mathcal{D}^\perp$ παράγεται από το αμοιβαίο πολυώνυμο του $g_2(x)$ (βλέπε Παρατήρηση 3.2.17), δηλαδή το πολυώνυμο $-g_1(x)$. Αυτό σημαίνει ότι $\mathcal{D}^\perp = \langle -g_1(x)\rangle = \mathcal{C}$. Επομένως, για το $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$ έχουμε ότι είναι κάθετο στον εαυτό του. Δηλαδή $\sum_{i=0}^{10} d_i^2 \equiv 0 \mod 3$.

Έστω w το βάρος του στοιχείου $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$. Το w παριστά τον αριθμό των μη μηδενικών συντελεστών d_i. Αλλά, επειδή $d_i \in \mathbb{Z}_3$, έχουμε ότι για $d_i \neq 0$ ισχύει $d_i^2 \equiv 1 \mod 3$, οπότε $w \equiv \sum_{i=0}^{10} d_i^2 \mod 3$.

Από τα προηγούμενα έπεται η επομένη πρόταση.

Πρόταση 4.2.13. *Έστω $\mathcal{D}$ και $\mathcal{C}$ όπως προηγουμένως, αν $d(x) = d_0 + d_1x + \cdots + d_{10}x^{10} \in \mathcal{D}$ με βάρος w, τότε $\sum_{i=0}^{10} d_i = 0$ και $w \equiv \sum_{i=0}^{10} d_i^2 \equiv 0 \mod 3$.*

Επειδή η διάσταση του κώδικα $\mathcal{C}$ είναι 6 υπάρχουν τρία διαφορετικά σύμπλοκα του υπόχωρου $\mathcal{D}$ στο χώρο $\mathcal{C}$. Η (κωδικο)λέξη $a(x) = x^{10} + x^9 + \cdots + x + 1$ ανήκει στον κώδικα $\mathcal{C}$, αλλά δεν ανήκει στον $\mathcal{D}$, επομένως ο κώδικας $\mathcal{C}$ είναι η διακεκριμένη ένωση $\mathcal{C} = \mathcal{D} \cup (a(x) + \mathcal{D}) \cup (-a(x) + \mathcal{D})$.

Έστω $c(x) \in \mathcal{C}$ με $c(x) \notin \mathcal{D}$. Χωρίς βλάβη, υποθέτουμε ότι $c(x) = d(x) + a(x)$ με $d(x) = d_0 + d_1 x + \cdots + d_{10} x^{10} \in \mathcal{D}$, δηλαδή:

$$c(x) = (d_0 + 1) + (d_1 + 1)x + \cdots + (d_{10} + 1)x^{10}.$$

Οπότε, όπως προηγουμένως $w(c(x)) \equiv \sum_{i=0}^{10} (d_i + 1)^2 \mod 3$. Από την τελευταία σχέση έχουμε ότι $w(c(x)) \equiv [\sum_{i=0}^{10} d_i^2 + 2\sum_{i=0}^{10} d_i + 11] \mod 3$. Αλλά από την προηγούμενη πρόταση έχουμε ότι $\sum_{i=0}^{10} d_i^2 \equiv \sum_{i=0}^{10} d_i \equiv 0 \mod 3$. Οπότε:

$$w(c(x)) \equiv 11 \equiv 2 \mod 3.$$

Από την τελευταία σχέση έπεται ότι το βάρος ενός $c(x) \in \mathcal{C}$ με $c(x) \notin \mathcal{D}$ είναι μεγαλύτερο ή ίσο του 5, εκτός εάν είναι ίσο με 2. Αλλά αν $w(c(x)) = 2$, τότε $c(x) = x^i + x^j$ με $0 \leq i < j \leq 10$. Όμως το γινόμενο $c(x) \cdot c(x^{-1})$ πρέπει να είναι πολλαπλάσιο του $g_1(x) \cdot g_2(x) = x^{10} + x^9 + \cdots + x + 1$, άτοπο.

Ανακεφαλαιώνοντας έχουμε την επομένη πρόταση.

Πρόταση 4.2.14. *Έστω $\mathcal{D}$ και $\mathcal{C}$ όπως προηγουμένως, αν $c(x) \in \mathcal{C}$ με $c(x) \notin \mathcal{D}$, τότε $w(c(x)) \equiv 2 \mod 3$ και $w(c(x)) \geq 5$.*

Θεώρημα 4.2.15. *Ο κώδικας $\mathcal{C} = \langle g_1(x) \rangle$ είναι ένας $[11, 6, 5]$ τέλειος κώδικας.*

Απόδειξη. Ο κώδικας $\mathcal{C} = \langle g_1(x) \rangle$ έχει ελάχιστη απόσταση το πολύ 5, αφού έχει ένα στοιχείο, το $g_1(x) = x^5 + x^4 - x^3 + x^2 - 1$, με βάρος ίσο με 5. Από την προηγούμενη πρόταση έχουμε ότι στοιχεία που δεν ανήκουν στον (υπο)κώδικα $\mathcal{D}$ έχουν βάρος μεγαλύτερο ή ίσον του 5. Επομένως, αν η ελάχιστη απόσταση του κώδικα ήταν μικρότερη από 5, τότε θα έπρεπε να υπάρχει ένα στοιχείο $a(x) \in \mathcal{D}$ με βάρος μικρότερο ή ίσο του 4. Όμως από την Πρόταση 4.2.13 το βάρος του $a(x)$ είναι πολλαπλάσιο του 3. Υποθέτουμε ότι το στοιχείο $a(x) \in \mathcal{D}$ έχει βάρος 3. Χωρίς βλάβη της γενικότητας, λαμβάνοντας

κυκλικές μεταθέσεις των στοιχείων του (επειδή ο κώδικας είναι κυκλικός), μπορούμε να υποθέσουμε ότι $a(x) = 1 + x^i + x^j$ με τα i και j μη μηδενικά και διάφορα μεταξύ τους. Το $a(x) \cdot a(x^{-1})$ πρέπει να είναι πολλαπλάσιο του $(x-1) \cdot g_1(x) \cdot g_2(x) = x^{11} - 1$, το οποίο είναι μηδέν στον $\mathcal{R}_{11}$. Δηλαδή έχουμε ότι $(1 + x^i + x^j) \cdot (1 + x^{-i} + x^{-j}) = x^i + x^{-i} + x^j + x^{-j} + x^{j-i} + x^{i-j} = 0$. Από την τελευταία σχέση έχουμε ότι $i \equiv j \equiv (j-i) \mod 11$, δηλαδή $i \equiv 0 \mod , 11$, άτοπο. Άρα, τελικά, η ελαχίστη απόσταση του κώδικα $\mathcal{C}$ ισούται με 5.

Επιπλέον, ο κώδικας είναι τέλειος, αφού ισχύει $3^6[1 + 2 \cdot 11 + 2^2\binom{11}{2}] = 3^{11}$. ό.έ.δ.

Ο κώδικας $\mathcal{C}$ έχει τις ίδιες παραμέτρους με τον κώδικα Golay $\mathcal{G}_{11}$. Όπως και στην περίπτωση του δυαδικού κώδικα Golay, ο κώδικας $\mathcal{C}$ είναι ισοδύναμος με τον τριαδικό κώδικα Golay $\mathcal{G}_{11}$. (Ιδέ Θεώρημα 4.3.3.)

Παρατήρηση 4.2.16. Στη σελίδα 241, είχαμε αναφερθεί στον αριθμό των συνδρόμων που απαιτούνται να υπολογισθούν για τη διόρθωση τριών λαθών με τον κώδικα $\mathcal{G}_{24}$. Εκεί είδαμε ότι η δομή του κώδικα (αν και δεν είναι κυκλικός) μας επέτρεψε να μειώσουμε δραματικά τους απαιτούμενους υπολογισμούς.

Για την κωδικοποίηση και αποκωδικωποίηση μέσω των κωδίκων $\mathcal{G}_{23}$ και $\mathcal{G}_{11}$, οι οποίοι είναι κυκλικοί, μπορούμε να χρησιμοποιήσουμε τη δομή τους και να εφαρμόσουμε τις μεθόδους που παρουσιάζονται στην Παράγραφο 3.2.4.

4.2.4 Η διασπορά βαρών στους κώδικες Golay

Ο κώδικας Goley $\mathcal{G}_{23}$ έχει προφανώς ακτίνα κάλυψης ίση με τρία (γιατί;). Επομένως, όλες οι σφαίρες με ακτίνα ίση με τρία και κέντρο τα στοιχεία του κώδικα είναι ξένες μεταξύ τους και καλύπτουν όλο τον χώρο $\mathbb{Z}_2^{23}$. Έστω μια σφαίρα με κέντρο μια (κωδικο)λέξη βάρους i. Ας συμβολίσουμε με $N_i(w)$ το πλήθος των στοιχείων βάρους w, τα οποία περιέχονται σε αυτή τη σφαίρα. Προφανώς ο αριθμός $N_i(w)$ δεν εξαρτάται από την επιλεγείσα (κωδικο)λέξη ως κέντρο της σφαίρας, αλλά μόνο από το βάρος της (γιατί;). Επισημαίνεται

επίσης ότι αν έχουμε μια (κωδικο)λέξη βάρους i, τότε για λέξεις με βάρος w, όπου $\mid w-i \mid > 3$, έχουμε $N_i(w) = 0$. Ο κώδικας είναι δυαδικός, επομένως υπάρχουν συνολικά $\binom{23}{w}$ το πλήθος λέξεις βάρους w στον χώρο $\mathbb{Z}_2^{23}$. Συνεπώς:

$$\sum_{i=0}^{23} N_i(w) A_i = \binom{23}{w}. \qquad (*)$$

Η τελευταία σχέση είναι χρήσιμη για τον υπολογισμό της διασποράς βαρών $\{ A_0, A_1, \ldots, A_{23} \}$ για τον κώδικα $\mathcal{G}_{23}$.

Θα δούμε την *στρατηγική*, με την οποία υπολογίζουμε τα A_i χρησιμοποιώντας την προηγούμενη σχέση. Προφανώς $A_0 = 1$ και $A_i = 0$ για $1 \leq i \leq 6$. Έστω μια λέξη $\mathbf{x} \in \mathbb{Z}_2^{23}$ βάρους 4. Η λέξη αυτή θα βρίσκεται σε μια μόνο σφαίρα ακτίνας 3 και με κέντρο μια (κωδικο)λέξη $\mathbf{c}$. Το βάρος της $\mathbf{c}$ είναι αναγκαστικά ίσον με 7, διότι αν η $\mathbf{c}$ είχε βάρος μεγαλύτερο ή ισον του 8, τότε $d(\mathbf{c}, \mathbf{x}) \geq 4$, άτοπο. Αυτό σημαίνει ότι $N_i(4) = 0$ για $8 \leq i \leq 23$. Συνεπώς το πλήθος των λέξεων βάρους 4, οι οποίες απέχουν απόσταση ίση με 3 από την $\mathbf{c}$ είναι ίσον με $\binom{7}{4}$. (Από τις 7 μη μηδενικές θέσεις της $\mathbf{c}$ επιλέγουμε τις 4 μη μηδενικές θέσεις της $\mathbf{x}$). Επομένως, έχουμε $N_7(4) = \binom{7}{4}$.

Από τη σχέση $(*)$ τώρα έχουμε ότι $N_7(4)\, A_7 = \binom{23}{4}$, δηλαδή $\binom{7}{4} A_7 = \binom{23}{4}$ απ' όπου έπεται ότι $A_7 = 253$.

Έστω τώρα μια λέξη $\mathbf{x} \in \mathbb{Z}_2^{23}$ βάρους 5. Η λέξη αυτή θα βρίσκεται σε μια μόνο σφαίρα ακτίνας 3 και με κέντρο μια (κωδικο)λέξη $\mathbf{c}$. Το βάρος της $\mathbf{c}$ είναι αναγκαστικά ίσον με 7 ή ίσον με 8. Οπότε, όπως προηγουμένως, θα έχουμε $N_7(5) = \binom{7}{5}$, $N_8(5) = \binom{8}{5}$ και $N_i(5) = 0$ για $9 \leq i \leq 23$. Επομένως, από την $(*)$ έχουμε $N_7(5)A_7 + N_8(5)A_8 = \binom{23}{5}$, δηλαδή $\binom{7}{5}A_7 + \binom{8}{5}A_8 = \binom{23}{5}$, απ' όπου έπεται ότι $A_8 = 506$.

Με την ίδια μέθοδο, αλλά με περισσότερους υπολογισμούς, μπορούμε να συνεχίσουμε και να υπολογίσουμε όλα τα A_i (Προσπαθήστε το!).

Τελικά αποδεικνύεται ότι ο (ομογενοποιημένος) απαριθμητής βάρους για τον κώδικα Golay $\mathcal{G}_{23}$ είναι ο:

$$W_{\mathcal{G}_{23}}(x, y) = y^{23} + 253x^7y^{16} + 506x^8y^{15} + 1288x^{11}y^{12} + \\ + 1288xy^{11} + 506x^{15}y^8 + 253x^{16}y^7 + x^{23}.$$

Στην περίπτωση του τριαδικού Golay κώδικα $\mathcal{G}_{11}$, επειδή και αυτός είναι τέλειος με ακτίνα ομαδοποίησης ίση με 2, μπορούμε να αποδείξουμε μια παρόμοια σχέση με την σχέση $(*)$. Συγκεκριμένα ισχύει:

$$\sum_{i=0}^{11} N_i(w)A_i = \binom{11}{w} \cdot 2^w.$$

Όπου και εδώ με $N_i(w)$ συμβολίζουμε το πλήθος των στοιχείων του $\mathbb{Z}_3^{11}$ βάρους w, τα οποία βρίσκονται σε μία σφαίρα ακτίνας ίσης με 2 και με κέντρο μια (κωδικο)λέξη βάρους i.

Εδώ αποδεικνύεται ότι ο (ομογενοποιημένος) απαριθμητής βάρους για τον Golay κώδικα $\mathcal{G}_{11}$ είναι ο:

$$W_{\mathcal{G}_{11}}(x, y) = y^{11} + 132x^5y^6 + 132x^6y^5 + 330x^8y^3 + 110x^9y^2 + 24x^{11}.$$

Παρατηρήσεις 4.2.17. 1. Ισχύει ότι η λέξη $1\,1, \cdots 1$ μήκους 23 ανήκει στον κώδικα $\mathcal{G}_{23}$ (ιδέ Άσκηση 3.2.5$_6$). Επομένως $A_i = A_{23-i}$ (ιδέ Άσκηση 2.5.1$_2$). Οπότε θα μπορούσαμε να μειώσουμε δραματικά τις πράξεις για τον υπολογισμό των A_i.

2. Στην προηγούμενη επιχειρηματολογία για τον υπολογισμό των A_i δεν χρησιμοποιήσαμε την δομή των Golay κωδίκων παρά μόνο το γεγονός ότι είναι τέλειοι κώδικες. Επομένως, την ίδια επιχειρηματολογία θα μπορούσαμε να εφαρμόσουμε και στην περίπτωση των δυαδικών κωδίκων Hamming.

   Συγκεκριμένα μπορείτε να αποδείξετε ότι σε έναν $\mathcal{H}(r, 2)$ μήκους $n = 2^r - 1$ κώδικα Hamming ισχύει: $\sum_{i=0}^{n} N_i(w)A_i = \binom{n}{w}$.

   Εδώ ο υπολογισμός των $N_i(w)$ είναι σχετικά πιο εύκολος, καθότι η ακτίνα κάλυψης ισούται με 1.

   Επίσης, μπορείτε να προχωρήσετε στον υπολογισμό του απαριθμητή βάρους του κώδικα $\mathcal{H}(r, 2)$ και να κάνετε σύγκριση με την Άσκηση 4.1.4$_{13}$.

4.2.5 Ασκήσεις

1. Έστω A_i το πλήθος των στοιχείων βάρους i σε έναν κώδικα. Δείξτε ότι στον κώδικα $\mathcal{G}_{24}$ ισχύει $A_{20} = A_4 = 0$ $A_8 = A_{16}$.

2. Δείξτε ότι αν $\mathbf{x}$ είναι μια δυαδική λέξη μήκους 23 και βάρους 4, τότε υπάρχει μοναδική (κωδικο)λέξη $\mathbf{c} \in \mathcal{G}_{23}$ βάρους 7 η οποία έχει 1 στις αντίστοιχες θέσεις που έχει 1 και η λέξη $\mathbf{x}$. Με τον τρόπο αυτό αποδείξτε ότι το πλήθος των κωδικολέξεων βάρους 7 στον κώδικα ισούται με 253.

3. Δείξτε ότι στον κώδικα $\mathcal{G}_{11}$ το πλήθος των στοιχείων βάρους 5 είναι ίσο με 132.

   Υπόδειξη: Χρησιμοποιήστε το γεγονός ότι ο κώδικας $\mathcal{G}_{11}$ είναι τέλειος και υπολογίστε το πλήθος των ζευγών των λέξεων $(\mathbf{x}, \mathbf{c})$, όπου $\mathbf{x} \in \mathbb{Z}_2^{11}$ και έχει βάρος 3 και $\mathbf{c} \in \mathcal{G}_{11}$, έχει βάρος 5 και οι μη μηδενικές θέσεις της $\mathbf{x}$ συμπίπτουν με τις αντίστοιχες μη μηδενικές θέσεις της $\mathbf{c}$.

4. Να αποδείξετε τις σχέσεις που αναφέρονται στους απαριθμητές βάρους για τους κώδικες Golay στη Σελίδα 250.

5. Δείξτε ότι μεταθέτοντας στήλες και εφαρμόζοντας στοιχειώδεις πράξεις γραμμών ένας γεννήτορας πίνακας του κώδικα $\mathcal{G}_{24}$ μπορεί να λάβει τη μορφή:
$$\begin{pmatrix} \mathrm{I}_7 & * \\ \mathbf{0}_5 & * \end{pmatrix},$$
   όπου η $8^η$ στήλη είναι το άθροισμα των επτά πρώτων στηλών.

6. Έστω H ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα Hamming $\mathcal{H}(2, 3)$ και J ο τετραγωνικός πίνακας 4×4 με όλα τα στοιχεία του ίσα με 1. Δείξτε ότι ο πίνακας:
$$\mathrm{G} = \begin{pmatrix} \mathrm{J} + \mathrm{I}_4 & \mathrm{I}_4 & \mathrm{I}_4 \\ \mathbf{0} & \mathrm{H} & -\mathrm{H} \end{pmatrix}$$
   είναι ο γεννήτορας πίνακας ενός κώδικα ισοδυνάμου με τον κώδικα $\mathcal{G}_{12}$.

7. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

4.3 Η μοναδικότητα των κωδίκων Hamming και Goley ως τέλειων κωδίκων

Στην Παράγραφο 1.5 είχαμε αναφέρει (αλλά είχαμε αναβάλει την απόδειξη) ότι παρόλο που οι παράμετροι $(n,\, M,\, d) = (90,\, 2^{78},\, 5)$ ικανοποιούν τη συνθήκη 1.2, δεν υπάρχουν κώδικες με αυτές τις παραμέτρους. Τώρα μπορούμε να δώσουμε μια απόδειξη.

Θεώρημα 4.3.1. *Δεν υπάρχει γραμμικός δυαδικός κώδικας με παραμέτρους* $[90,\, 78,\, 5]$.

Απόδειξη. Υποθέτουμε ότι υπάρχει ένας δυαδικός γραμμικός κώδικας με τις παραπάνω παραμέτρους. Έστω Η ένας πίνακας ελέγχου ισοτιμίας αυτού του κώδικα. Ο πίνακας αυτός είναι ένας 12×90 πίνακας, ας συμβολίσουμε με $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{90}$ τις στήλες του. Από την Πρόταση 2.2.25 έπεται ότι κάθε τετράδα από τις στήλες $\mathbf{h}_i$ αποτελείται από γραμμικά ανεξάρτητες στήλες. Επομένως, το σύνολο $\mathrm{A} = \{\, \mathbf{0},\, \mathbf{h}_i,\, \mathbf{h}_j + \mathbf{h}_k \mid 1 \leq i \leq 90,\, 1 \leq j < k \leq 90 \,\}$ περιέχει $1 + 90 + \binom{90}{2} = 2^{12}$ το πλήθος στοιχεία. Αν οι στήλες του πίνακα Η θεωρηθούν ως διανύσματα, βλέπουμε ότι το σύνολο Α είναι το $\mathbb{Z}_2^{12}$. Ως γνωστόν (ιδέ Άσκηση $2.1.2_2$), το ήμισυ των στοιχείων του $\mathbb{Z}_2^{12}$ έχουν περιττό βάρος, επομένως το σύνολο Α περιέχει 2^{11} το πλήθος στοιχεία περιττού βάρους.

Ας υπολογίσουμε το πλήθος των στοιχείων του συνόλου Α περιττού βάρους με διαφορετικό τρόπο. Υποθέτουμε ότι r το πλήθος από τις στήλες του πίνακα Η έχουν περιττό βάρος, άρα οι αρτίου βάρους στήλες είναι $90 - r$ το πλήθος. Από τη σχέση $w(\mathbf{h}_j + \mathbf{h}_k) = w(\mathbf{h}_j) + w(\mathbf{h}_k) - 2w(\mathbf{h}_j \cap \mathbf{h}_k)$ (ιδέ Πρόταση 1.2.11) έχουμε ότι το βάρος του στοιχείου $\mathbf{h}_j + \mathbf{h}_k$ είναι περιττό, αν και μόνο αν ακριβώς ένα από τα στοιχεία $\mathbf{h}_j$ και $\mathbf{h}_k$ είναι περιττού βάρους. Άρα το σύνολο Α έχει $r + r(90 - r)$ το πλήθος στοιχεία περιττού βάρους. Τελικά πρέπει να ισχύει $r + r(90 - r) = 2^{11}$. Όπως εύκολα διαπιστώνουμε δεν υπάρχει θετικός ακέραιος που να πληροί την τελευταία σχέση. Άρα δεν υπάρχει γραμμικός δυαδικός κώδικας με παραμέτρους $[90,\, 78,\, 5]$. ό.έ.δ.

Το προηγούμενο θεώρημα αναφέρεται στην μη ύπαρξη γραμμικών κωδί-

κων με τις παραμέτρους $(n,\, M,\, d) = (90,\, 2^{78},\, 5)$. Μπορούμε να αποδείξουμε ένα αποτέλεσμα που αναφέρεται στην μη ύπαρξη μη γραμμικών $(90,\, 2^{78},\, 5)$ κωδίκων.

Έστω $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^n$. Υπενθυμίζουμε ότι:
Το διάνυσμα $\mathbf{u}$ **καλύπτει** το $\mathbf{v}$, αν και μόνο αν $\mathbf{u} \cap \mathbf{v} = \mathbf{v}$. Δηλαδή στις θέσεις που το $\mathbf{v}$ έχει 1, έχει 1 οπωσδήποτε και το $\mathbf{u}$.

Για παράδειγμα το $\mathbf{u} = 110101$ καλύπτει το $\mathbf{v} = 010001$.

Πρόταση 4.3.2. *Δεν υπάρχει* $(90,\, 2^{78},\, 5)$ *δυαδικός κώδικας.*

Απόδειξη. Υποθέτουμε ότι υπάρχει ένας $(90,\, 2^{78},\, 5)$ κώδικας $\mathcal{C}$. Από την Πρόταση 1.4.5 έπεται ότι μπορούμε να υποθέσουμε ότι η μηδενική λέξη είναι στοιχείο του κώδικα ($\mathbf{0} \in \mathcal{C}$). Επειδή η ελάχιστη απόσταση είναι ίση με 5, κάθε μη μηδενική (κωδικο)λέξη έχει βάρος τουλάχιστον 5. Έστω Y το υποσύνολο του $\mathbb{Z}_2^{90}$, τα στοιχεία του οποίου έχουν βάρος 3 και τα δύο πρώτα ψηφία τους είναι 1. Δηλαδή μόνο τρία ψηφία τους είναι 1 εκ των οποίων τα δύο καταλαμβάνουν τις δύο πρώτες θέσεις και το τρίτο μια από τις υπόλοιπες 88. Προφανώς $|Y| = 88$.

Ο κώδικας $\mathcal{C}$ είναι τέλειος, επομένως κάθε στοιχείο, έστω $\mathbf{y}$, του Y βρίσκεται σε μια μοναδική σφαίρα $S(\mathbf{x},\, 2)$ ακτίνας ίσης με 2. Το κέντρο $\mathbf{x}$ της σφαίρας πρέπει να έχει βάρος ίσο με 5 και να καλύπτει το $\mathbf{y}$ (γιατί;).

Έστω X το σύνολο όλων των (κωδικο)λέξεων του $\mathcal{C}$, οι οποίες έχουν στις δύο πρώτες θέσεις 1 και το βάρος τους ισούται με 5. Κάθε στοιχείο $\mathbf{x}$ του συνόλου X καλύπτει ακριβώς τρία στοιχεία του συνόλου Y. Πράγματι ένα στοιχείο $\mathbf{x}$ του X έχει δύο 1 στις δύο πρώτες θέσεις και τρία 1, τα οποία κατανέμονται στις υπόλοιπες 88 θέσεις, επομένως καλύπτει τα τρία στοιχεία του Y που το καθένα έχει (το τρίτο) 1 σε μια από τις τρείς θέσεις (εκτός της πρώτης και δεύτερης) που καταλαμβάνουν τα 1 του $\mathbf{x}$. Επομένως, για ένα $\mathbf{x} \in X$ έχουμε τρία διαφορετικά ζεύγη $(\mathbf{x},\, \mathbf{y}_i)$, $i = 1, 2, 3$ με $\mathbf{y}_i \in Y$, έτσι ώστε το $\mathbf{x}$ να καλύπτει το $\mathbf{y}_i$. Άρα αν $R = \{\, (\mathbf{x},\, \mathbf{y}) \,|\, \mathbf{x} \in X,\, \mathbf{y} \in Y \text{ και } \mathbf{x} \text{ καλύπτει το } \mathbf{y} \,\}$, τότε $|\, R \,| = 3 \,|\, X \,|$. Αλλά ο κώδικας είναι τέλειος, συνεπώς δεν υπάρχουν δύο διαφορετικά $\mathbf{x}_1, \mathbf{x}_2 \in X$ που να καλύπτουν το ίδιο $\mathbf{y} \in Y$. Επομένως, $|\, R \,| = |\, Y \,| = 88$.

Από τα προηγούμενα έπεται ότι $\mid X \mid = \frac{88}{3}$, άτοπο, άρα δεν υπάρχει $(90, 2^{78}, 5)$ δυαδικός κώδικας. ό.έ.δ.

Ανακεφαλαιώνοντας βλέπουμε ότι, πέραν των τετριμμένων, τέλειοι κώδικες είναι οι κώδικες Hamming $\mathcal{H}(r, p)$ και οι κώδικες Golay $\mathcal{G}_{23}$ και $\mathcal{G}_{11}$. Οι κώδικες αυτοί είναι γραμμικοί. Στην Παρατήρηση $4.1.4_4$ είχαμε δει ότι υπάρχουν δυαδικοί κώδικες με τις παραμέτρους ενός κώδικα Hamming, οι οποίοι δεν είναι γραμμικοί. Έχουν κατασκευασθεί κώδικες επί ενός αλφάβητου $\mathbb{F}$, όπου $\mathbb{F}$ είναι ένα τυχαίο πεπερασμένο σώμα, με τις παραμέτρους ενός κώδικα Hamming, οι οποίοι δεν είναι γραμμικοί.

Στην πραγματικότητα δεν υπάρχουν άλλοι τέλειοι κώδικες επί ενός αλφάβητου $\mathbb{F}$, όπου $\mathbb{F}$ είναι ένα πεπερασμένο σώμα. Συγκεκριμένα ισχύει το εξής Θεώρημα:

Θεώρημα 4.3.3. *Ένας μη τετριμμένος τέλειος κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ πρέπει να έχει είτε τις παραμέτρους ένος κώδικα Hamming είτε τις παραμέτρους ενός από τους κώδικες Golay $\mathcal{G}_{23}, \mathcal{G}_{11}$.*

Επιπλέον, αν ένας κώδικας έχει τις παραμέτρους ενός από τους κώδικες Golay, τότε είναι ισοδύναμος προς αυτόν. Αν ένας κώδικας έχει τις παραμέτρους ενός από τους κώδικες Hamming και είναι γραμμικός, τότε είναι ισοδύναμος προς αυτόν.

Η απόδειξη αυτού του θεωρήματος είναι πέραν του σκοπού του παρόντος. Ο ενδιαφερόμενος μπορεί να βρει μια απόδειξη στο βιβλίο των MacWilliams, F.J. and Sloane, N.J.A. [1977] (Κεφ. 6 Παρ. 10). Αξίζει όμως να αναφέρουμε την κεντρική ιδέα, η οποία βασίζεται στο εξής θεώρημα του Lloyd, το οποίο παραθέτουμε και αυτό χωρίς απόδειξη.

Θεώρημα 4.3.4. *Εάν υπάρχει ένας τέλειος $(n, M, 2\lambda+1)$ κώδικας επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία, τότε το πολυώνυμο:*

$$L(x) = \sum_{i=0}^{\lambda} (-1)^i (q-1)^{\lambda-i} \binom{x-1}{i} \binom{n-x}{\lambda-i}$$

έχει λ διακεκριμένες ακέραιες ρίζες μεταξύ του 1 και του n.

Από το Θεώρημα αυτό αποδεικνύεται ότι αν υπάρχει ένας τέλειος κώδικας επί του $\mathbb{F}$, τότε πρέπει να ισχύει $\lambda \leq 11$, $q \leq 8$ και $n < 485$. Με την βοήθεια υπολογιστού στην αρχή και κατόπιν θεωρητικά απεδείχθη ότι αν υπάρχουν κώδικες των οποίων οι παράμετροι ικανοποιούν τα ανωτέρω φράγματα και οι οποίοι είναι τέλειοι, δηλαδή ισχύει η Πρόταση 1.5.12, τότε αυτοί είναι: Οι τετριμμένοι, οι κώδικες με παραμέτρους ίδιες με τις παραμέτρους των κωδίκων Hamming και Golay, καθώς και κώδικες με παραμέτρους $(90, 2^{78}, 5)$. Αλλά έχουμε ήδη αποδείξει ότι δεν υπάρχουν κώδικες με αυτές τις παραμέτρους.

Εδώ μπορούμε να παρατηρήσουμε ότι η μη ύπαρξη τέλειων κωδίκων με παραμέτρους $(90, 2^{78}, 5)$ απορρέει και από το προηγούμενο θεώρημα, καθότι για $\lambda = 2$ και $n = 90$ $L(x) = 0$, αν και μόνο αν $x^2 - 91x + 2048 = 0$. Η τελευταία όμως εξίσωση δεν έχει ακέραιες λύσεις.

Το Θεώρημα 4.3.3 δίνει μια απάντηση ως προς τους τέλειους κώδικες, αλλά αφήνει πολλά ερωτηματικά.

Προκύπτει, από τον τρόπο κατασκευής των κωδίκων Hamming (ιδέ Παρατήρηση 4.1.4), ότι ένας γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ με τις παραμέτρους ενός κώδικα Hamming είναι ισοδύναμος με τον αντίστοιχο κώδικα Hamming. Αλλά αν ο κώδικας δεν είναι γραμμικός, τότε προκύπτει το εξής πρόβλημα:

Να βρεθούν όλοι οι (μη ισοδύναμοι) μη γραμμικοί κώδικες, οι οποίοι έχουν τις παραμέτρους ενός κώδικα Hamming.

Το πρόβλημα παραμένει ανοικτό. Για παράδειγμα, πιστεύεται ότι υπάρχουν πάρα πολλοί δυαδικοί κώδικες με παραμέτρους $(15, 2^{11}, 3)$.

Από την άλλη πλευρά έχει αποδειχθεί (όπως αναφέρεται και στο Θεώρημα 4.3.3) ότι κάθε κώδικας με τις παραμέτρους ενός από τους κώδικες Golay είναι ισοδύναμος προς έναν από αυτούς.

Ένα άλλο μεγάλο πρόβλημα, το οποίο και αυτό παραμένει ανοικτό, είναι το εξής:

Υπάρχουν τέλειοι κώδικες επί ενός αλφαβήτου του οποίου το πλήθος των στοιχείων δεν είναι δύναμη ενός πρώτου αριθμού;

Σχετικά με το τελευταίο πρόβλημα έχει αποδειχθεί ότι για $\lambda \geq 3$ ο μόνος

μη τετριμμένος τέλειος κώδικας που διορθώνει λ το πλήθος λάθη είναι ο δυαδικός κώδικας Golay. Αλλά οι περιπτώσεις $\lambda = 2$ ή $\lambda = 1$ παραμένουν αναπάντητες.

Εδώ αξίζει να αναφέρουμε ένα μερικό αποτέλεσμα: Δεν υπάρχει κώδικας επί ενός αλφαβήτου με έξι στοιχεία και παραμέτρους $(7, 6^5, 3)$.

Ενδιαφέρον παρουσιάζει μια απόδειξη, όπου η ύπαρξη ενός τέτοιου κώδικα ανάγεται στην επίλυση του γνωστού προβλήματος του Euler των '36 αξιωματικών'. Όπως όμως είναι γνωστόν[1] το πρόβλημα αυτό έχει αρνητική απάντηση, επομένως δεν υπάρχει κώδικας με παραμέτρους $(7, 6^5, 3)$.

4.4 Κώδικες Reed-Muller

Οι κώδικες Reed-Muller είναι από τις πρώτες οικογένειες κωδίκων, οι οποίοι, αν και δεν είναι τόσο αποτελεσματικοί, έχουν χρησιμοποιηθεί εκτενώς, διότι έχουν το πλεονέκτημα της εύκολης αποκωδικοποίησης. Όπως έχουμε ήδη αναφέρει (ιδέ σελ. 11), οι κώδικες Reed-Muller έχουν χρησιμοποιηθεί για την αποστολή ασπρόμαυρων φωτογραφιών από τον πλανήτη Άρη.

Υπάρχουν πολλοί τρόποι για να ορίσουμε τους κώδικες Reed-Muller. Εδώ θα παρουσιάσουμε έναν αναδρομικό τρόπο ορισμού των δυαδικών κωδίκων Reed-Muller.

Ορισμός 4.4.1. *Για κάθε ακέραιο αριθμό $m \geq 1$ ορίζουμε τους κώδικες Reed-Muller πρώτης τάξης και συμβολίζουμε $\mathcal{RM}_1(m) =: \mathcal{RM}(m)$ ως εξής:*

Για $m = 1$ $\mathcal{RM}(1) = \mathbb{Z}_2^2 = \{00, 01, 10, 11\}$.

Για $m \geq 1$ $\mathcal{RM}(m+1) = \mathcal{RM}(m) \odot \mathcal{R}_2(2^m) = \{\mathbf{u}(\mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in \mathcal{RM}(m), \mathbf{v} \in \mathcal{R}_2(2^m)\}$, όπου $\mathcal{R}_2(2^m)$ είναι ο επαναληπτικός δυαδικός κώδικας:

$$\{ \underbrace{00\cdots0}_{2^m-\text{φορές}} , \underbrace{11\cdots1}_{2^m-\text{φορές}} \}.$$

[1] Για περισσότερες πληροφορίες ως προς αυτό το πρόβλημα, όπως και γενικότερα για τα Λατινικά τετράγωνα, ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει σε ένα εγχειρίδιο Συνδυαστικής. Εμείς θα επανέλθουμε για τα Λατινικά Τετράγωνα στο Κεφάλαιο 6.

[Για την $(\mathbf{u}, \mathbf{u}+\mathbf{v})$-κατασκευή που χρησιμοποιούμε για τον ορισμό του κώδικα $\mathcal{RM}(m) \odot \mathcal{R}_2(2^m)$ ιδέ σελ. 50.]

Παράδειγμα 4.4.2. Εφαρμόζοντας τον ορισμό, εύκολα μπορούμε να κατασκευάσουμε τον κώδικα:

$$\mathcal{RM}(2) = \{\, 0000,\, 0011,\, 0101,\, 0110,\, 1010,\, 1001,\, 1111,\, 1100 \,\}.$$

Θεώρημα 4.4.3. *Για κάθε $m \geq 1$ ο κώδικας $\mathcal{RM}(m)$ είναι γραμμικός με παραμέτρους $[2^m, m+1, 2^{m-1}]$. Επίσης κάθε (κωδικο)λέξη, εκτός της $\mathbf{0}$ και $\mathbf{1}$, έχει βάρος ίσο με 2^{m-1}.*

Απόδειξη. Προφανώς ο κώδικας $\mathcal{RM}(1)$ είναι γραμμικός. Υποθέτοντας ότι ο $\mathcal{RM}(m)$ είναι γραμμικός αποδεικνύεται εύκολα ότι και ο $\mathcal{RM}(m+1)$ είναι γραμμικός. Επίσης, από τον ορισμό έπεται ότι το μήκος κάθε (κωδικο)λέξης του $\mathcal{RM}(m+1)$ είναι διπλάσιο από το μήκος κάθε (κωδικο)λέξης του $\mathcal{RM}(m)$, οπότε με επαγωγή έπεται ότι το μήκος του $\mathcal{RM}(m)$ είναι ίσο με 2^m.

Ο κώδικας $\mathcal{RM}(m+1)$ αποτελείται από δύο κατηγορίες στοιχείων. Τα στοιχεία της μορφής $\mathbf{uu}$ με $\mathbf{u} \in \mathcal{RM}(m)$ και τα στοιχεία της μορφής $\mathbf{u}(\mathbf{u}+\mathbf{1})$ με $\mathbf{u} \in \mathcal{RM}(m)$ και $\mathbf{1} = \underbrace{11\cdots1}_{2^m-\text{φορές}}$. Κάθε κατηγορία περιλαμβάνει $|\mathcal{RM}(m)|$ το πλήθος στοιχεία και δεν υπάρχει στοιχείο που να ανήκει και στις δύο κατηγορίες, επομένως $|\mathcal{RM}(m+1)| = 2 \cdot |\mathcal{RM}(m)| = 2 \cdot 2^{m+1}$.

Έστω τώρα ένα στοιχείο $\mathbf{c} \in \mathcal{RM}(m+1)$, το οποίο είναι διάφορο των $\mathbf{0}$ και $\mathbf{1}$. Αν είναι της μορφής $\mathbf{uu}$ με $\mathbf{u} \in \mathcal{RM}(m)$, τότε το $\mathbf{u}$ είναι διάφορο των $\mathbf{0}$ και $\mathbf{1}$ και συνεπώς, υποθέτοντας ότι το βάρος του $\mathbf{u}$ είναι ίσο με 2^{m-1}, έχουμε $w(\mathbf{c}) = 2w(\mathbf{u}) = 2 \cdot 2^{m-1} = 2^m$. Έστω ότι το $\mathbf{c}$ είναι της μορφής $\mathbf{u}(\mathbf{u}+\mathbf{1})$ με $\mathbf{u} \in \mathcal{RM}(m)$. Στην περίπτωση που $\mathbf{u} = \mathbf{0}$ ή $\mathbf{u} = \mathbf{1}$, προφανώς το βάρος του $\mathbf{c} = \mathbf{u}(\mathbf{u}+\mathbf{1})$ είναι ίσο με 2^m. Υποθέτουμε ότι το $\mathbf{u}$ είναι διάφορο των $\mathbf{0}$ και $\mathbf{1}$, τότε $w(\mathbf{c}) = w(\mathbf{u}) + w(\mathbf{u}+\mathbf{1}) = w(\mathbf{u}) + w(\mathbf{u}) + w(\mathbf{1}) - 2w(\mathbf{u} \cap \mathbf{1})$ (ιδέ Πρόταση 1.2.11). Αλλά $\mathbf{u} \cap \mathbf{1} = \mathbf{u}$, οπότε από την προηγούμενη σχέση έχουμε $w(\mathbf{c}) = w(\mathbf{u}) + w(\mathbf{u}) + w(\mathbf{1}) - 2w(\mathbf{u}) = w(\mathbf{1}) = 2^m$. Επομένως, σε όλες τις περιπτώσεις έχουμε $w(\mathbf{c}) = 2^m$ και η απόδειξη τελείωσε. ό.έ.δ.

Αναδρομικά μπορούμε να υπολογίσουμε τους γεννήτορες πίνακες των κωδίκων $\mathcal{RM}(m)$ για $m \geq 1$.

Θεώρημα 4.4.4. *Ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(1)$ είναι ο πίνακας:*

$$\mathrm{R}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Αν R_m είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(m)$, τότε ο πίνακας:

$$\mathrm{R}_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right)$$

είναι γεννήτορας πίνακας του $\mathcal{RM}(m+1)$.

Απόδειξη. Προφανώς ο πίνακας R_1 είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(1)$.

Υποθέτουμε ότι ο πίνακας R_m είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}(m)$. Τότε $\mathcal{RM}(m) = \{\, \mathbf{r} \cdot \mathrm{R}_m \mid \mathbf{r} \in \mathbb{Z}_2^{m+1} \,\}$.

Έστω ένα στοιχείο $\mathbf{u} \in \mathcal{RM}(m)$. Τότε υπάρχει $\mathbf{r} \in \mathbb{Z}_2^{m+1}$, έτσι ώστε $\mathbf{u} = \mathbf{r} \cdot \mathrm{R}_m$. Επισυνάπτοντας στην αρχή του $\mathbf{r}$ την συντεταγμένη 0, το στοιχείο $0\,\mathbf{r}$ ανήκει στο $\mathbb{Z}_2^{m+2}$ και για το στοιχείο $\mathbf{uu} \in \mathcal{RM}(m+1)$ έχουμε ότι:

$$\mathbf{uu} = (0\,\mathbf{r}) \cdot \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right).$$

Επισυνάπτοντας στην αρχή του $\mathbf{r}$ την συντεταγμένη 1, το στοιχείο $1\,\mathbf{r}$ ανήκει στο $\mathbb{Z}_2^{m+2}$ και για το στοιχείο $\mathbf{u}(\mathbf{u}+\mathbf{1}) \in \mathcal{RM}(m+1)$ έχουμε ότι:

$$\mathbf{u}(\mathbf{u}+\mathbf{1}) = (1\,\mathbf{r}) \cdot \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right).$$

Από τα προηγούμενα έπεται ότι $\mathcal{RM}(m+1) \subseteq \{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\}$.

Η τάξη του πίνακα R_{m+1} είναι το πολύ ίση με $m+2$, επομένως ο χώρος $\{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\}$ έχει διάσταση το πολύ ίση με $m+2$, οπότε από την προηγούμενη σχέση έχουμε ότι (αφού η διάσταση του $\mathcal{RM}(m+1)$ είναι ίση με $m+2$) $\mathcal{RM}(m+1) = \{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\}$ και ο πίνακας R_{m+1} είναι γεννήτορας πίνακας του $\mathcal{RM}(m+1)$.

[Επειδή κάθε στοιχείο $\mathbf{c} \in \mathbb{Z}_2^{m+2}$ είναι της μορφής $0\,\mathbf{r}$ ή $1\,\mathbf{r}$ με $\mathbf{r} \in \mathbb{Z}_2^{m+1}$, έχουμε ότι και $\{\, \mathbf{c} \cdot \mathrm{R}_{m+1} \mid \mathbf{c} \in \mathbb{Z}_2^{m+2} \,\} \subseteq \mathcal{RM}(m+1)$.] ό.έ.δ.

Παράδειγμα 4.4.5. Έχοντας ότι ο πίνακας:

$$\mathrm{R}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

είναι γεννήτορας πίνακας του κώδικα $\mathcal{RM}(1)$, οι πίνακες:

$$\mathrm{R}_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{και} \quad \mathrm{R}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

είναι γεννήτορες πίνακες των κωδίκων $\mathcal{RM}(2)$ και $\mathcal{RM}(3)$ αντίστοιχα.

Από τον προηγούμενο αναδρομικό τρόπο κατασκευής των γεννητόρων πινάκων των κωδίκων $\mathcal{RM}(m)$ μπορούμε να συνάγουμε έναν απευθείας τρόπο υπολογισμού των.

Πρόταση 4.4.6. 1) *Η πρώτη γραμμή του πίνακα* R_m *αποτελείται από ένα τμήμα με* 2^{m-1} *το πλήθος 0 και από ένα τμήμα με* 2^{m-1} *το πλήθος 1, δηλαδή είναι της μορφής* $\underbrace{00\cdots0}_{2^{m-1}}\,\underbrace{11\cdots1}_{2^{m-1}}$. *Η δεύτερη γραμμή αποτελείται από δύο τμήματα με* 2^{m-2} *το πλήθος 0 και από δύο τμήματα με* 2^{m-2} *το πλήθος 1, τα οποία εναλλάσσονται μεταξύ τους, δηλαδή είναι της μορφής:*

$$\underbrace{00\cdots0}_{2^{m-2}}\,\underbrace{11\cdots1}_{2^{m-2}}\,\underbrace{00\cdots0}_{2^{m-2}}\,\underbrace{11\cdots1}_{2^{m-2}}.$$

Γενικά η i *γραμμή αποτελείται από τμήματα που αποτελούνται από 0 και από τμήματα που αποτελούνται από 1 μήκους* 2^{m-i}, *τα οποία εναλλάσσονται μεταξύ τους. Οπότε η προτελευταία γραμμή αποτελείται απο εναλλασσόμενα 0 και 1. Απομένει η τελευταία γραμμή, της οποίας όλα τα στοιχεία είναι 1.*

2) *Οι στήλες του* R_m *μπορούν να περιγραφούν ως εξής: Αν εξαιρέσουμε το τελευταίο στοιχείο κάθε στήλης, το οποίο είναι πάντα 1, τότε τα τμήματα που απομένουν αναπαριστούν (διαβάζοντας από άνω προς τα κάτω) κατά σειρά τους αριθμούς* $0, 1, \ldots, 2^m - 1$ *σε δυαδική μορφή.*

Απόδειξη. Η απόδειξη συνίσταται σε απλή παρατήρηση του πίνακα:

$$\mathrm{R}_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{R}_m} & \multicolumn{3}{c}{\mathrm{R}_m} \end{array}\right).$$

ό.έ.δ.

Από τον τρόπο κατασκευής ενός γεννήτορα πίνακα του κώδικα $\mathcal{RM}(m)$, που περιγράψαμε στην προηγούμενη πρόταση, βλέπουμε ότι όλα τα στοιχεία της τελευταίας γραμμής είναι 1. Αυτό σημαίνει ότι ο επαναληπτικός κώδικας $\mathcal{R}_2(2^{m+1})$ μήκους 2^{m+1} περιέχεται ως υποκώδικας του κώδικα $\mathcal{RM}(m)$.

4.4.1 Σύγκριση των κωδίκων Hamming και Reed-Muller

Έστω ότι έχουμε τον δυαδικό κώδικα Hamming $\mathcal{H}(m,\,2)$ με παραμέτρους $[n = 2^m - 1,\, k = 2^m - 1 - m,\, 3]$ και τον κώδικα Reed-Muller $\mathcal{RM}(m)$ με παραμέτρους $[2^m,\, m+1,\, 2^{m-1}]$. Ο δυϊκός κώδικας $\mathcal{H}(m,\,2)^\perp$ έχει παραμέτρους $[n = 2^m - 1,\, m,\, 2^{m-1}]$. Όπως βλέπουμε, αν θέλουμε να συγκρίνουμε δύο κώδικες, προτιμητέο είναι να συγκρίνουμε τον κώδικα $\mathcal{S}(m) =: \mathcal{H}(m,\,2)^\perp$ με τον κώδικα $\mathcal{RM}(m)$ που έχουν *παρεμφερείς* παραμέτρους.

Επεκτείνουμε τον κώδικα Hamming $\mathcal{H}(m,\,2)$ επισυνάπτοντας στην αρχή κάθε στοιχείου του ένα ψηφίο ελέγχου ισοτιμίας[2]. Την επέκταση που προκύπτει τη συμβολίζουμε με $\mathcal{EH}(m,\,2)$. Ο πίνακας Hamming H_m είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{H}(m,\,2)$, επομένως για κάθε $\mathbf{c} \in \mathcal{H}(m,\,2)$ ισχύει $\mathbf{c}\mathrm{H}_m^t = \mathbf{0}$. Δεν είναι δύσκολο να δούμε ότι ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{EH}(m,\,2)$ είναι ο πίνακας:

$$\mathrm{EH}_m = \left(\begin{array}{c|ccc} 0 & & & \\ \vdots & & \mathrm{H}_m & \\ 0 & & & \\ \hline & & & \\ 1 & 1 & \cdots & 1 \end{array}\right).$$

[2] Συνήθως το ψηφίο ελέγχου ισοτιμίας επισυνάπτεται στο τέλος κάθε (κωδικο)λέξης (ιδέ σελ. 44), εδώ το επισυνάπτουμε στην αρχή.

Δηλαδή ο πίνακας EH_m προέρχεται από τον πίνακα H_m, αν επισυνάψουμε μια πρώτη στήλη που αποτελείται από 0 και, κατόπιν, επισυνάψουμε μια τελευταία γραμμή που αποτελείται από 1.

Από τα δύο πρώτα Παραδείγματα 4.1.2 έχουμε ότι οι πίνακες ελέγχου ισοτιμίας για τους κώδικες $\mathcal{EH}(2,\,2)$ και $\mathcal{EH}(3,\,2)$ αντίστοιχα είναι οι πίνακες:

$$\mathrm{EH}_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{και} \quad \mathrm{EH}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Παρατηρούμε ότι:

$$\mathrm{EH}_3 = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{EH}_2} & \multicolumn{3}{c}{\mathrm{EH}_2} \end{array}\right).$$

Η παρατήρηση αυτή ισχύει γενικά για κάθε $m \geq 2$. Πράγματι, από την Πρόταση 4.1.5 έχουμε έναν αναδρομικό τρόπο για τον υπολογισμό του πίνακα H_{m+1}, δηλαδή:

$$\mathrm{H}_{m+1} = \left(\begin{array}{ccc|c|ccc} 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \\ \hline & & & 0 & & & \\ & \mathrm{H}_m & & \vdots & & \mathrm{H}_m & \\ & & & 0 & & & \end{array}\right).$$

Αν τον *συνδυάσουμε* με τον πίνακα:

$$\mathrm{EH}_m = \left(\begin{array}{c|ccc} 0 & & & \\ \vdots & & \mathrm{H}_m & \\ 0 & & & \\ \hline & & & \\ 1 & 1 & \cdots & 1 \end{array}\right),$$

έχουμε ότι:

$$\mathrm{EH}_{m+1} = \left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & \cdots & 1 \\ \hline \multicolumn{3}{c|}{\mathrm{EH}_m} & \multicolumn{3}{c}{\mathrm{EH}_m} \end{array}\right).$$

Στο Παράδειγμα 4.4.5 είχαμε υπολογίσει τους γεννήτορες πίνακες:

$$\mathrm{R}_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{και} \quad \mathrm{R}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

των κωδίκων $\mathcal{RM}(2)$ και $\mathcal{RM}(3)$ αντίστοιχα. Όπως βλέπουμε $\mathrm{R}_2 = \mathrm{EH}_2$ και $\mathrm{R}_3 = \mathrm{EH}_3$. Από το Θεώρημα 4.4.4 και τα προηγούμενα βλέπουμε ότι $\mathrm{R}_m = \mathrm{EH}_m$, για κάθε $m \geq 1$.

Πρόταση 4.4.7. *Ο κώδικας Reed-Muller $\mathcal{RM}(m)$ είναι ίσος με τον δυϊκό κώδικα του επεκταμένου δυαδικού κώδικα Hamming $\mathcal{EH}(m, 2)$.*

Απόδειξη. Οι δύο κώδικες είναι γραμμικοί και έχουν τον ίδιο γεννήτορα πίνακα. ό.έ.δ.

Παρατήρηση 4.4.8. Έχοντας τον κώδικα Reed-Muller $\mathcal{RM}(m)$ εφαρμόζουμε την αντίστροφη διαδικασία. Δηλαδή παίρνουμε μόνο τις (κωδικο)λέξεις που αρχίζουν από 0 και κατόπιν διαγράφουμε το 0 από την πρώτη θέση. Ο κώδικας που προκύπτει από αυτή τη συμπύκνωση δεν είναι παρά ο δυϊκός κώδικας $\mathcal{S}(m) = \mathcal{H}(m, 2)^{\perp}$.

4.4.2 Κώδικες Reed-Muller ανώτερης τάξης

Έχοντας ορίσει τους δυαδικούς κώδικες Reed-Muller $\mathcal{RM}_1(m) = \mathcal{RM}(m)$ πρώτης τάξης για $m \geq 1$, μπορούμε για $2 \leq r \leq m$ να ορίσουμε τους δυαδικούς κώδικες Reed-Muller $r-$τάξης ως εξής:

Ορισμός 4.4.9. *Έστω m θετικός ακέραιος και r μη αρνητικός ακέραιος με $0 \leq r \leq m$. Ορίζουμε ως κώδικα Reed-Muller μηδενικής τάξης και συμβολίζουμε με $\mathcal{RM}_0(m)$ τον επαναληπτικό κώδικα $\mathcal{R}_2(2^m)$ μήκους 2^m. Ως Reed-Muller κώδικα m τάξης, και συμβολίζουμε με $\mathcal{RM}_m(m)$, ορίζουμε ολόκληρο τον χώρο $\mathbb{Z}_2^{2^m}$.*

Για $1 \leq r < m$ ορίζουμε τον Reed-Muller κώδικα r τάξης αναδρομικά ως εξής $\mathcal{RM}_r(m) = \mathcal{RM}_r(m-1) \odot \mathcal{RM}_{r-1}(m-1)$, όπου $\odot$ παριστά την $(\mathbf{u}, \mathbf{u}+\mathbf{v})$- κατασκευή.

Σημειώνουμε ότι ο Ορισμός 4.4.1 για τους κώδικες πρώτης τάξης συνάδει με τον παραπάνω γενικό ορισμό.

Αν θεωρήσουμε τον πίνακα $\mathrm{R}(0,\, m) = (\underbrace{11\cdots 1}_{2^m})$ ως γεννήτορα πίνακα του κώδικα $\mathcal{RM}_0(m)$ και τον πίνακα $\mathrm{R}(m,\, m) = \mathrm{I}_{2^m}$ ως γεννήτορα πίνακα του κώδικα $\mathcal{RM}_m(m)$, τότε για $1 \leq r < m$ ο πίνακας:

$$\mathrm{R}(r,\, m) = \begin{pmatrix} \mathrm{R}(r,\, m-1) & \mathrm{R}(r,\, m-1) \\ \mathbf{0} & \mathrm{R}(r-1,\, m-1) \end{pmatrix}$$

είναι ένας γεννήτορας πίνακας του κώδικα $\mathcal{RM}_r(m)$ (γιατί;). (Ιδέ Άσκηση $2.1.2_{15}$.)

Το επόμενο θεώρημα γενικεύει το Θεώρημα 4.4.3, το οποίο είχε αποδειχθεί για κώδικες Reed-Muller πρώτης τάξης.

Θεώρημα 4.4.10. *Έστω m θετικός ακέραιος και r μη αρνητικός ακέραιος με $0 \leq r \leq m$. Τότε ισχύουν τα ακόλουθα:*

1. *$\mathcal{RM}_i(m) \subseteq \mathcal{RM}_j(m)$ για $0 \leq i \leq j \leq m$.*
2. *Η διάσταση του κώδικα $\mathcal{RM}_r(m)$ ισούται με $\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$.*
3. *Η ελάχιστη απόσταση του κώδικα $\mathcal{RM}_r(m)$ είναι ίση με 2^{m-r}.*
4. *Για τους δυϊκούς των κωδίκων Reed-Muller έχουμε $\mathcal{RM}_m(m)^\perp = \mathbf{0}$ και $\mathcal{RM}_r(m)^\perp = \mathcal{RM}_{m-r-1}(m)$, για $0 \leq r < m$.*

Απόδειξη. 1. Όπως έχουμε παρατηρήσει (μετά την Πρόταση 4.4.6), για κάθε m ο μηδενικής τάξης κώδικας $\mathcal{RM}_0(m)$, ο οποίος είναι ο επαναληπτικός κώδικας μήκους 2^m, περιέχεται στον κώδικα πρώτης τάξης $\mathcal{RM}_1(m)$.

Επίσης, επειδή $\mathcal{RM}_m(m) = \mathbb{Z}_2^m$, απομένει να αποδειχθεί η σχέση για $0 < i \leq j < m$ και $m \geq 2$.

Θα χρησιμοποιήσουμε επαγωγή επί του m.

Υποθέτουμε ότι $\mathcal{RM}_k(m-1) \subseteq \mathcal{RM}_n(m-1)$ για $0 \leq k \leq n \leq m-1$. Έστω $\mathbf{c} \in \mathcal{RM}_i(m)$. Τότε $\mathbf{c} = \mathbf{u}(\mathbf{u}+\mathbf{v}) \mid \mathbf{u} \in \mathcal{RM}_i(m-1),\, \mathbf{v} \in \mathcal{RM}_{i-1}(m-1)$.

Αλλά από την υπόθεση της επαγωγής έχουμε ότι $u \in \mathcal{RM}_j(m-1)$ και $\mathbf{v} \in \mathcal{RM}_{j-1}(m-1)$, δηλαδή $\mathbf{c} = \mathbf{u}(\mathbf{u}+\mathbf{v}) \in \mathcal{RM}_j(m)$.

2. Για $r = 0$ προφανώς η διάσταση του $\mathcal{RM}_0(m)$ είναι ίση με $1 = \binom{m}{0}$. Από το Θεώρημα 4.4.3 έχουμε ότι, για $r = 1$, η διάσταση του $\mathcal{RM}_1(m)$ είναι ίση με $m+1 = \binom{m}{0}+\binom{m}{1}$. Επίσης, για $r = m$ έχουμε ότι η διάσταση του $\mathcal{RM}_m(m) = \mathbb{Z}_2^{2^m}$ είναι ίση με $2^m = \binom{m}{0}+\binom{m}{1}+\cdots+\binom{m}{m}$.

   Θα χρησιμοποιήσουμε επαγωγή επί του m με την υπόθεση ότι $1 < r < m$. Από τον τρόπο κατασκευής ενός γεννήτορα πίνακα του κώδικα $\mathcal{RM}_r(m)$, έχουμε ότι η διάστασή του είναι ίση με το άθροισμα των διαστάσεων του κώδικα $\mathcal{RM}_r(m-1)$ και του κώδικα $\mathcal{RM}_{r-1}(m-1)$. Δηλαδή, βάσει της επαγωγής, $dim(\mathcal{RM}_r(m)) = \binom{m-1}{0}+\binom{m-1}{1}+\cdots+\binom{m-1}{r}+\binom{m-1}{0}+\binom{m-1}{1}+\cdots+\binom{m-1}{r-1}$. Χρησιμοποιώντας τις στοιχειώδεις ιδιότητες $\binom{m}{0} = \binom{m-1}{0}$ και $\binom{m-1}{i-1}+\binom{m-1}{i} = \binom{m}{i}$ έπεται ότι τελικά $dim(\mathcal{RM}_r(m)) = \binom{m}{0}+\binom{m}{1}+\cdots+\binom{m}{r}$.

3. Για $r = 0$ προφανώς η ελάχιστη απόσταση του $\mathcal{RM}_0(m)$ είναι ίση με 2^m. Επίσης, για $r = m$ έχουμε ότι η ελάχιστη απόσταση του $\mathcal{RM}_m(m) = \mathbb{Z}_2^{2^m}$ είναι ίση με $1 = 2^{m-m}$.

   Γενικά έχουμε ορίσει τον κώδικα Reed-Muller r τάξης ως εξής:

$$\mathcal{RM}_r(m) = \mathcal{RM}_r(m-1) \odot \mathcal{RM}_{r-1}(m-1),$$

   όπου $\odot$ παριστά την $(\mathbf{u}, \mathbf{u}+\mathbf{v})$- κατασκευή. Έστω d η ελάχιστη απόσταση του κώδικα $\mathcal{RM}_r(m)$. Από την Πρόταση 1.4.15 έχουμε ότι $d = min(2d_1, d_2)$, όπου d_1 είναι η ελάχιστη απόσταση του $\mathcal{RM}_r(m-1)$ και d_2 είναι η ελάχιστη απόσταση του $\mathcal{RM}_{r-1}(m-1)$. Οπότε το αποτέλεσμα είναι άμεσο με επαγωγή επί του m.

ό.έ.δ.

Πρόταση 4.4.11. *Για κάθε $m \geq 1$ ο κώδικας $\mathcal{RM}_{m-1}(m)$ αποτελείται από όλα τα στοιχεία του $\mathbb{Z}_2^{2^m}$ αρτίου βάρους. Επομένως, για κάθε $r < m$ ο κώδικας $\mathcal{RM}_r(m)$ αποτελείται από στοιχεία αρτίου βάρους.*

Απόδειξη. Απο το προηγούμενο θεώρημα έχουμε ότι $\mathcal{RM}_i(m) \subseteq \mathcal{RM}_j(m)$ για $0 \leq i \leq j \leq m$. Επομένως, αν αποδείξουμε το πρώτο μέρος της πρότασης, το υπόλοιπο είναι προφανές.

Προφανώς για $m = 1$ έχουμε ότι ο κώδικας $\mathcal{RM}_0(1) = \{00, 11\}$ αποτελείται από όλες τις λέξεις μήκους 2 αρτίου βάρους. Υποθέτουμε ότι ο κώδικας $\mathcal{RM}_{m-2}(m-1)$ αποτελείται από όλες τις λέξεις μήκους 2^{m-1} αρτίου βάρους. Από τον τρόπο ορισμού των κωδίκων Reed-Muller $(m-1)$–τάξης έχουμε ότι $\mathcal{RM}_{m-1}(m) = \mathcal{RM}_{m-1}(m-1) \odot \mathcal{RM}_{m-2}(m-1)$. Επομένως, ένα στοιχείο του κώδικα $\mathcal{RM}_{m-1}(m)$ είναι της μορφής $\mathbf{u}(\mathbf{u}+\mathbf{v}) = \mathbf{uu}+\mathbf{0v}$ με $\mathbf{u} \in \mathcal{RM}_{m-1}(m-1)$ και $\mathbf{v} \in \mathcal{RM}_{m-2}(m-1)$. Το στοιχείο $\mathbf{uu}$ έχει άρτιο βάρος και το στοιχείο $\mathbf{v}$ έχει άρτιο βάρος από την υπόθεση, επομένως και το στοιχείο $\mathbf{0v}$ έχει άρτιο βάρος. Άρα, για το βάρος του στοιχείου $\mathbf{u}(\mathbf{u}+\mathbf{v}) = \mathbf{uu}+\mathbf{0v}$ έχουμε $w(\mathbf{uu}+\mathbf{0v}) = w(\mathbf{uu}) + w(\mathbf{0v}) - 2w(\mathbf{uu} \cap \mathbf{0v})$, το οποίο είναι άρτιο. Η διάσταση του κώδικα $\mathcal{RM}_{m-1}(m)$ είναι ίση με $2^m - 1$, επομένως αποτελείται από όλες τις λέξεις μήκους 2^m αρτίου βάρους. ό.έ.δ.

Στην Πρόταση 4.4.7 είχαμε αποδείξει ότι ο δυϊκός κώδικας ενός κώδικα Reed-Muller πρώτης τάξης ισούται με τον επεκταταμένο δυαδικό κώδικα Hamming.

Έστω m ένας θετικός ακέραιος. Από τον ορισμό έχουμε ότι ο κώδικας Reed-Muller $\mathcal{RM}_m(m)$, τάξης m, ισούται με όλοκληρο τον χώρο $\mathbb{Z}_2^{2^m}$. Επομένως, για τον δυϊκό κώδικα έχουμε $\mathcal{RM}_m(m)^\perp = \mathbf{0}$.

Επίσης, από τον ορισμό έχουμε ότι ο κώδικας Reed-Muller $\mathcal{RM}_0(m)$, τάξης 0, ισούται με τον δυαδικό επαναληπτικό κώδικα μήκους 2^m. Όπως εύκολα βλέπουμε (ιδέ και Άσκηση $2.2.3_4$), ο δυϊκός κώδικας $\mathcal{RM}_0(m)^\perp$ αποτελείται από όλα τα στοιχεία του $\mathbb{Z}_2^{2^m}$ αρτίου βάρους. Οπότε από την προηγούμενη πρόταση έχουμε ότι $\mathcal{RM}_0(m)^\perp = \mathcal{RM}_{m-1}(m)$.

Έστω τώρα r ένας μη αρνητικός ακέραιος με $0 \leq r \leq m$. Θα δούμε τι ισχύει για τους δυϊκούς κώδικες $\mathcal{RM}_r(m)^\perp$. Από τα προηγούμενα μπορούμε να υποθέσουμε ότι $0 < r < m$.

Έστω $\mathcal{RM}_{m-r-1}(m)$ ο κώδικας Reed-Muller τάξης $m-r-1$. Θα δείξουμε ότι κάθε στοιχείο του είναι κάθετο με όλα τα στοιχεία του κώδικα Reed-Muller $\mathcal{RM}_r(m)$. Δηλαδή $\mathcal{RM}_{m-r-1}(m) \subseteq \mathcal{RM}_r(m)^\perp$.

Υποθέτουμε ότι ο ισχυρισμός ισχύει για το $m-1$. Δηλαδή ότι:

$$\mathcal{RM}_{(m-1)-r-1}(m-1) \subseteq \mathcal{RM}_r(m-1)^{\perp}.$$

Ένα στοιχείο $\mathbf{x} \in \mathcal{RM}_{m-r-1}(m)$ είναι της μορφής $\mathbf{x} = \mathbf{a}(\mathbf{a}+\mathbf{b})$ και ένα στοιχείο $\mathbf{y} \in \mathcal{RM}_r(m)$ είναι της μορφής $\mathbf{y} = \mathbf{u}(\mathbf{u}+\mathbf{v})$, όπου $\mathbf{a} \in \mathcal{RM}_{m-r-1}(m-1)$, $\mathbf{b} \in \mathcal{RM}_{m-r-2}(m-1)$, $\mathbf{u} \in \mathcal{RM}_r(m-1)$ και $\mathbf{v} \in \mathcal{RM}_{r-1}(m-1)$.

Από τις ιδιότητες του εσωτερικού γινομένου έπεται ότι $\langle \mathbf{x}, \mathbf{y} \rangle = 2\langle \mathbf{a}, \mathbf{u} \rangle + \langle \mathbf{a}, \mathbf{v} \rangle + \langle \mathbf{b}, \mathbf{u} \rangle + \langle \mathbf{b}, \mathbf{v} \rangle = \langle \mathbf{a}, \mathbf{v} \rangle + \langle \mathbf{b}, \mathbf{u} \rangle + \langle \mathbf{b}, \mathbf{v} \rangle$. Από την υπόθεση της επαγωγής έχουμε ότι $\langle \mathbf{a}, \mathbf{v} \rangle = \langle \mathbf{b}, \mathbf{u} \rangle = \langle \mathbf{b}, \mathbf{v} \rangle = 0$. Συνεπώς $\langle \mathbf{x}, \mathbf{y} \rangle = 0$.

Άρα πράγματι $\mathcal{RM}_{m-r-1}(m) \subseteq \mathcal{RM}_r(m)^{\perp}$.

Από το Θεώρημα 4.4.10 έχουμε ότι $dim(\mathcal{RM}_r(m)) + dim(\mathcal{RM}_{m-r-1}(m)) = 2^m$. Επομένως, τελικά $\mathcal{RM}_{m-r-1}(m) = \mathcal{RM}_r(m)^{\perp}$.

Παρατήρηση 4.4.12. Στην προηγούμενη επιχειρηματολογία, υπάρχει η περίπτωση όπου $r = m-1$, οπότε $(m-1)-r-1 = -1$. Δηλαδή ο κώδικας $\mathcal{RM}_{(m-1)-r-1}(m-1)$ είναι *αρνητικής* τάξης. Αυτό δεν δημιουργεί πρόβλημα, καθότι μπορούμε να θεωρήσουμε, εξορισμού, ότι $\mathcal{RM}_{(m-1)-r-1}(m-1) = \mathbf{0}$ κάτι που συνάδει με το ότι $\mathcal{RM}_{(m-1)}(m-1)^{\perp} = (\mathbb{Z}_2^{2^{(m-1)}})^{\perp} = \mathbf{0}$. Για τον λόγο αυτό, άλλωστε, εξετάσαμε στην αρχή τις ακραίες περιπτώσεις για τους κώδικες $\mathcal{RM}_0(m)$ και $\mathcal{RM}_m(m)$.

Τα προηγούμενα συνοψίζονται στην επομένη πρόταση.

Πρόταση 4.4.13. *Έστω m ένας θετικός ακέραιος και r ένας μη αρνητικός ακέραιος με $0 \leq r \leq m$. Τότε ισχύει $\mathcal{RM}_m(m)^{\perp} = \mathbf{0}$ και για $r \neq m$ $\mathcal{RM}_r(m)^{\perp} = \mathcal{RM}_{m-r-1}(m)$.*

4.4.3 Ασκήσεις

1. Δείξτε ότι ο γεννήτορας πίνακας ενός κώδικα Reed-Muller πρώτης τάξης, που κατασκευάζεται βάσει της Πρότασης 4.4.6 και ο γεννήτορας πίνακας, που κατασκεάζεται βάσει του Ορισμού 4.4.9, αποτελούν γεννήτορες πίνακες του ιδίου κώδικα.

2. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{RM}(2)$ και για τον κώδικα $\mathcal{RM}(3)$.

3. Ποίοι από τους κώδικες Reed-Muller είναι αυτοδυϊκοί; Ποίοι είναι μέγιστης απόστασης;

4. Εξετάστε αν ένας κώδικας Reed-Muller ικανοποιεί το άνω φράγμα του Plotkin (Θεώρημα 1.5.25) με ισότητα.

5. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

4.5 "Διττοί" Κώδικες

Μια ενδιαφέρουσα κατηγορία κυκλικών κωδίκων είναι οι κώδικες τετραγωνικών υπολοίπων. Οι κώδικες αυτοί υπάγονται σε μια γενικότερη κατηγορία κωδίκων, οι οποίοι ονομάζονται διττοί κωδικες, καθότι εμφανίζονται ως *αλληλοσυμπληρούμενα* ζεύγη κωδίκων.

Στην παράγραφο αυτή θα παρουσιάσουμε έναν τρόπο κατασκευής, καθώς και ορισμένες ιδιότητες των διττών κωδίκων.

Ως γνωστόν ένας κώδικας $\mathcal{C}$ επί ενός πεπερασμένου σώματος $\mathbb{F}$ ονομάζεται κώδικας μηδενικού αθροίσματος αν το άθροισμα των χαρακτήρων κάθε (κωδικο)λέξης ισούται με μηδέν, διαφορετικά ονομάζεται κώδικας μη μηδενικού αθροίσματος. Στην περίπτωση, όπου έχουμε δυαδικούς κώδικες, προφανώς ένας κώδικας είναι μηδενικού αθροίσματος, αν και μόνο αν το πλήθος των μονάδων που εμφανίζονται ως χαρακτήρες σε κάθε (κωδικο)λέξη είναι άρτιο, διαφορετικά, ένας κώδικας είναι μη μηδενικού αθροίσματος, αν και μόνο αν υπάρχει (τουλάχιστον) μια (κωδικο)λέξη με περιττό πλήθος μονάδων.

Τις περισσότερες φορές οι διάφορες κατηγορίες κωδίκων έχουν ορισθεί επί του $\mathbb{Z}_2$ και μετά γενικεύθηκαν επί τυχαίου πεπερασμένου σώματος. Για τον λόγο αυτό έχει καθιερωθεί ένας κώδικας μηδενικού αθροίσματος να ονομάζεται **άρτιος** κώδικας και ένας κώδικας μη μηδενικού αθροίσματος να ονομάζεται **περιττός** κώδικας, ορολογία την οποία θα χρησιμοποιούμε στο εξής.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας φυσικός αριθμός πρώτος προς τον q. Ως συνήθως, συμβολίζουμε με $\mathcal{R}_n$ τον

δακτύλιο πηλίκων $\mathbb{F}[x]/\langle x^n - 1\rangle$. Έστω $x^n - 1 = (x-1)\varphi(x)$, όπου $\varphi(x) = x^{n-1} + x^{n-2} + \cdots x + 1$ και $\vartheta(x) = (1/n)\varphi(x)$[3].

Ένα πολυώνυμο $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R}_n$ θα ονομάζεται άρτιο αν το άθροισμα των συντελεστών του ισούται με μηδέν, διαφορετικά θα ονομάζεται περιττό.

Στο επόμενο λήμμα έχουμε συγκεντρώσει διάφορα αποτελέσματα, τα οποία βρίσκονται *διάσπαρτα* στο κεφάλαιο που αναφέρεται στους κυκλικούς κώδικες, αλλά εδώ θα τα επικαλούμαστε συχνά.

Λήμμα 4.5.1. *Με τις προηγούμενες υποθέσεις, έστω $\mathcal{E}_n$ ο κυκλικός κώδικας που αποτελείται από όλες τις λέξεις μηδενικού αθροίσματος. Τότε ισχύουν τα εξής:*

1. *Ο δυϊκός κώδικας $\mathcal{E}_n^{\perp}$ είναι ο επαναληπτικός κώδικας μήκους n επί του σώματος $\mathbb{F}$ και έχει αδύναμο γεννήτορα το πολυώνυμο $\vartheta(x)$.*

2. *Ο κώδικας $\mathcal{E}_n$ έχει αδύναμο γεννήτορα το πολυώνυμο $1 - \vartheta(x)$.*

3. *Έστω $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R}_n$.*

   Το $f(x)$ είναι άρτιο, αν και μόνο αν $f(1) = 0$ αν και μόνο αν $f(x)\vartheta(x) = 0$.

   Το $f(x)$ είναι περιττό, αν και μόνο αν $f(1) \neq 0$ αν και μόνο αν $f(x)\vartheta(x) = \alpha\vartheta(x)$, όπου α είναι ένα μη μηδενικό στοιχείο του σώματος $\mathbb{F}$.

4. *Έστω $\mathcal{C} \subseteq \mathcal{R}_n$ ένας κυκλικός κώδικας με πολυώνυμο γεννήτορα $\gamma(x)$.*

   Ο κώδικας $\mathcal{C}$ είναι άρτιος, αν και μόνο αν $\gamma(1) = 0$, αν και μόνο αν $\vartheta(x) \notin \mathcal{C}$.

   Ο κώδικας $\mathcal{C}$ είναι περιττός, αν και μόνο αν $\gamma(1) \neq 0$, αν και μόνο αν $\vartheta(x) \in \mathcal{C}$.

Απόδειξη. Όπως προαναφέραμε, η απόδειξη βρίσκεται *διάχυτη* στο κεφάλαιο που αναφέρεται στους κυκλικούς κώδικες. Βλέπε για παράδειγμα το Θεώ-

[3]Το $1/n$ παριστά το αντίστροφο του $n \cdot 1_{\mathbb{F}}$ στο σώμα $\mathbb{F}$.

ρημα 3.2.21, το Πόρισμα 3.2.37 και τις Ασκήσεις 3.2.5 5, 6, 7, 8, 9, 21, 24, 25. ό.έ.δ.

Υπενθυμίζουμε (ιδέ σελίδα 110) ότι για έναν φυσικό αριθμό n και κάθε ακέραιο a πρώτο προς τον n η απεικόνιση $\varrho_a(i) = ia \bmod n \; i = 1, 2, \ldots, n$ ορίζει μια μετάθεση σε n σύμβολα, η οποία ονομάζεται πολλαπλασιαστής.

Έστω $\mathcal{C}$ ένας κυκλικός κώδικας. Η μετάθεση ϱ_a ορίζει τον μεταθετικά ισοδύναμο κώδικα $\mathcal{C}_{\varrho_a}$, ο οποίος είναι και αυτός κυκλικός (ιδέ Πρόταση 3.2.38).

Τώρα είμαστε σε θέση να ορίσουμε τους διττούς κώδικες.

Ορισμός 4.5.2. *Έστω $\epsilon_1(x)$ και $\epsilon_2(x)$ δύο άρτια αδύναμα στοιχεία του δακτυλίου $\mathcal{R}_n = \mathbb{F}[x]/\langle x^n - 1\rangle$ και $\mathcal{C}_1 = [[\epsilon_1(x)]]$, $\mathcal{C}_2 = [[\epsilon_2(x)]]$ οι κυκλικοί κώδικες που έχουν αντίστοιχα τα $\epsilon_1(x)$ και $\epsilon_2(x)$ ως αδύναμους γεννήτορες. Οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ αποτελούν ένα* ***ζεύγος αρτίων διττών*** *κωδίκων, αν ικανοποιούνται οι ακόλουθες συνθήκες:*

(α) $\epsilon_1(x) + \epsilon_2(x) = 1 - \vartheta(x) = 1 - (1/n) \cdot (x^{n-1} + x^{n-2} + \cdots x + 1)$.

(β) *Υπάρχει πολλαπλασιαστής ϱ_a, έτσι ώστε $(\mathcal{C}_1)_{\varrho_a} = \mathcal{C}_2$ και $(\mathcal{C}_2)_{\varrho_a} = \mathcal{C}_1$.*

Οι κώδικες $\mathcal{D}_1 = [[1 - \epsilon_2(x)]]$ και $\mathcal{D}_2 = [[1 - \epsilon_1(x)]]$ αποτελούν το αντίστοιχο ***ζεύγος περιττών διττών*** *κωδίκων.*

Παρατηρήσεις 4.5.3.

1. Επειδή τα $\epsilon_i(x)$ $i = 1, 2$ έχουν υποτεθεί άρτια έχουμε ότι $\epsilon_i(1) = 0$, συνεπώς για κάθε $f_i(x) \in \mathcal{C}_i$ έχουμε ότι $f_i(1) = 0$. Επομένως, οι κώδικες $\mathcal{C}_i$ είναι πράγματι άρτιοι και οι κώδικες $\mathcal{D}_i$ είναι πράγματι περιττοί.

2. Η συνθήκη (β) στον ορισμό προφανώς είναι ισοδύναμη με τη συνθήκη: $\varrho_a(\epsilon_1(x)) = \epsilon_2(x)$ και $\varrho_a(\epsilon_2(x)) = \epsilon_1(x)$.

   Ο πολλαπλασιαστής ϱ_a επιτελεί τον *διαχωρισμό* και ταυτόχρονα την *σύνδεση* μεταξύ των δύο κωδίκων. (Στα επόμενα θα δούμε υπό ποίαν έννοια εννοούμε τον διαχωρισμό).

3. Αν υποθέσουμε ότι οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ αποτελούν ένα ζεύγος αρτίων διττών κωδίκων και ότι οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}'_2$ αποτελούν ένα (άλλο) ζεύγος αρτίων διττών κωδίκων, τότε είναι εύκολο να δούμε ότι $\mathcal{C}_2 = \mathcal{C}'_2$.

Συνεπώς, δεν υπάρχει *αβεβαιότητα* ως προς το *ταίρι* του καθενός από τους δύο κώδικες.

4. Μια συνθήκη ανάλογη με τη συνθήκη (β) ισχύει και για το ζεύγος των περιττών διττών κωδίκων $\mathcal{D}_1$ και $\mathcal{D}_2$. Δηλαδή $(\mathcal{D}_1)_{\varrho_a} = \mathcal{D}_2$ και $(\mathcal{D}_2)_{\varrho_a} = \mathcal{D}_1$.

   Πράγματι, από τον ορισμό έχουμε ότι $\mathcal{D}_1 = [[1-\epsilon_2(x)]]$ και $\mathcal{D}_2 = [[1-\epsilon_1(x)]]$. Από την δεύτερη παρατήρηση όμως έχουμε ότι $\varrho_a(1-\epsilon_1(x)) = 1-\varrho_a(\epsilon_1(x)) = 1-\epsilon_2(x)$, το οποίο αποδεικνύει τον ισχυρισμό.

Στο επόμενο θεώρημα συνοψίζονται μερικές από τις βασικές ιδιότητες των διττών κωδίκων.

Θεώρημα 4.5.4. *Έστω $\mathcal{C}_1 = [[\epsilon_1(x)]]$, $\mathcal{C}_2 = [[\epsilon_2(x)]]$ ένα ζεύγος αρτίων διττών κωδίκων μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Υποθέτουμε ότι ο πολλαπλασιαστής ϱ_a επιτελεί τον διαχωρισμό των δύο κωδίκων και ότι οι κώδικες $\mathcal{D}_1$ και $\mathcal{D}_2$ είναι το αντίστοιχο ζεύγος περιττών διττών κωδίκων. Τότε ισχύουν τα ακόλουθα.*

1. *$\epsilon_1(x) \cdot \epsilon_2(x) = 0$.*

2. *Ο κυκλικός κώδικας $\mathcal{E}_n$, που αποτελείται από όλες τις λέξεις μηδενικού αθροίσματος, είναι το ευθύ άθροισμα των $\mathcal{C}_1$ και $\mathcal{C}_2$.*

3. *Το μήκος n είναι περιττός αριθμός και η διάσταση καθενός από τους $\mathcal{C}_1$ και $\mathcal{C}_2$ ισούται με $(n-1)/2$.*

4. *Ο κώδικας $\mathcal{D}_1$ είναι το κυκλικό συμπλήρωμα του $\mathcal{C}_2$ και ο κώδικας $\mathcal{D}_2$ είναι το κυκλικό συμπλήρωμα του $\mathcal{C}_1$. Οπότε η διάσταση καθενός από τους $\mathcal{D}_1$ και $\mathcal{D}_2$ ισούται με $(n+1)/2$.*

5. *Ο κώδικας $\mathcal{C}_i$ αποτελείται από όλα τα άρτια στοιχεία του $\mathcal{D}_i$, $i = 1, 2$.*

6. *$\mathcal{D}_i = \mathcal{C}_i + [[\vartheta(x)]]$, όπου $\vartheta(x) = (1/n)(x^{n-1}+x^{n-2}+\cdots x+1)$, $i = 1, 2$.*

7. *$\mathcal{D}_1 \cap \mathcal{D}_2 = [[\vartheta(x)]]$ και $\mathcal{D}_1 + \mathcal{D}_2 = \mathcal{R}_n$.*

Απόδειξη. 1. Από τη συνθήκη (α) έχουμε $\epsilon_1(x)+\epsilon_2(x)=1-\vartheta(x)$, οπότε πολλαπλασιάζοντας και τα δύο μέλη με το πολυώνυμο $\epsilon_1(x)$ έπεται το αποτέλεσμα από το (3) του Λήμματος 4.5.1.

2. Το αποτέλεσμα είναι άμεσο από την Πρόταση 3.2.32 και το (2) του Λήμματος 4.5.1.

3. Οι δύο κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ είναι (μεταθετικά) ισοδύναμοι, άρα ισοδιάστατοι. Επομένως, το αποτέλεσμα έπεται από το προηγούμενο.

4. Το αποτέλεσμα είναι άμεσο από τον ορισμό και το Πόρισμα 3.2.37.

5. Από την Άσκηση 3.2.5 $_{26}$ έχουμε ότι ο υποκώδικας του $\mathcal{D}_1$, που αποτελείται από τα άρτια στοιχεία, έχει ως αδύναμο γεννήτορα το πολυώνυμο $1-\epsilon_2(x)-\vartheta(x)=\epsilon_1(x)$. Οπότε έπεται ο ισχυρισμός.

6. Από τη σχέση $\epsilon_1(x)+\epsilon_2(x)=1-\vartheta(x)$ έπεται άμεσα ο ισχυρισμός.

7. Από την Πρόταση 3.2.32 έπεται άμεσα ο ισχυρισμός, δεδομένου ότι το 1 είναι αδύναμος γεννήτορας του $\mathcal{R}_n$.

ό.έ.δ.

Παραδείγματα 4.5.5. 1. Έστω $\epsilon_1(x)=1+x+x^2+x^4$, $\epsilon_2(x)=1+x^3+x^5+x^6\in\mathcal{R}_7=\mathbb{Z}_2[x]/\langle x^7-1\rangle$. Τα πολυώνυμα αυτά είναι αδύναμα. (Να κάνετε τον έλεγχο! Ιδέ και Άσκηση 3.2.5 $_{12}$.)

Παρατηρούμε ότι $\epsilon_1(x)+\epsilon_2(x)=x+x^2+x^3+x^4+x^5+x^6=1-\vartheta(x)$. Επίσης, παρατηρούμε ότι $\varrho_3(\epsilon_1(x))=\epsilon_2(x)$ και $\varrho_3(\epsilon_2(x))=\epsilon_1(x)$.

Επομένως, οι κώδικες $\mathcal{C}_1=[[\epsilon_1(x)]]$ και $\mathcal{C}_2=[[\epsilon_2(x)]]$ αποτελούν ένα ζεύγος αρτίων διττών κωδίκων, με αντίστοιχους περιττούς διττούς κώδικες το ζεύγος $\mathcal{D}_1=[[1-\epsilon_2(x)]]$ και $\mathcal{D}_2=[[1-\epsilon_1(x)]]$.

2. Έστω $\epsilon_1(x)=1+x+x^3+x^4+x^5+x^9$, $\epsilon_2(x)=1+x^2+x^6+x^7+x^8+x^{10}\in\mathcal{R}_{11}=\mathbb{Z}_3[x]/\langle x^{11}-1\rangle$. Τα πολυώνυμα αυτά είναι αδύναμα. (Να κάνετε τον έλεγχο! Ιδέ και Άσκηση 3.2.5 $_{13}$.)

Παρατηρούμε ότι $\epsilon_1(x)+\epsilon_2(x)=-1+x+x^2+\cdots+x^{10}=1-\vartheta(x)$. Επίσης, παρατηρούμε ότι $\varrho_2(\epsilon_1(x))=\epsilon_2(x)$ και $\varrho_2(\epsilon_2(x))=\epsilon_1(x)$.

Επομένως, οι κώδικες $\mathcal{C}_1 = [[\epsilon_1(x)]]$ και $\mathcal{C}_2 = [[\epsilon_2(x)]]$ αποτελούν ένα ζεύγος αρτίων διττών κωδίκων, με αντίστοιχους περιττούς διττούς κώδικες το ζεύγος $\mathcal{D}_1 = [[1-\epsilon_2(x)]]$ και $\mathcal{D}_2 = [[1-\epsilon_1(x)]]$.

Έστω $\mathcal{C}_1 = [[\epsilon_1(x)]]$ και $\mathcal{C}_2 = [[\epsilon_2(x)]]$ ένα ζεύγος αρτίων διττών κωδίκων με αντίστοιχο ζεύγος περιττών διττών κωδίκων $\mathcal{D}_1 = [[1-\epsilon_2(x)]]$ και $\mathcal{D}_2 = [[1-\epsilon_1(x)]]$. Μπορούμε, από την Παρατήρηση 3.2.29$_1$, να υπολογίσουμε τα αντίστοιχα πολυώνυμα γεννήτορες. Εδώ θα δούμε πώς σχετίζονται τα πολυώνυμα γεννήτορες σε ζεύγη διττών κωδίκων.

Έστω $\mathcal{C}_1$, $\mathcal{C}_2$ ένα ζεύγος αρτίων διττών κωδίκων μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Υποθέτουμε ότι ο πολλαπλασιαστής ϱ_a επιτελεί τον διαχωρισμό των δύο κωδίκων.

Έστω $\gamma_1(x) = (x-1)g_1(x)$ και $\gamma_2(x) = (x-1)g_2(x)$ τα πολυώνυμα γεννήτορες των $\mathcal{C}_1$ και $\mathcal{C}_2$ αντίστοιχα. Από το Θεώρημα 4.5.4$_2$ και την Πρόταση 3.2.14 έχουμε ότι $x^n - 1 = (x-1)g_1(x)g_2(x)$ με τα $g_1(x)$ και $g_2(x)$ να είναι σχετικά πρώτα.

Επίσης, έχουμε ότι $(\mathcal{C}_1)_{\varrho_a} = \mathcal{C}_2$ και $(\mathcal{C}_2)_{\varrho_a} = \mathcal{C}_1$. Αυτό σημαίνει ότι το πολυώνυμο $\varrho_a((x-1)g_1(x))$ παράγει τον κώδικα $\mathcal{C}_2$ [Προσοχή! δεν είναι (κατ' ανάγκη) το πολυώνυμο γεννήτορας.] Επομένως, από την Πρόταση 3.2.8 έχουμε ότι τα πολυώνυμα $\varrho_a((x-1)g_1(x)) = (x^a-1)g_1(x^a)$ και $\gamma_2(x) = (x-1)g_2(x)$ έχουν το ίδιο σύνολο ριζών. Αλλά το ξ είναι ρίζα του $\gamma_1(x) = (x-1)g_1(x)$, αν και μόνο αν το $\xi^{a^{-1}}$ είναι ρίζα του $\varrho_a((x-1)g_1(x)) = (x^a-1)g_1(x^a)$.

Από τα προηγούμενα συνάγουμε την εξής πρόταση.

Πρόταση 4.5.6. *Έστω $\mathcal{C}_1$, $\mathcal{C}_2$ ένα ζεύγος αρτίων διττών κωδίκων μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία με πολυώνυμα γεννήτορες $\gamma_1(x) = (x-1)g_1(x)$ και $\gamma_2(x) = (x-1)g_2(x)$ αντίστοιχα. Υποθέτουμε ότι ο πολλαπλασιαστής ϱ_a επιτελεί τον διαχωρισμό των δύο κωδίκων και έστω ω μια n-οστη πρωταρχική ρίζα της μονάδος επί του σώματος $\mathbb{F}$.*

Τότε το σύνολο $E = \{\omega, \omega^2, \ldots, \omega^{n-1}\}$ είναι το σύνολο ριζών του πολυωνύμου $g_1(x)g_2(x)$ και υπάρχουν δύο, ξένα μεταξύ τους, υποσύνολα E_1 και E_2 του E, καθένα με $(n-1)/2$ το πλήθος στοιχεία, έτσι ώστε

$\varrho_b(E_1) = \{\omega^{ib} \mid \omega^i \in E_1\} = E_2$ *και* $\varrho_b(E_2) = \{\omega^{jb} \mid \omega^j \in E_2\} = E_1$, *όπου* $b = a^{-1}$ *είναι ο αντίστροφος του* $a \mod n$.

Απόδειξη. Η απόδειξη έχει προηγηθεί με τις λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Πριν διατυπώσουμε και αποδείξουμε το αντίστροφο της προηγουμένης πρότασης ας παρατηρήσουμε τα εξής:

Παρατήρηση 4.5.7. Έστω $S = \{i \mid \omega^i \in E\}$ και $S_1 = \{i \mid \omega^i \in E_1\}$, $S_2 = \{i \mid \omega^i \in E_2\}$.

Ο πολλαπλασιαστής ϱ_b *διαχωρίζει/διαμερίζει* το σύνολο των ακεραίων αριθμών $S = \{1, 2, \ldots, n-1\}$ στα δύο υποσύνολα S_1, S_2, έτσι ώστε:

1. $S_1 \cup S_2 = \{1, 2, \ldots, n-1\}$
2. $S_1 \cap S_2 = \emptyset$
3. $\varrho_b(S_1) = \{ib \mod n \mid i \in S_1\} = S_2$ και $\varrho_b(S_2) = \{jb \mod n \mid j \in S_2\} = S_1$
4. Τα πολυώνυμα $g_1(x) = \prod_{i \in S_1}(x - \omega^i)$ και $g_2(x) = \prod_{j \in S_2}(x - \omega^j)$ έχουν συντελεστές στο σώμα $\mathbb{F}$.

Πρόταση 4.5.8. *Έστω* $\mathbb{F}$ *ένα πεπερασμένο σώμα με* q *το πλήθος στοιχεία,* n *ένας φυσικός αριθμός πρώτος προς τον* q *και* ω *μια* n*-οστή πρωταρχική ρίζα της μονάδος.*

Υποθέτουμε ότι υπάρχει ένας πολλαπλασιαστής ϱ_b*, ο οποίος διαμερίζει το σύνολο των ακεραίων αριθμών* $S = \{1, 2, \ldots, n-1\}$ *σε δύο υποσύνολα* S_1, S_2*, τα οποία ικανοποιούν τις παραπάνω ιδιότητες.*

Τότε υπάρχει ένα ζεύγος αρτίων διττών κωδίκων $\mathcal{C}_1$ *και* $\mathcal{C}_2$*, μήκους* n *επί του σώματος* $\mathbb{F}$*, με πολυώνυμα γεννήτορες* $\gamma_1(x) = (x-1)g_1(x)$ *και* $\gamma_2(x) = (x-1)g_2(x)$ *αντίστοιχα και σύνολα ριζών για τα πολυώνυμα* $g_1(x)$ *και* $g_2(x)$ *τα σύνολα* $E_1 = \{\omega^i \mid i \in S_1\}$ *και* $E_2 = \{\omega^j \mid j \in S_2\}$.

Απόδειξη. Οι κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$ με πολυώνυμα γεννήτορες $\gamma_1(x) = (x-1)g_1(x)$ και $\gamma_2(x) = (x-1)g_2(x)$ αντίστοιχα και σύνολα ριζών για τα πολυώνυμα $g_1(x)$ και $g_2(x)$ τα σύνολα $E_1 = \{\omega^i \mid i \in S_1\}$ και $E_2 = \{\omega^j \mid j \in S_2\}$

προφανώς είναι άρτιοι. Θα δείξουμε ότι πληρούν τις ιδιότητες του Ορισμού 4.5.2.

Έστω $\epsilon_1(x)$ και $\epsilon_2(x)$ οι αδύναμοι γεννήτορες των $\mathcal{C}_1$ και $\mathcal{C}_2$ αντίστοιχα. Από τις Προτάσεις 3.2.32 και 3.2.14 έχουμε ότι:
Η τομή $\mathcal{C}_1 \cap \mathcal{C}_2$ έχει ως αδύναμο γεννήτορα το πολυώνυμο $\epsilon_1(x)\epsilon_2(x)$ και ως πολυώνυμο γεννήτορα το πολυώνυμο $(x-1)g_1(x)g_2(x) = 0 \in \mathcal{R}_n$. Συνεπώς, $\epsilon_1(x)\epsilon_2(x) = 0$.

Το άθροισμα $\mathcal{C}_1 + \mathcal{C}_2$ έχει ως αδύναμο γεννήτορα το πολυώνυμο $\epsilon_1(x) + \epsilon_2(x) - \epsilon_1(x)\epsilon_2(x) = \epsilon_1(x) + \epsilon_2(x)$ και ως πολυώνυμο γεννήτορα το πολυώνυμο $x-1$.

Οπότε, προφανώς, έχουμε ότι $\epsilon_1(x) + \epsilon_2(x) = 1 - \vartheta(x)$, όπου $\vartheta(x) = (1/n)(x^{n-1} + x^{n-2} + \cdots x + 1)$.

Από την υπόθεση έχουμε ότι $\varrho_b(S_1) = \{ ib \bmod n \mid i \in S_1 \} = S_2$ και $\varrho_b(S_2) = \{ jb \bmod n \mid j \in S_2 \} = S_1$. Αυτό σημαίνει ότι $\varrho_b(E_1) = \{ \omega^{ib} \mid \omega^i \in E_1 \} = E_2$ και $\varrho_b(E_2) = \{ \omega^{jb} \mid \omega^j \in E_2 \} = E_1$, από το οποίο έπεται (ιδέ Πόρισμα 3.2.39) ότι $(\mathcal{C}_1)_{\varrho_a} = \mathcal{C}_2$ και $(\mathcal{C}_2)_{\varrho_a} = \mathcal{C}_1$ με $a = b^{-1}$. ό.έ.δ.

Παρατηρήσεις 4.5.9. 1. Από τα προηγούμενα έπεται ότι, αν έχουμε έναν φυσικό αριθμό n και ένα πεπερασμένο σώμα $\mathbb{F}$ με q το πλήθος στοιχεία (με τον n, όπως πάντα, πρώτο προς τον q), τότε υπάρχουν ζεύγη διττών κωδίκων, αν και μόνο αν υπάρχει ένας πολλαπλασιαστής ϱ_b, ο οποίος διαμερίζει το σύνολο των ακεραίων αριθμών $S = \{ 1, 2, \ldots, n-1 \}$ σύμφωνα με την Παρατήρηση 4.5.7.

   Το γεγονός αυτό δικαιολογεί την παρατήρηση που είχαμε κάνει ότι ένας πολλαπλασιαστής διαχωρίζει ένα ζεύγος διττών κωδίκων.

2. Είδαμε ότι αν ο πολλαπλασιαστής ϱ_a διαχωρίζει ένα ζεύγος διττών κωδίκων μήκους n, τότε ο πολλαπλασιαστής ϱ_b ($b = a^{-1}$) διαμερίζει το σύνολο $S = \{ 1, 2, \ldots, n-1 \}$ σε δύο υποσύνολα S_1 και S_2, έτσι ώστε $\varrho_b(S_1) = \{ ib \bmod n \mid i \in S_1 \} = S_2$ και $\varrho_b(S_2) = \{ jb \bmod n \mid j \in S_2 \} = S_1$. Αλλά τότε, προφανώς, και $\varrho_a(S_1) = S_2$ και $\varrho_a(S_2) = S_1$.

Παράδειγμα 4.5.10. Έστω $\mathbb{F} = \mathbb{Z}_3$, $n = 11$. Θα δείξουμε ότι υπάρχει ένα μόνο ζεύγος αρτίων διττών κωδίκων, μήκους n επί του $\mathbb{F}$.

Έστω ω μια 11−οστή πρωταρχική ρίζα της μονάδος επί του $\mathbb{F}$ και $g_1(x) = m_\omega(x)$, το ελάχιστο πολυώνυμο της ω. Το σύνολο ριζών του $g_1(x)$ είναι το σύνολο $E_1 = \{\omega, \omega^3, \omega^9, \omega^5, \omega^4\}$. Έστω $S_1 = \{1, 3, 9, 5, 4\}$. Παρατηρούμε ότι για $a = 2 \mod 11$ το $b = 6 \mod 11$ είναι το αντίστροφο του a στο σώμα $\mathbb{F}$ και ότι $\varrho_b(S_1) = \{ib \mod 11 \mid i \in S_1\} = \{2, 6, 7, 10, 8\}$. Τα σύνολα S_1 και $S_2 = \varrho_b(S_1)$ αποτελούν μια διαμέριση του συνόλου $S = \{1, 2, \ldots, n-1\}$, Επομένως, από την προηγούμενη πρόταση, υπάρχει ένα ζεύγος αρτίων διττών κωδίκων $\mathcal{C}_1$ και $\mathcal{C}_2$, μήκους n επί του σώματος $\mathbb{F}$, με πολυώνυμα γεννήτορες $\gamma_1(x) = (x-1)g_1(x)$ και $\gamma_2(x) = (x-1)g_2(x)$, όπου το πολυώνυμο $g_2(x)$ έχει ως σύνολο ριζών το σύνολο $E_2 = \{\omega^j \mid j \in S_2\}$.

Προφανώς (γιατί;) δεν υπάρχει άλλη διαμέριση του συνόλου:

$$S = \{1, 2, \ldots, n-1\},$$

η οποία να πληροί και τα τέσσερα σκέλη της Παρατήρησης 4.5.7. Επομένως, υπάρχει μοναδικό ζεύγος αρτίων διττών (όπως και περιττών) τριαδικών κωδίκων μήκους 11.

Στο δεύτερο από τα Παραδείγματα 4.5.5 είχαμε κατασκευάσει ένα ζεύγος τριαδικών αρτίων διττών κωδίκων μήκους 11 κατασκευάζοντας αδύναμους γεννήτορες. Εδώ είδαμε ότι υπάρχει μοναδικό ζεύγος τριαδικών αρτίων διττών κωδίκων μήκους 11. Επομένως πρόκειται για τους ίδιους κώδικες. Μάλιστα δε, όπως θα πρέπει να έχετε ήδη παρατηρήσει, οι αντίστοιχοι περιττοί διττοί κώδικες είναι οι τριαδικοί Golay κώδικες.

Παρατήρηση 4.5.11. Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ ένα ζεύγος αρτίων διττών κωδίκων, μήκους n επί του σώματος $\mathbb{F}$, με q το πλήθος στοιχεία. Τότε, εξ ορισμού, υπάρχει ένας πολλαπλασιαστής ϱ_a, έτσι ώστε $(\mathcal{C}_1)_{\varrho_a} = \mathcal{C}_2$ και $(\mathcal{C}_2)_{\varrho_a} = \mathcal{C}_1$.

Γεννάται το εξής ερώτημα. Ο πολλαπλασιαστής ϱ_a είναι μοναδικός με την παραπάνω ιδιότητα;

Από την Πρόταση 3.2.40 έχουμε ότι ο πολλαπλασιαστής ϱ_q είναι αυτομορφισμός των $\mathcal{C}_1$ και $\mathcal{C}_2$. Επομένως και ο πολλαπλασιαστής $\varrho_{qa} = \varrho_q\varrho_a$ διαχωρίζει τους δύο κώδικες $\mathcal{C}_1$ και $\mathcal{C}_2$.

Παρομοίως, αν ο πολλαπλασιαστής ϱ_b διαμερίζει το σύνολο:

$$S = \{\, 1, 2, \ldots, n-1 \,\},$$

σύμφωνα με την Παρατήρηση 4.5.7, σε δύο υποσύνολα S_1 και S_2 με $\varrho_b(S_1) = \{ib \bmod n \mid i \in S_1\} = S_2$ και $\varrho_b(S_2) = \{jb \bmod n \mid j \in S_2\} = S_1$, τότε $\varrho_{qa}(S_1) = S_2$ και $\varrho_{qa}(S_2) = S_1$.

4.5.1 Οι δυϊκοί κώδικες των διττών κωδίκων

Οι διττοί κώδικες, εξ ορισμού, είναι κυκλικοί κώδικες. Επομένως, για τους δυϊκούς τους ισχύουν γενικά οι ιδιότητες, που ισχύουν για τους δυϊκούς κώδικες κυκλικών κωδίκων (ιδέ Θεώρημα 3.2.16 και Πρόταση 3.2.33). Όμως ένα ζεύγος διττών κωδίκων διαχωρίζεται/συνδέεται μέσω ενός πολλαπλασιαστή. Θα δούμε κάτι *ανάλογο* να συμβαίνει και με τους δυϊκούς κώδικες διττών κωδίκων.

Υπενθυμίζουμε ότι αυτο-ορθογώνιος ονομάζεται ένας γραμμικός κώδικας $\mathcal{C}$ αν $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. Στην περίπτωση των κυκλικών κωδίκων υπάρχει χαρακτηρισμός των κυκλικών αυτοδυϊκών κωδίκων ([ιδέ Ασκήσεις 3.2.5 (14), (15), (16)]. Εδώ θα δούμε έναν άλλο χαρακτηρισμό των αυτο-ορθογωνίων κυκλικών κωδίκων περιττού μήκους.

Πρόταση 4.5.12. *Έστω $\mathcal{C}$ ένας κυκλικός κώδικας περιττού μήκους n και διάστασης $k = (n-1)/2$ επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Ο κώδικας $\mathcal{C}$ είναι αυτο-ορθογώνιος, αν και μόνο αν είναι ένας άρτιος διττός κώδικας, του οποίου ένας πολλαπλασιαστής που επιτελεί τον διαχωρισμό είναι ο ϱ_{-1}.*

Απόδειξη. Υποθέτουμε ότι ο κυκλικός κώδικας $\mathcal{C} = \mathcal{C}_1$ είναι αυτο-ορθογώνιος με διάσταση $k = (n-1)/2$. Θα δείξουμε ότι είναι το ένα μέλος ενός ζεύγους άρτιων διττών κωδίκων. Μάλιστα δε, αν το άλλο μέλος είναι ο κώδικας $\mathcal{C}_2$, τότε $(\mathcal{C}_1)_{\varrho_{-1}} = \mathcal{C}_2$ και $(\mathcal{C}_2)_{\varrho_{-1}} = \mathcal{C}_1$.

Έστω $\epsilon_1(x)$ ο αδύναμος γεννήτορας του $\mathcal{C}_1$. Θέτουμε $\epsilon_2(x) = \varrho_{-1}(\epsilon_1(x))$ και $\mathcal{C}_2 = [[\epsilon_2(x)]]$. Το πολυώνυμο $\vartheta(x) = (1/n) \cdot (x^{n-1} + x^{n-2} + \cdots x + 1)$ δεν είναι κάθετο προς τον εαυτό του (γιατί;) και ο κώδικας $\mathcal{C}_1$ έχει υποτεθεί

αυτο-ορθογώνιος, επομένως $\vartheta(x) \notin \mathcal{C}_1$. Από το Λήμμα 4.5.1 έπεται αφενός ότι ο κώδικας $\mathcal{C}_1$ είναι άρτιος αφετέρου ότι $\vartheta(x) \in \mathcal{C}_1^{\perp} = [[1 - \varrho_{-1}(\epsilon_1(x))]] = [[1 - \epsilon_2(x)]]$ (ιδέ Πρόταση 3.2.33).

Ο κώδικας $\mathcal{C}_1^{\perp}$ έχει διάσταση ίση με $(n+1)/2$ και περιέχει τον κώδικα $\mathcal{C}_1$. Συνεπώς έχουμε ότι ο αδύναμος γεννήτορας του $\mathcal{C}_1^{\perp}$ είναι το πολυώνυμο $\epsilon_1(x) + \vartheta(x)$. Από την μοναδικότητα του αδυνάμου γεννήτορα έπεται ότι $\epsilon_1(x) + \vartheta(x) = 1 - \epsilon_2(x)$, δηλαδή ισχύει η συνθήκη (α) του ορισμού για τους διττούς κώδικες. Προφανώς, από τον ορισμό του $\epsilon_2(x) = \varrho_{-1}(\epsilon_1(x))$, έχουμε ότι $\epsilon_1(x) = \varrho_{-1}(\epsilon_2(x))$ και συνεπώς (από την Πρόταση 3.2.38) ισχύει και η συνθήκη (β) του ορισμού.

Αντίστροφα, υποθέτουμε ότι ο κώδικας $\mathcal{C} = \mathcal{C}_1 = [[\epsilon(x)]]$ είναι ένας άρτιος διττός κώδικας διαχωριζόμενος από το άλλο μέλος του ζεύγους με τον πολλαπλασιαστή ϱ_{-1}. Τότε το άλλο μέλος του ζεύγους είναι ο κώδικας $\mathcal{C}_2 = [[\varrho_{-1}(\epsilon_1(x))]]$. Συνεπώς, από το Θεώρημα 4.5.4 και την Πρόταση 3.2.33 έχουμε ότι $\mathcal{C}_1 \subseteq \mathcal{D}_1 = [[1 - \varrho_{-1}(\epsilon_1(x))]] = \mathcal{C}_1^{\perp}$. ό.έ.δ.

Θεώρημα 4.5.13. *Έστω $\mathcal{C}_1$, $\mathcal{C}_2$ ένα ζεύγος αρτίων διττών κωδίκων μήκους n επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία και $\mathcal{D}_1$, $\mathcal{D}_2$ το αντίστοιχο ζεύγος περιττών διττών κωδίκων.*

(α) *Τα ακόλουθα είναι ισοδύναμα:*

1. $\mathcal{C}_1^{\perp} = \mathcal{D}_1$.
2. $\mathcal{C}_2^{\perp} = \mathcal{D}_2$.
3. $(\mathcal{C}_1)_{\varrho_{-1}} = \mathcal{C}_2$.
4. $(\mathcal{C}_2)_{\varrho_{-1}} = \mathcal{C}_1$.

(β) *Τα ακόλουθα είναι ισοδύναμα:*

1. $\mathcal{C}_1^{\perp} = \mathcal{D}_2$.
2. $\mathcal{C}_2^{\perp} = \mathcal{D}_1$.
3. $(\mathcal{C}_1)_{\varrho_{-1}} = \mathcal{C}_1$.

4. $(\mathcal{C}_2)_{\varrho_{-1}} = \mathcal{C}_2$.

Απόδειξη. Θα αποδείξουμε το (α) αφήνοντας το (β) ως άσκηση.

Από τον ορισμό των διττών κωδίκων (Ορισμός 4.5.2), την Παρατήρηση 4.5.3 $_4$ και την Άσκηση 2.3.3 $_6$ έπεται εύκολα ότι τα (1) και (2) είναι ισοδύναμα.

Προφανώς ισχύει ότι $(\varrho_{-1})^{-1} = \varrho_{-1}$. Επομένως, τα (3) και (4) είναι ισοδύναμα.

Υποθέτουμε ότι ισχύει το (1). Επειδή $\mathcal{C}_1 \subseteq \mathcal{D}_1$ (ιδέ Θεώρημα 4.5.4$_5$) έχουμε ότι ο κώδικας $\mathcal{C}_1$ είναι αυτοδυϊκός. Οπότε, από το προηγούμενο θεώρημα, έχουμε ότι $(\mathcal{C}_1)_{\varrho_{-1}} = \mathcal{C}_2$, δηλαδή ισχύει το (3).

Αντίστροφα, υποθέτουμε ότι ισχύει το (3). Αν $\epsilon_1(x)$ είναι ο αδύναμος γεννήτορας του κώδικα $\mathcal{C}_1$, τότε το πολυώνυμο $\epsilon_2(x) = \varrho_{-1}(\epsilon_1(x))$ είναι ο αδύναμος γεννήτορας του κώδικα $\mathcal{C}_2$ (γιατί;). Επομένως, έπεται το (1) (ιδέ την Πρόταση 3.2.33). ό.έ.δ.

Παράδειγμα 4.5.14. Στο πρώτο από τα Παραδείγματα 4.5.5 είχαμε δει ένα ζεύγος $\mathcal{C}_1$ και $\mathcal{C}_2$ αρτίων διττών κωδίκων μήκους $n = 7$ επί του σώματος $\mathbb{Z}_2$ με τον πολλαπλασιαστή ϱ_3 να επιτελεί τον διαχωρισμό. Σύμφωνα με την Παρατήρηση 4.5.11 και ο πολλαπλασιαστής $\varrho_2\,\varrho_3 = \varrho_6 = \varrho_{-1}$ επιτελεί τον διαχωρισμό των δύο κωδίκων. Άρα, σύμφωνα με το προηγούμενο θεώρημα, γνωρίζουμε τους δυϊκούς κώδικες των $\mathcal{C}_1$ και $\mathcal{C}_2$.

Με παρόμοιο τρόπο μπορούμε να προσδιορίσουμε τους δυϊκούς κώδικες των αντιστοίχων αρτίων διττών κωδίκων και στο δεύτερο από τα Παραδείγματα 4.5.5.

Στους διττούς κώδικες η ελάχιστη απόστασή τους σχετίζεται με το μήκος τους.

Θεώρημα 4.5.15. *Έστω $\mathcal{D}_1$ και $\mathcal{D}_2$ ένα ζεύγος περιττών διττών κωδίκων επί του πεπερασμένου σώματος $\mathbb{F}$. Αν d είναι η ελάχιστη απόστασή τους, τότε $d^2 \geq n$.*

Αν επιπλέον ο πολλαπλασιαστής, ο οποίος επιτελεί τον διαχωρισμό τους, είναι ο ϱ_{-1}, τότε $d^2 - d + 1 \geq n$.

Απόδειξη. Υποθέτουμε ότι ο πολλαπλασιαστής, που επιτελεί τον διαχωρισμό των δύο κωδίκων, είναι ο ϱ_a. Τότε για κάθε $c(x) \in \mathcal{D}_1$ έχουμε ότι $\varrho_a(c(x)) \in \mathcal{D}_2$. Μάλιστα δε τα $c(x)$ και $\varrho_a(c(x))$ έχουν το ίδιο βάρος. Επομένως, αν έχουμε ένα στοιχείο $c(x) \in \mathcal{D}_1$ ελαχίστου βάρους, δηλαδή $w(c(x)) = d$, τότε και $w(\varrho_a(c(x))) = d$. Το γινόμενο $c(x) \cdot (\varrho_a(c(x)))$ έχει τις εξής ιδιότητες:

Το πλήθος των μη μηδενικών όρων (άρα το βάρος του) είναι το πολύ ίσον με d^2.

Το $c(x) \cdot (\varrho_a(c(x))) \in \mathcal{D}_1 \cap \mathcal{D}_2 = [[\vartheta(x)]]$. Αφού οι $\mathcal{D}_1$ και $\mathcal{D}_2$ είναι ιδεώδη του δακτυλίου $\mathcal{R}_n$.

Από το Λήμμα 4.5.1 έπεται ότι το $c(x) \cdot (\varrho_a(c(x)))$ είναι μη μηδενικό πολλαπλάσιο του $\vartheta(x)$, άρα περιττού βάρους. Το βάρος όμως του:

$$\vartheta(x) = (1/n)(x^{n-1} + x^{n-2} + \cdots x + 1)$$

ισούται με n. Συνεπώς $d^2 \geq n$.

Αν τώρα υποθέσουμε ότι ο πολλαπλασιαστής είναι ο ϱ_{-1}, τότε $c(x) \cdot (\varrho_{-1}(c(x))) = c(x) \cdot c(x^{-1}) = c(x) \cdot c(x^{n-1})$ (ο πολλαπλασιασμός γίνεται $\bmod (x^n - 1)$). Από τους d^2 το πλήθος όρους του γινομένου $c(x) \cdot c(x^{-1}) = c(x) \cdot c(x^{n-1})$ οι d το πλήθος είναι ίσοι με 1 (γιατί;). Συνεπώς, το μέγιστο βάρος του $c(x) \cdot c(x^{-1}) = c(x) \cdot c(x^{n-1})$ είναι ίσον με $d^2 - d + 1$ και κατά συνέπεια $d^2 - d + 1 \geq n$. ό.έ.δ.

Παρατηρήσεις 4.5.16.

1. Το κάτω φράγμα της ελάχιστης απόστασης ($d \geq \sqrt{n}$) που ικανοποιεί η ελάχιστη απόσταση περιττών διττών κωδίκων σε σχέση με το μήκος τους είναι γνωστό ως **φράγμα της τετραγωνικής ρίζας** και η σημασία του έγκειται στο γεγονός ότι μας δίνει ένα *μέτρο* ως προς την ικανότητα διόρθωσης λαθών, με τους συγκεκριμμένους κώδικες, σε σχέση με το μήκος τους.

2. Για την απόδειξη ότι οι κώδικες Golay είναι κυκλικοί είχαμε αποδείξει το Λήμμα 4.2.9. Αν επιστρέψουμε τώρα και δούμε την απόδειξη αυτού του λήμματος, αμέσως θα διαπιστώσουμε ότι πρόκειται για την απόδειξη του προηγουμένου θεωρήματος *προσαρμοσμένη* στην συγκεκριμένη περίπτωση των $\mathcal{G}_{23}$ κωδίκων Golay.

4.5.2 Η ύπαρξη διττών κωδίκων

Στα προηγούμενα ορίσαμε τους διττούς κώδικες, μελετήσαμε ιδιότητες τους και δώσαμε παραδείγματα διττών κωδίκων. Όπως έχουμε ήδη παρατηρήσει (ιδέ Παρατήρηση 4.5.9) η ύπαρξη διττών κωδίκων μήκους n επί ενός σώματος με q το πλήθος στοιχεία είναι ισοδύναμη με την υπάρξη ενός πολλαπλασιαστή, ο οποίος διαμερίζει κατάλληλα το σύνολο $S = \{1, 2, \ldots, n-1\}$.

Επομένως, η μελέτη της ύπαρξης διττών κωδίκων *παραπέμπει* στην περετέρω μελέτη της σχέσης μεταξύ των δύο αριθμών n και q.

Αν παρατηρήσουμε σε όλα τα παραδείγματα διττών κωδίκων, θα δούμε ότι μεταξύ του μήκους τους n και του πλήθους q των στοιχείων του σώματος, επί του οποίου ορίζονται, ισχύει η εξής σημαντική σχέση.

Υπάρχει ένα $x \in \mathbb{Z}_n$ έτσι ώστε $q \equiv x^2 \mod n$. Για παράδειγμα $2 \equiv 3^2 \mod 7$, $3 \equiv 6^2 \mod 11$.

Όπως θα δούμε η σχέση αυτή, μεταξύ n και q, αποτελεί ικανή και αναγκαία συνθήκη για την ύπαρξη διττών κωδίκων μήκους n επί ενός σώματος με q το πλήθος στοιχεία.

Πριν προχωρήσουμε θα υπενθυμίσουμε ορισμένα αποτελέσματα από την στοιχειώδη Θεωρία Αριθμών που αφορούν τα τετραγωνικά υπόλοιπα[4].

Ορισμός 4.5.17. *Έστω n ένας περιττός θετικός ακέραιος. Ο ακέραιος a θα ονομάζεται* ***τετραγωνικό υπόλοιπο*** $\mod n$ *(ή ως προς n) αν υπάρχει ακέραιος x, έτσι ώστε $a \equiv x^2 \mod n$.*

Προφανώς, αν $a \equiv b \mod n$, τότε ο a είναι τετραγωνικό υπόλοιπο αν και μόνο αν ο b είναι τετραγωνικό υπόλοιπο. Συνεπώς, μπορούμε άνευ βλάβης να υποθέτουμε ότι $a \in \mathbb{Z}_n$.

Σχόλιο 4.5.18. Συνήθως στον ορισμό των τετραγωνικών υπολοίπων ο n υποτίθεται περιττός πρώτος. Θα δούμε ότι η γενική περίπτωση ανάγεται στην

[4] Τα αποτελέσματα που παραθέτουμε εδώ είναι αποσπασματικά και προσαρμοσμένα για τις ανάγκες των όσων παρουσιάζουμε. Για περισσότερα πρέπει να ανατρέξετε σε ένα εγχειρίδιο της Θεωρίας Αριθμών, για παράδειγμα στο Niven, I. and Zuckerman, H.S. and Montgomery, H.L. [1991].

περίπτωση όπου ο n είναι πρώτος. Επίσης, θα δούμε ότι οι πλέον ενδιαφέρουσες εφαρμογές εμφανίζονται στην περίπτωση αυτή.

Το σύνολο των μη μηδενικών στοιχείων του σώματος $\mathbb{Z}_p$, όπου ο p είναι ένας περιττός πρώτος, τα οποία είναι τετραγωνικά υπόλοιπα $\mod p$ θα το συμβολίζουμε με Q_p και το σύνολο των μη μηδενικών στοιχείων του σώματος $\mathbb{Z}_p$, τα οποία είναι μη τετραγωνικά υπόλοιπα $\mod p$ θα το συμβολίζουμε με N_p.

Λήμμα 4.5.19. *Έστω p ένας περιττός πρώτος.*

1. $|\, Q_p \,| = |\, N_p \,| = (p-1)/2$.
2. $\varrho_a(Q_p) = Q_p$ *και* $\varrho_a(N_p) = N_p$ *για κάθε* $a \in Q_p$.
   $\varrho_b(Q_p) = N_p$ *και* $\varrho_b(N_p) = Q_p$ *για κάθε* $b \in N_p$.

Απόδειξη. Ως γνωστόν, η πολλαπλασιαστική ομάδα $U(\mathbb{Z}_p)$ του σώματος $\mathbb{Z}_p$ είναι κυκλική. Αν c είναι ένας γεννήτοράς της, τότε εύκολα βλέπουμε ότι το σύνολο των τετραγωνικών υπολοίπων Q_p είναι η (μοναδική) υποομάδα της $U(\mathbb{Z}_p)$ η παραγόμενη από το c^2. Συνεπώς, έχει τάξη ίση με $(p-1)/2$ και είναι δείκτου 2. Το αποτέλεσμα τώρα είναι άμεσο. ό.έ.δ.

Παρατήρηση 4.5.20. Από το προηγούμενο λήμμα έπεται ότι ένα $0 \neq a \in \mathbb{Z}_p$ είναι τετραγωνικό υπόλοιπο, αν και μόνο αν η τάξη του (ως στοιχείο της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_p)$) είναι διαιρέτης του $(p-1)/2$.

Επίσης, από το γεγονός ότι η εξίσωση $x^2 \equiv 1 \mod p$ έχει ως λύσεις το $\pm 1 \mod p$, έπεται ότι ένα $0 \neq a \in \mathbb{Z}_p$ δεν είναι τετραγωνικό υπόλοιπο, αν και μόνο αν $a^{(p-1)/2} \equiv -1 \mod p$.

Λήμμα 4.5.21. (i) *Έστω $n = n_1 \cdot n_2$ ένας περιττός θετικός ακέραιος, όπου οι n_1 και n_2 είναι σχετικά πρώτοι. Ο ακέραιος a είναι τετραγωνικό υπόλοιπο $\mod n$, αν και μόνο αν είναι τετραγωνικό υπόλοιπο $\mod n_1$ και τετραγωνικό υπόλοιπο $\mod n_2$.*

(ii) *Έστω p ένας περιττός πρώτος. Ο ακέραιος a είναι (μη μηδενικό) τετραγωνικό υπόλοιπο $\mod p^\nu$, αν και μόνο αν είναι τετραγωνικό υπόλοιπο $\mod p$.*

Απόδειξη. (i) Επικαλούμαστε το εξής αποτέλεσμα της Θεωρίας Αριθμών.

Έστω n_1 και n_2 δύο σχετικά πρώτοι θετικοί ακέραιοι και $n = n_1 \cdot n_2$. Η απεικόνιση $\theta : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ με $\theta(a \mod n) = (a \mod n_1, a \mod n_2)$ είναι ένας ισομορφισμός δακτυλίων.

Η απόδειξη είναι απλή, στηρίζεται στο (Κινέζικο) Θεώρημα Υπολοίπων και αφίεται ως άσκηση (ιδέ Άσκηση 4.5.3 $_8$).

Υποθέτουμε ότι $a \equiv x^2 \mod n_1$ και $a \equiv y^2 \mod n_2$. Τότε για το στοιχείο $(x \mod n_1, y \mod n_2) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ υπάρχει μοναδικό $z \mod n \in \mathbb{Z}_n$ με $\theta(z \mod n) = (x \mod n_1, y \mod n_2)$. Οπότε προφανώς $a = z^2 \mod n$.

Αντίστροφα, αν ο ακέραιος a είναι τετραγωνικό υπόλοιπο $\mod n_1$ και τετραγωνικό υπόλοιπο $\mod n_2$, τότε προφανώς είναι και τετραγωνικό υπόλοιπο $\mod n$.

(ii) Προφανώς, αν ο a είναι τετραγωνικό υπόλοιπο $\mod p^\nu$, τότε είναι και τετραγωνικό υπόλοιπο $\mod p$.

Αντίστροφα, υποθέτουμε ότι ο a είναι τετραγωνικό υπόλοιπο $\mod p$. Τότε, από το προηγούμενο λήμμα έχουμε ότι $a^{(p-1)/2} \equiv 1 \mod p$. Από την τελευταία σχέση έπεται ότι $(a^{(p-1)/2})^{p^{\nu-1}} \equiv 1 \mod p^\nu$ (ιδέ Άσκηση 4.5.3$_9$).

Αν $U = U(\mathbb{Z}_{p^\nu})$ είναι η πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}_{p^\nu}$, τότε αυτή είναι κυκλική (ιδέ την Άσκηση στη σελίδα 391) και έχει τάξη ίση με $\varphi(p^\nu) = (p-1)p^{\nu-1}$, όπου φ είναι η συνάρτηση του Euler. Συνεπώς, από την παραπάνω σχέση, αν r είναι ένας γεννήτορας της U, έπεται ότι το a περιέχεται στην υποομάδα της U την παραγόμενη από το r^2, άρα είναι τετραγωνικό υπόλοιπο $\mod p^\nu$. ό.έ.δ.

Λήμμα 4.5.22. *Έστω $n = n_1 \cdot n_2$ ένας θετικός ακέραιος, όπου οι n_1 και n_2 είναι σχετικά πρώτοι.*

Έστω a ένας ακέραιος πρώτος προς τον n. Θέτουμε $a_1 \equiv a \mod n_1$ και $a_2 \equiv a \mod n_2$.

Ο πολλαπλασιαστής ϱ_a διαμερίζει το σύνολο $S = \{1, 2, \ldots, n-1\}$, αν και μόνο αν οι πολλαπλασιαστές ϱ_{a_1} και ϱ_{a_2} διαμερίζουν τα σύνολα $R = \{1, 2, \ldots, n_1 - 1\}$ και $T = \{1, 2, \ldots, n_2 - 1\}$ αντίστοιχα.

Απόδειξη. Όπως προαναφέραμε η απεικόνιση $\theta : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ με

$\theta(a \mod n) = (a \mod n_1, a \mod n_2)$ είναι ένας ισομορφισμός δακτυλίων. Οπότε στο εξής, άνευ βλάβης, θα ταυτοποιήσουμε τον δακτύλιο $\mathbb{Z}_n$ με τον δακτύλιο $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Τους δακτυλίους $\mathbb{Z}_{n_1}$ και $\mathbb{Z}_{n_2}$ με τους υποδακτυλίους $\mathbb{Z}_{n_1} \times \{0\}$ και $\mathbb{Z}_{n_2} \times \{0\}$ αντίστοιχα και θα τους θεωρούμε ως υποδακτυλίους του $\mathbb{Z}_n$.

Επομένως, μέσω αυτής της ταυτοποίησης, ορίζονται οι προβολές $\pi_1 : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1}$ και $\pi_2 : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_2}$ με $\pi_1(r \mod n) = r \mod n_1$ και $\pi_2(r \mod n) = r \mod n_2$. Καθώς, επίσης, και οι εμφυτεύσεις $e_1 : \mathbb{Z}_{n_1} \longrightarrow \mathbb{Z}_n$ και $e_2 : \mathbb{Z}_{n_2} \longrightarrow \mathbb{Z}_n$.

Όπου εδώ ταυτίζουμε τους δακτυλίους $\mathbb{Z}_{n_1}$ και $\mathbb{Z}_{n_2}$ με τους υποδακτυλίους $\mathbb{Z}_{n_1} \times \{0\}$ και $\{0\} \times \mathbb{Z}_{n_2}$ αντίστοιχα του δακτυλίου $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \approx \mathbb{Z}_n$.

Είναι προφανές (να κάνετε τον έλεγχο!) ότι $\pi_1 \circ \varrho_a = \varrho_{a_1} \circ \pi_1$ και $\pi_2 \circ \varrho_a = \varrho_{a_2} \circ \pi_2$.

Υποθέτουμε ότι ο πολλαπλασιαστής ϱ_a διαμερίζει το σύνολο:

$$S = \{1, 2, \ldots, n-1\}$$

σε δύο υποσύνολα S_1 και S_2. Έστω $R_1 = \pi_1(S_1)$, $R_2 = \pi_1(S_2)$ και $T_1 = \pi_2(S_1), T_2 = \pi_2(S_2)$. Τότε έχουμε ότι $\varrho_{a_1}(R_1) = \varrho_{a_1}(\pi_1(S_1)) = \pi_1(\varrho_a(S_1)) = \pi_1(S_2) = R_2$. Οπότε εύκολα βλέπουμε ότι:

$$R = \{1, 2, \ldots, n_1 - 1\} = R_1 \cup R_2 \quad \text{και} \quad R_1 \cap R_2 = \emptyset.$$

Επίσης, επειδή κάθε ένα από τα S_1 και S_2 είναι ένωση q-κυκλοτομικών συμπλόκων $\mod n$, έχουμε ότι $x^n - 1 = (x-1)g_1(x)g_2(x)$ με:

$$g_1(x) = \prod_{i \in S_1} (x - \omega^i) \quad \text{και} \quad g_2(x) = \prod_{j \in S_2} (x - \omega^j),$$

όπου ω είναι μια n-οστή πρωταρχική ρίζα της μονάδας (ιδέ Παρατήρηση 4.5.7). Επομένως, εύκολα έπεται ότι τα σύνολα R_1 και R_2 είναι ένωση q-κυκλοτομικών συμπλόκων $\mod n_1$. Μάλιστα δε $x^{n_1} - 1 = (x-1)\phi_1(x)\phi_2(x)$, όπου $\phi_1(x) = \prod_{i \in R_1}(x - \omega^{n_2 i})$ και $\phi_2(x) = \prod_{j \in R_2}(x - \omega^{n_2 j})$. Δηλαδή ο πολλαπλασιαστής ϱ_{a_1} διαμερίζει το σύνολο R.

Συμμετρικά αποδεικνύεται ότι ο πολλαπλασιαστής ϱ_{a_2} διαμερίζει το σύνολο $T = \{1, 2, \ldots, n_2 - 1\}$.

Αντίστροφα, υποθέτουμε ότι ο πολλαπλασιαστής ϱ_{a_1} διαμερίζει το σύνολο $R = \{1, 2, \ldots, n_1 - 1\}$ σε δύο υποσύνολα R_1 και R_2 και ότι ο πολλαπλασιαστής ϱ_{a_2} διαμερίζει το σύνολο $T = \{1, 2, \ldots, n_2 - 1\}$ σε δύο υποσύνολα T_1 και T_2 αντίστοιχα.

Θεωρούμε τα σύνολα $S_1 = \theta^{-1}((R_1 \times \mathbb{Z}_{n_2}) \cup (\{0 \mod n_1\} \times T_1))$ και $S_2 = \theta^{-1}((R_2 \times \mathbb{Z}_{n_2}) \cup (\{0 \mod n_1\} \times T_2))$. Προφανώς ισχύει ότι $S_1 \cap S_2 = \emptyset$ και $S_1 \cup S_2 = S = \{1, 2, \ldots, n - 1\}$. Επίσης, είναι εύκολο να ελέγξουμε (να κάνετε τον έλεγχο!) ότι αν $a \mod n = \theta^{-1}((a_1 \mod n_1, a_2 \mod n_2))$, τότε $\varrho_a(S_1) = S_2$ και $\varrho_a(S_2) = S_1$.

Επίσης, επειδή τα σύνολα R_1 και R_2 είναι ένωση q-κυκλοτομικών συμπλόκων $\mod n_1$ και τα σύνολα T_1 και T_2 είναι ένωση q-κυκλοτομικών συμπλόκων $\mod n_2$, έπεται ότι τα σύνολα S_1 και S_2 είναι ένωση κυκλοτομικών q-κυκλοτομικών συμπλόκων. (Ιδέ άσκηση $4.5.3_{11}$.) ό.έ.δ.

Θεώρημα 4.5.23. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας θετικός ακέραιος (όπως πάντα ο n θεωρείται πρώτος προς τον q). Υπάρχουν διττοί κώδικες μήκους n επί του σώματος $\mathbb{F}$, αν και μόνο αν ο q είναι τετραγωνικό υπόλοιπο $\mod n$.*

Πριν ξεκινήσουμε την απόδειξη του Θεωρήματος θα επισημάνουμε ότι:

Από την Παρατήρηση 4.5.9 έχουμε ότι υπάρχουν ζεύγη διττών κωδίκων, μήκους n επί του σώματος $\mathbb{F}$, αν και μόνο αν υπάρχει ένας πολλαπλασιαστής ϱ_a, ο οποίος διαμερίζει το σύνολο των ακεραίων αριθμών $S = \{1, 2, \ldots, n - 1\}$.

Έστω $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_\kappa^{\lambda_\kappa}$ η ανάλυση του n σε πρώτους παράγοντες.

Από το προηγούμενο λήμμα έχουμε ότι ο πολλαπλασιαστής ϱ_a διαμερίζει το σύνολο $S = \{1, 2, \ldots, n - 1\}$, αν και μόνο οι πολλαπλασιαστές ϱ_{a_i} διαμερίζουν τα σύνολα $S_i = \{1, 2, \ldots, p_i^{\lambda_i} - 1\}$, $i = 1, \ldots, \kappa$, όπου $a_i \equiv a \mod p_i^{\lambda_i}$.

Από το Λήμμα 4.5.21 έχουμε ότι ο q είναι τετραγωνικό υπόλοιπο $\mod n$ αν και μόνο αν ο ο q είναι τετραγωνικό υπόλοιπο $\mod p_i^{\lambda_i}$ για κάθε $i = 1, \ldots, \kappa$.

Επομένως, μπορούμε να υποθέσουμε ότι $n = p^\lambda$.

Απόδειξη. Από τα προηγούμενα έπεται ότι η προς απόδειξη ισοδυναμία ανάγεται στην απόδειξη της ισοδυναμίας:

Έστω $n = p^\lambda$, όπου p είναι ένας περιττός πρώτος. Τότε υπάρχει πολλαπλασιαστης ϱ_a, ο οποίος διαμερίζει το σύνολο $S = \{1, 2, \ldots, n-1\}$, αν και μόνο αν ο q είναι τετραγωνικό υπόλοιπο $\mod n$.

Θα αποδείξουμε την ανωτέρω ισοδυναμία στη μερική περίπτωση όπου $\lambda = 1$, δηλαδή $n = p$ πρώτος.

Υποθέτουμε ότι ο πολλαπλασιαστής ϱ_a διαμερίζει το σύνολο:

$$S = \{1, 2, \ldots, n-1\}$$

σε δύο υποσύνολα S_1 και S_2. Έστω $U = U(\mathbb{Z}_p)$ η πολλαπλασιαστική ομάδα του σώματος $\mathbb{Z}_p$. Τότε αυτή είναι κυκλική και έχει τάξη ίση με $p-1$. Επειδή ο q είναι πρώτος προς τον p, έχουμε ότι $q \in U$. Από το Λήμμα 4.5.19 έχουμε ότι το σύνολο Q_p των τετραγωνικών υπολοίπων $\mod p$ είναι η (μοναδική) υποομάδα δείκτου 2 στην U. Θα δείξουμε ότι $q \in Q_p$.

Έστω R η υποομάδα της U η παραγόμενη από το q. Από την σχέση $aq \in U$, για κάθε $a \in U$, έχουμε ότι η U είναι η ένωση q- κυκλοτομικών συμπλόκων $\mod p$. Όμως κάθε q-κυκλοτομικό σύμπλοκο είναι ένα σύμπλοκο της R στην U. Συνεπώς, το πλήθος των (διακεκριμένων) q-κυκλοτομικών συμπλόκων ισούται με τον δείκτη της R στην U. Επειδή ο πολλαπλασιαστής ϱ_a διαμερίζει το σύνολο $U = S = \{1, 2, \ldots, p-1\}$ στα υποσύνολα S_1 και S_2 και κάθε ένα από τα S_1 και S_2 είναι ένωση q-κυκλοτομικών συμπλόκων, έχουμε ότι υπάρχουν άρτιο το πλήθος q-κυκλοτομικών συμπλόκων. Δηλαδή ο δείκτης της R στην U είναι άρτιος. Συνεπώς, $R \subseteq Q_p$ και τελειώσαμε.

Αντίστροφα, υποθέτουμε ότι ο q είναι τετραγωνικό υπόλοιπο $\mod p$. Θα βρούμε έναν πολλαπλασιαστή ϱ_a, ο οποίος θα διαμερίζει το σύνολο $U = S = \{1, 2, \ldots, p-1\}$.

Έστω, όπως προηγουμένως, R η υποομάδα της U η παραγόμενη από το q. Τότε έχουμε $R \subseteq Q_p \subseteq U$. Επειδή ο δείκτης της Q_p στην U είναι ίσος με 2, υπάρχει μοναδική υποομάδα, έστω K, της U, η οποία είναι υποομάδα δείκτου $(p-1)/2$ στην U και περιέχει την R ως υποομάδα δείκτου 2 (γιατί;).[5]

[5]Εδώ επικαλούμαστε δύο πολύ γνωστά αποτελέσματα από τη Θεωρία Ομάδων. Πρώτον,

Έστω $a \in K \setminus R$. Τότε $K = R \cup aR$. Επίσης, αν $U = r_1K \cup r_2K \cup \cdots, r_\nu K$ ($\nu = (p-1)/2$), ως ένωση διακεκριμένων συμπλόκων, τότε $U = r_1R \cup r_2R \cup \cdots \cup r_\nu R \cup ar_1R \cup ar_2R \cup \cdots \cup ar_\nu R$. Θέτουμε $S_1 = r_1R \cup r_2R \cup \cdots \cup r_\nu R$ και $S_2 = ar_1R \cup ar_2R \cup \cdots \cup ar_\nu R$. Από τον τρόπο ορισμού τους τα υποσύνολα S_1 και S_2 αποτελούν μια διαμέριση του σύνόλου S.

Άρα, η απόδειξη του θεωρήματος ολοκληρώθηκε. ό.έ.δ.

Παρατήρηση 4.5.24. Η γενική περίπτωση, όπου $n = p^\lambda$ αποδεικνύεται αναλόγως.

Η απόδειξη της κατεύθυνσης: *Αν υπάρχει πολλαπλασιαστής ϱ_a, ο οποίος διαμερίζει το σύνολο $S = \{1, 2, \ldots, n-1\}$, τότε ο q είναι τετραγωνικό υπόλοιπο* $\mod n$, είναι ακριβώς η ίδια. Αρκεί να δούμε ότι η πολλαπλασιαστική ομάδα του $U(\mathbb{Z}_n)$ είναι κυκλική με άρτια τάξη ίση με $(p-1)p^{\lambda-1}$ (ιδέ την Άσκηση στη σελίδα 391).

Η απόδειξη της αντίστροφης κατεύθυνσης δεν είναι δύσκολη, απλώς απαιτεί λεπτότερους χειρισμούς, οι οποίοι, κατά τη γνώμη μας, στο σημείο αυτό δεν προσφέρουν στον αναγνώστη.

Το προηγούμενο θεώρημα ανάγει το πρόβλημα της ύπαρξης διττών κωδίκων, όπως άλλωστε είχαμε επισημάνει στην αρχή της παραγράφου, στην μελέτη της σχέσης μεταξύ των θετικών αριθμών n, το μήκος των κωδίκων, και του q, το πλήθος των στοιχείων του σώματος επί του οποίου ορίζονται οι κώδικες.

Πόρισμα 4.5.25. *Εστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Υποθέτουμε ότι το q είναι άρτια δύναμη ενός πρώτου αριθμού. Για κάθε θετικό ακέραιο n πρώτο προς τον q υπάρχουν διττοί κώδικες μήκους n επί του $\mathbb{F}$.*

για κάθε διαιρέτη της τάξης μιας πεπερασμένης κυκλικής ομάδας υπάρχουν δύο μοναδικές υποομάδες της, η μία με τάξη αυτόν τον διαιρέτη και η άλλη με δείκτη αυτόν τον διαιρέτη.

Δεύτερον, αν G είναι μια ομάδα και H, K είναι υποομάδες της, με $G \geq H \geq K$, τότε ο δείκτης της K στην G ισούται με το γινόμενο του δείκτη της K στην H επί το δείκτη της H στην G. Για παράδειγμα παραπέμπουμε στο Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη [2013], παρ. 4.6.

Στα επόμενα θα περιορισθούμε, και θα λεπτολογήσουμε, στις περιπτώσεις όπου $q = 2, 3$.

Πριν ξεκινήσουμε, παραθέτουμε, χωρίς απόδειξη, δύο λήμματα από τη Θεωρία Αριθμών. Αν και τα επιχειρήματα που χρησιμοποιούνται για την απόδειξη είναι στοιχειώδη, οι αποδείξεις είναι σχετικά μακροσκελείς. Ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει σε ένα εγχειρίδιο της Θεωρίας Αριθμών. Για την απόδειξη παραπέμπουμε στο Niven, I. and Zuckerman, H.S. and Montgomery, H.L. [1991].

Λήμμα 4.5.26. *Έστω p ένας περιττός πρώτος. Το 2 είναι τετραγωνικό υπόλοιπο* $\mod p$, *αν και μόνο αν* $p \equiv \pm 1 \mod 8$.

Λήμμα 4.5.27. *Έστω $p \neq 3$ ένας περιττός πρώτος. Το 3 είναι τετραγωνικό υπόλοιπο* $\mod p$, *αν και μόνο αν* $p \equiv \pm 1 \mod 12$.

Θεώρημα 4.5.28. *Έστω n περιττός θετικός ακέραιος και $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_\kappa^{\lambda_\kappa}$ η ανάλυση του σε πρώτους παράγοντες.*

1. *Υπάρχουν διττοί κώδικες μήκους n επί του $\mathbb{Z}_2$, αν και μόνο αν $p_i \equiv \pm 1 \mod 8$, για όλα τα $1 \leq i \leq \kappa$.*

2. *Υπάρχουν διττοί κώδικες μήκους n επί του $\mathbb{Z}_3$, αν και μόνο αν $p_i \equiv \pm 1 \mod 12$, για όλα τα $1 \leq i \leq \kappa$.*

Απόδειξη. Η απόδειξη είναι απλός συνδυασμός του Θεωρήματος 4.5.23, του Λήμματος 4.5.21 και των Λημμάτων 4.5.26 και 4.5.27. ό.έ.δ.

4.5.3 Ασκήσεις

1. Έστω $\delta_1(x)$ και $\delta_2(x)$ δύο περιττά αδύναμα στοιχεία του δακτυλίου $\mathcal{R}_n = \mathbb{F}[x]/\langle x^n - 1\rangle$ και $\mathcal{D}_1 = [[\delta_1(x)]]$, $\mathcal{D}_2 = [[\delta_2(x)]]$ οι κυκλικοί κώδικες που έχουν αντίστοιχα τα $\delta_1(x)$ και $\delta_2(x)$ ως αδύναμους γεννήτορες.

   Δείξτε ότι οι κώδικες $\mathcal{D}_1$ και $\mathcal{D}_2$ αποτελούν ένα ζεύγος περιττών διττών κωδίκων, αν και μόνο αν ικανοποιούνται οι ακόλουθες συνθήκες:

   (i) $\delta_1(x) + \delta_2(x) = 1 + \vartheta(x) = 1 + (1/n) \cdot (x^{n-1} + x^{n-2} + \cdots x + 1)$.

(*ii*) Υπάρχει πολλαπλασιαστής ϱ_a έτσι ώστε:

$$(\mathcal{D}_1)_{\varrho_a} = \mathcal{D}_2 \quad \text{και} \quad (\mathcal{D}_2)_{\varrho_a} = \mathcal{D}_1.$$

Ποίο είναι το αντίστοιχο ζεύγος αρτίων διττών κωδίκων;

(Η άσκηση αυτή μας δίνει την δυνατότητα (δυϊκά) πρώτα να ορίζουμε τα ζεύγη των περιττών διττών κωδίκων και μετά τα ζεύγη των αρτίων διττών κωδίκων.)

2. Έστω $x^{23}-1 = (x-1)\cdot(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1)\cdot(x^{11}+x^9+x^7+x^6+x^5+x+1) \in \mathbb{Z}_2[x]$. Θέτουμε $g_1(x) = x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$ και $g_2(x) = x^{11}+x^9+x^7+x^6+x^5+x+1$. Έστω $\mathcal{D}_1 = \langle g_1(x)\rangle$ και $\mathcal{D}_2 = \langle g_2(x)\rangle$ οι κυκλικοί κώδικες με πολυώνυμα γεννήτορες τα $g_1(x)$ και $g_2(x)$ αντίστοιχα.

   (α′) Να βρεθούν αδύναμοι γεννήτορες $d_1(x)$, $d_2(x)$ για τους $\mathcal{D}_1$ και $\mathcal{D}_2$ αντίστοιχα.

   (β′) Δείξτε ότι οι $\mathcal{D}_1$ και $\mathcal{D}_2$ αποτελούν ένα ζεύγος περιττών διττών κωδίκων.

   (γ′) Να υπολογίσετε αδύναμους γεννήτορες για το αντίστοιχο ζεύγος των αρτίων διττών κωδίκων.

3. Θεωρώντας γνωστό ότι $x^7-1 = (x-1)(x^3+x+1)(x^3+x^2+1) \in \mathbb{Z}_2[x]$ και ότι $x^{11}-1 = (x-1)(x^5+x^4-x^3+x^2-1)(x^5-x^3+x^2-x-1) \in \mathbb{Z}_3[x]$, να υπολογίσετε όλα τα δυνατά ζεύγη αρτίων διττών κωδίκων μήκους 7 επί του $\mathbb{Z}_2$ και μήκους 11 επί του $\mathbb{Z}_3$. Συγκρίνατε με τα Παραδείγματα 4.5.5.

4. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας θετικός ακέραιος πρώτος προς τον q. Έστω $U(\mathbb{Z}_n)$ η πολλαπλασιαστική ομάδα του δακτυλίου $\mathbb{Z}_n$, Q η κυκλική υποομάδα της $U(\mathbb{Z}_n)$ η παραγομένη από το q και T ένα σύστημα αντιπροσώπων της Q στην $U(\mathbb{Z}_n)$.

   Έστω $\mathcal{C}_1$ και $\mathcal{C}_2$ ένα ζεύγος αρτίων κωδίκων, μήκους n επί του σώματος $\mathbb{F}$, με q το πλήθος στοιχεία. Δείξτε ότι στον έλεγχο, αν οι δύο αυτοί

κώδικες αποτελούν ζεύγος διττών κωδίκων, για να δούμε αν πληρούται η συνθήκη (β) του Ορισμού 4.5.2 πρέπει και αρκεί να ελέγξουμε τους πολλαπλασιαστές ϱ_a, όπου $a \in T$.

Υπόδειξη: Επικαλεσθήτε την Παρατήρηση 4.5.11.

5. Ποίοι είναι οι πολλαπλασιαστές που πρέπει να θεωρήσουμε, όταν κατασκευάζουμε διττούς κώδικες μήκους n επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία στις ακόλουθες περιπτώσεις;

   (i) $n = 5, \quad q = 4$

   (ii) $n = 7, \quad q = 4$

   (iii) $n = 15, \quad q = 4$

   (iv) $n = 13, \quad q = 3$

   (v) $n = 23, \quad q = 2$.

6. Σε κάθε μια από τις περιπτώσεις στην προηγούμενη άσκηση να υπολογίσετε όλα τα ζεύγη των αρτίων διττών κωδίκων που μπορούν να κατασκευασθούν, καθώς, επίσης, και τους αντίστοιχους δυϊκούς κώδικες.

7. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Δείξτε ότι το ζεύγος $\mathcal{C}_1,\ \mathcal{C}_2$ αποτελεί ένα ζεύγος αρτίων διττών κωδίκων (αντίστοιχα το ζεύγος $\mathcal{D}_1,\ \mathcal{D}_2$ αποτελεί ένα ζεύγος περιττών διττών κωδίκων) μήκους n, με αντίστοιχη διαμέριση του συνόλου $S = \{1, 2, \ldots, n-1\}$ σε δύο υποσύνολα S_1 και S_2, αν και μόνο αν για οποιονδήποτε πολλαπλασιαστή ϱ_c το ζεύγος $(\mathcal{C}_1)_{\varrho_c},\ (\mathcal{C}_2)_{\varrho_c}$ αποτελεί ένα ζεύγος αρτίων διττών κωδίκων [αντίστοιχα το ζεύγος $(\mathcal{D}_1)_{\varrho_c},\ (\mathcal{D}_2)_{\varrho_c}$ αποτελεί ένα ζεύγος περιττών διττών κωδίκων] μήκους n, με αντίστοιχη διαμέριση του συνόλου $S = \{1, 2, \ldots, n-1\}$ στα υποσύνολα $\varrho_{c^{-1}}(S_1)$ και $\varrho_{c^{-1}}(S_2)$.

8. Έστω n_1 και n_2 δύο σχετικά πρώτοι θετικοί ακέραιοι και $n = n_1 \cdot n_2$. Δείξτε ότι η απεικόνιση $\theta : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ με $\theta(a \mod n) = (a \mod n_1,\ a \mod n_2)$ είναι ένας ισομορφισμός δακτυλίων.

9. Έστω p ένας πρώτος, a ένας ακέραιος και ν ένας θετικός ακέραιος. Δείξτε ότι υπάρχει ακέραιος b, έτσι ώστε $(1+ap)^{\nu-1} = 1 + bp^{\nu}$.

10. Να βρεθούν όλοι οι ακέραιοι $3 < n < 200$ για τους οποίους υπάρχουν διττοί κώδικες μήκους n επί του σώματος $\mathbb{Z}_2$ και επί του σώματος $\mathbb{Z}_3$.

11. Να αποδείξετε λεπτομερώς όλους τους ισχυρισμούς που επικαλούμαστε στην απόδειξη του Λήμματος 4.5.22.

12. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

4.6 Κώδικες τετραγωνικών υπολοίπων

Στην προηγούμενη παράγραφο μελετήσαμε την ύπαρξη και ιδιότητες διττών κωδίκων μήκους n επί ενός σώματος $\mathbb{F}$ με q το πλήθος στοιχεία.

Η πλέον ενδιαφέρουσα κατηγορία διττών κωδίκων είναι οι διττοί κώδικες, των οποίων το μήκος είναι ένας περιττός πρώτος. Οι κώδικες αυτοί ονομάζονται κώδικες τετραγωνικών υπολοίπων.

Πριν δώσουμε τον (αυστηρό) ορισμό τους, θα υπενθυμίσουμε ορισμένα αποτελέσματα.

Εις το εξής θα υποθέτουμε ότι $n = p$, όπου p είναι περιττός πρώτος.

Υπενθυμίζουμε ότι το σύνολο των μη μηδενικών στοιχείων του σώματος $\mathbb{Z}_p$, τα οποία είναι τετραγωνικά υπόλοιπα $\mod p$ το συμβολίζουμε με Q_p και το σύνολο των μη μηδενικών στοιχείων του σώματος $\mathbb{Z}_p$, τα οποία είναι μη τετραγωνικά υπόλοιπα $\mod p$ το συμβολίζουμε με N_p.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και p ένας περιττός πρώτος, ο οποίος είναι πρώτος προς τον q. Αν ω είναι μια πρωταρχική p-οστή ρίζα της μονάδος επί του σώματος $\mathbb{F}$, τότε το σύνολο $E = \{\omega, \omega^2, \ldots, \omega^{p-1}\}$ διαμερίζεται σε δύο υποσύνολα $E_1 = \{\omega^i \mid i \in Q_p\}$ και $E_2 = \{\omega^j \mid j \in N_p\}$.

Από το Λήμμα 4.5.19 έπεται ότι τα δύο αυτά σύνολα έχουν τις εξής ιδιότητες:

Για κάθε $b \in N_p$ ισχύει ότι $\varrho_b(E_1) = \{\omega^{ib} \mid \omega^i \in E_1\} = E_2$ και $\varrho_b(E_2) = \{\omega^{jb} \mid \omega^j \in E_2\} = E_1$.

Κάθε ένα από τα E_1 και E_2 είναι ένωση κλάσεων συζυγίας, αν και μόνο αν $q \in Q_p$.

Επομένως τα σύνολα Q_p και N_p είναι ένωση κυκλοτομικών συμπλόκων, αν και μόνο αν $q \in Q_p$.

(Για τον ορισμό των κλάσεων συζυγίας και των κυκλοτομικών συμπλόκων πρέπει να ανατρέξετε στο Παράρτημα στις σελίδες 442 και 451.)

Με τις προηγούμενες προϋποθέσεις έχουμε ότι τα πολυώνυμα $q(x) = \prod_{i \in Q_p}(x - \omega^i)$ και $n(x) = \prod_{j \in N_p}(x - \omega^j)$ έχουν συντελεστές στο σώμα $\mathbb{F}$.

Ορισμός 4.6.1. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και p ένας περιττός πρώτος, ο οποίος είναι πρώτος προς τον q. Υποθέτουμε ότι ο q είναι τετραγωνικό υπόλοιπο $\mod p$.*

Οι κυκλικοί κώδικες, μήκους p, $\mathcal{Q}_p = \langle q(c) \rangle$ και $\mathcal{N}_p = \langle n(x) \rangle$ αποτελούν ένα ***ζεύγος περιττών κωδίκων τετραγωνικών υπολοίπων.***

Οι κυκλικοί κώδικες, μήκους p, $\overline{\mathcal{Q}}_p = \langle (x-1)q(c) \rangle$ και $\overline{\mathcal{N}}_p = \langle (x-1)n(x) \rangle$ αποτελούν ένα ***ζεύγος αρτίων κωδίκων τετραγωνικών υπολοίπων.***

Παρατηρήσεις 4.6.2.

1. Από την Παρατήρηση 4.5.9 έπεται ότι οι κώδικες τετραγωνικών υπολοίπων είναι πράγματι διττοί κώδικες.

2. Όπως είδαμε το σύνολο Q_p, των τετραγωνικών υπολοίπων και το σύνολο N_p, των μη τετραγωνικών υπολοίπων διαμερίζουν το σύνολο $S = \{1, 2, \ldots, p-1\}$ σύμφωνα με την Παρατήρηση 4.5.7, αν και μόνο αν το q είναι τετραγωνικό υπόλοιπο $\mod p$. Αυτό συνάδει με το Θεώρημα 4.5.23.

Παραδείγματα 4.6.3.

1. Ως γνωστόν, $x^{23} - 1 = (x-1) \cdot (x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1) \cdot (x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1) \in \mathbb{Z}_2[x]$.

   Εύκολα βλέπουμε ότι το 2 είναι τετραγωνικό υπόλοιπο $\mod 23$. Έστω ω μια πρωταρχική 23^η ρίζα της μονάδος επί του σώματος $\mathbb{Z}_2$. Τότε $x^{23} - 1 = (x-1) \cdot q(x) \cdot n(x)$, όπου τα πολυώνυμα $q(x) = \prod_{i \in Q_{23}}(x - \omega^i)$ και $n(x) = \prod_{j \in N_{23}}(x - \omega^j)$ έχουν συντελεστές στο σώμα $\mathbb{Z}_2$. Συνεπώς,

ο κώδικας Golay $\mathcal{G}_{23}$ είναι ισοδύναμος με τον κώδικα τετραγωνικών υπολοίπων $\mathcal{Q}_{23} = \langle q(c) \rangle$.

Όμοια έχουμε ότι $x^{11} - 1 = (x-1) \cdot (x^5 + x^4 - x^3 + x^2 - 1) \cdot (x^5 - x^3 + x^2 - x - 1) \in \mathbb{Z}_3[x]$.

Εύκολα βλέπουμε ότι το 3 είναι τετραγωνικό υπόλοιπο $\mod 11$. Έστω ζ μια πρωταρχική 11^η ρίζα της μονάδος επί του σώματος $\mathbb{Z}_3$. Τότε $x^{11} - 1 = (x-1) \cdot q(x) \cdot n(x)$, όπου τα πολυώνυμα $q(x) = \prod_{i \in Q_{11}} (x - \zeta^i)$ και $n(x) = \prod_{j \in N_{11}} (x - \zeta^j)$ έχουν συντελεστές στο σώμα $\mathbb{Z}_3$. Συνεπώς, ο Golay κώδικας $\mathcal{G}_{11}$ είναι ισοδύναμος με τον κώδικα τετραγωνικών υπολοίπων $\mathcal{Q}_{11} = \langle q(c) \rangle$.

2. Έστω $x^7 - 1 = (x-1) \cdot (x^3 + x + 1) \cdot (x^3 + x^2 + 1) \in \mathbb{Z}_2$.

   Εύκολα βλέπουμε ότι το 2 είναι τετραγωνικό υπόλοιπο $\mod 7$. Έστω ω μια πρωταρχική 7^η ρίζα της μονάδος επί του σώματος $\mathbb{Z}_2$, η οποία μηδενίζει το πολυώνυμο $x^3 + x + 1$, τότε $q(x) = x^3 + x + 1 = (x - \omega)(x - \omega^2)(x - \omega^4)$ και $n(x) = x^3 + x^2 + 1 = (x - \omega^3)(x - \omega^5)(x - \omega^6)$.

   Όπως βλέπουμε ο κώδικας τετραγωνικών υπολοίπων $\mathcal{Q}_7 = \langle q(c) \rangle$ είναι ισοδύναμος με τον κώδικα Hamming $\mathcal{H}(3, 2)$ (ιδέ Θεώρημα 4.1.9).

Παρατήρηση 4.6.4. Στον ορισμό των κωδίκων τετραγωνικών υπολοίπων λαμβάνουμε αυθαίρετα μια πρωταρχική p-οστή ρίζα της μονάδος. Οπότε, ευλόγως, γεννάται το ερώτημα. Τι συμβαίνει αν λάβουμε μια άλλη πρωταρχική ρίζα της μονάδος;

Έστω ω, ζ δύο πρωταρχικές p-οστες ρίζες της μονάδας επί του πεπερασμένου σώματος $\mathbb{F}$. Θέτουμε $q_\omega(x) = \prod_{i \in Q_p} (x - \omega^i)$, $q_\zeta(x) = \prod_{i \in Q_p} (x - \zeta^i)$ και $n_\omega(x) = \prod_{i \in N_p} (x - \omega^i)$, $n_\zeta(x) = \prod_{i \in N_p} (x - \zeta^i)$.

Ως γνωστόν για τις δύο ρίζες ω και ζ υπάρχει k πρώτος προς τον p, έτσι ώστε $\zeta = \omega^k$. Διακρίνουμε δύο περιπτώσεις:

Αν $k \in Q_p$, τότε προφανώς (γιατί;) $q_\omega(x) = q_\zeta(x)$ και $n_\omega(x) = n_\zeta(x)$.

Αν $k \in N_p$, τότε προφανώς (γιατί;) $q_\omega(x) = n_\zeta(x)$ και $n_\omega(x) = q_\zeta(x)$.

Επομένως, το αυθαίρετο της επιλογής της πρωταρχικής p-οστης ρίζας της μονάδας δεν επηρεάζει τη δομή των κωδίκων τετραγωνικών υπολοίπων, απλώς ενδέχεται να εναλλάσσονται οι δύο κώδικες $\mathcal{Q}_p$ και $\mathcal{N}_p$.

Οι κώδικες τετραγωνικών υπολοίπων, ως ειδική κατηγορία διττών κωδίκων, πληρούν όλες τις ιδιότητες διττών κωδίκων, που έχουμε αποδείξει στην προηγούμενη παράγραφο.

Οι διττοί κώδικες έχουν ορισθεί (Ορισμός 4.5.2) με τη βοήθεια αδυνάμων γεννητόρων. Στα επόμενα θα περιγράψουμε τους αδύναμους γεννήτορες κωδίκων τετραγωνικών υπολοίπων.

Πρόταση 4.6.5. *Έστω p ένας περιττός πρώτος και $\mathcal{C}$ ένας κώδικας τετραγωνικών υπολοίπων μήκους p επί ενός πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία.*

Υποθέτουμε ότι το $\epsilon(x)$ είναι ο αδύναμος γεννήτορας του κώδικα $\mathcal{C}$. Τότε για κάθε $c \in Q_p$ ισχύει ότι $\varrho_c(\epsilon(x)) = \epsilon(x)$. Μάλιστα δε το $\epsilon(x)$ είναι της μορφής $\epsilon(x) = a_0 + a_1 \sum_{i \in Q_p} x^i + a_2 \sum_{j \in N_p} x^j$, $a_0, a_1, a_2 \in \mathbb{F}$.

Απόδειξη. Από τον ορισμό των κωδίκων τετραγωνικών υπολοίπων έχουμε ότι $\mathcal{C}_{\varrho_c} = \mathcal{C}$, για κάθε $c \in Q_p$. Οπότε, προφανώς, έχουμε ότι $\varrho_c(\epsilon(x)) = \epsilon(x)$ (ιδέ Πρόταση 3.2.38).

Υποθέτουμε ότι $\epsilon(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1} \in \mathcal{R}_p$. *Ομαδοποιούμε* τους συντελεστές a_i σε δύο κατηγορίες, σ' αυτούς που ο εκθέτης του αντίστοιχου x^i ανήκει στο σύνολο Q_p και σ' αυτούς που ο εκθέτης του αντίστοιχου x^i ανήκει στο σύνολο N_p. Από το Λήμμα 4.5.19 και το γεγονός ότι $\varrho_c(\epsilon(x)) = \epsilon(x^c)$ έπεται άμεσα ότι $\epsilon(x) = a_0 + a_1 \sum_{i \in Q_p} x^i + a_2 \sum_{j \in N_p} x^j$, $a_0, a_1, a_2 \in \mathbb{F}$. ό.έ.δ.

Στα επόμενα θα επικεντρωθούμε στη μελέτη κωδίκων τετραγωνικών υπολοίπων επί σωμάτων χαρακτηριστικής ίσης με 2 ή 3.

Θεώρημα 4.6.6. *Έστω p ένας περιττός πρώτος και $\mathbb{F}$ ένα πεπερασμένο σώμα με 2^t το πλήθος στοιχεία.*

Αν ο t είναι άρτιος, τότε πάντα υπάρχουν κώδικες τετραγωνικών υπολοίπων μήκους p επί του $\mathbb{F}$.

Αν ο t είναι περιττός, τότε υπάρχουν κώδικες τετραγωνικών υπολοίπων μήκους p επί του $\mathbb{F}$ αν, και μόνο αν $p \equiv \pm 1 \mod 8$.

Θεώρημα 4.6.7. *Έστω $p \neq 3$ ένας περιττός πρώτος και $\mathbb{F}$ ένα πεπερασμένο σώμα με 3^t το πλήθος στοιχεία.*

Αν ο t είναι άρτιος, τότε πάντα υπάρχουν κώδικες τετραγωνικών υπολοίπων μήκους p επί του $\mathbb{F}$.

Αν ο t είναι περιττός, τότε υπάρχουν κώδικες τετραγωνικών υπολοίπων μήκους p επί του $\mathbb{F}$, αν και μόνο αν $p \equiv \pm 1 \mod 12$.

Απόδειξη. Η απόδειξη και των δύο θεωρημάτων έπεται άμεσα, ως πόρισμα, από το Πόρισμα 4.5.25, το Θεώρημα 4.5.28 και το δεύτερο σκέλος του Λήμματος 4.5.21. ό.έ.δ.

Πρόταση 4.6.8. *Έστω p ένας περιττός πρώτος με $p \equiv \pm 1 \mod 8$.*

Έστω $\epsilon(x) = \sum_{i \in Q_p} x^i$ και $f(x) = \sum_{i \in N_p} x^i$. Τότε ισχύουν τα ακόλουθα:

i) Υποθέτουμε ότι $p \equiv -1 \mod 8$.

Οι περιτοί δυαδικοί κώδικες τετραγωνικών υπολοίπων $\mathcal{Q}_p$ και $\mathcal{N}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $\epsilon(x)$ και $f(x)$ αντίστοιχα.

Οι άρτιοι δυαδικοί κώδικες τετραγωνικών υπολοίπων $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $1 + f(x)$ και $1 + \epsilon(x)$ αντίστοιχα.

ii) Υποθέτουμε ότι $p \equiv 1 \mod 8$.

Οι περιτοί δυαδικοί κώδικες τετραγωνικών υπολοίπων $\mathcal{Q}_p$ και $\mathcal{N}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $1 + f(x)$ και $1 + \epsilon(x)$ αντίστοιχα.

Οι άρτιοι δυαδικοί κώδικες τετραγωνικών υπολοίπων $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $\epsilon(x)$ και $f(x)$ αντίστοιχα.

Απόδειξη. Είναι εύκολο να δούμε ότι τα πολυώνυμα $\epsilon(x)$, $f(x)$, $1 + \epsilon(x)$ και $1 + f(x)$ είναι πράγματι αδύναμα.

Έστω ω μια πρωταρχική p-οστή ρίζα της μονάδας επί του $\mathbb{Z}_2$. Τότε είναι εύκολο να δούμε ότι ισχύει μια από τις περιπτώσεις:

$\epsilon(\omega^s) = 0$, αν $s \in Q_p$ και $\epsilon(\omega^s) = 1$, αν $s \in N_p$

ή $\epsilon(\omega^s) = 1$, αν $s \in Q_p$ και $\epsilon(\omega^s) = 0$, αν $s \in N_p$ (γιατί;).

Από την Παρατήρηση 4.6.4 έπεται ότι μπορούμε χωρίς βλάβη να επιλέξουμε την ρίζα ω, ώστε να ισχύει η πρώτη περίπτωση.

Επίσης έχουμε ότι:

$$\epsilon(1) = (p-1)/2 = \begin{cases} 1 & \text{αν } p = 8m-1 \\ 0 & \text{αν } p = 8m+1 \end{cases}$$

Έστω $\mathcal{Q}_p$ και $\mathcal{N}_p$ οι περιττοί κώδικες τετραγωνικών υπολοίπων που έχουν ως πολυώνυμα γενήτορες τα πολυώνυμα $q(x) = \prod_{i \in Q_p}(x - \omega^i)$ και $n(x) = \prod_{j \in N_p}(x - \omega^j)$ αντίστοιχα. Τότε, στην περίπτωση όπου $p = 8m-1$, προφανώς έχουμε ότι $\mathcal{Q}_p = \langle q(x) \rangle = [[\epsilon(x)]]$ και $\mathcal{N}_p = \langle n(x) \rangle = [[f(x)]]$ (ιδέ Πρόταση 3.2.8).

Από τον Ορισμό 4.6.1 έπονται όλες οι υπόλοιπες περιπτώσεις. ό.έ.δ.

Παρατηρήσεις 4.6.9. 1. Από την Πρόταση 4.6.5 έχουμε ότι για κάθε έναν από τους τέσσερεις κώδικες $\mathcal{Q}_p$, $\mathcal{N}_p$ και $\overline{\mathcal{Q}}_p$, $\overline{\mathcal{N}}_p$ ο αδύναμος γεννήτορας είναι της μορφής $a_0 + a_1 \sum_{i \in Q_p} x^i + a_2 \sum_{j \in N_p} x^j$, με $a_0, a_1, a_2 \in \mathbb{Z}_2$.

Επομένως, στην προηγουμένη πρόταση θα μπορούσαμε να υπολογίσουμε τους αδύναμους γεννήτορες, υπολογίζοντας σε κάθε περίπτωση τα a_0, a_1 και a_2.

2. Έστω $\mathbb{F}$ ένα σώμα με 2^t το πλήθος στοιχεία. Από το Θεώρημα 4.6.6 έχουμε ότι, αν ο t είναι περιττός, τότε υπάρχουν κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{F}$ μήκους p, αν και μόνο αν ο περιττός πρώτος p είναι της μορφής $p \equiv \pm 1 \mod 8$. Στην περίπτωση αυτή οι αδύναμοι γεννήτορες, που έχουν υπολογισθεί, στην προηγουμένη πρόταση, για τους τέσσερεις κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{Z}_2$ παραμένουν αδύναμα πολυώνυμα αν θεωρηθούν επί του σώματος $\mathbb{F}$. Επομένως, (εξακολουθούν να) αποτελούν τους αδύναμους γεννήτορες για τους τέσσερεις κώδικες τετραγωνικών υπολοίπων επί του σώματος $\mathbb{F}$.

Επίσης, από το Θεώρημα 4.6.6 έχουμε ότι, αν ο t είναι άρτιος, τότε υπάρχουν κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{F}$ μήκους p για οποιονδήποτε περιττό πρώτο. Για $p \equiv \pm 1 \mod 8$ έχουμε τους αδύναμους γεννήτορες που έχουν υπολογισθεί στην προηγούμενη πρόταση. Για $p \equiv \pm 3 \mod 8$ οι αντίστοιχοι αδύναμοι γεννήτορες μπορούν να υπολογισθούν από την Πρόταση 4.6.5 υπολογίζοντας σε κάθε περίπτωση τα αντίστοιχα a_0, a_1 και a_2 (ιδέ Άσκηση 4.6.1 $_4$).

Για τους αδύναμους γεννήτορες κωδίκων τετραγωνικών υπολοίπων επί του σώματος $\mathbb{Z}_3$ ισχύει η ακόλουθη πρόταση.

Πρόταση 4.6.10. *Έστω $p > 3$ ένας πρώτος με $p \equiv \pm 1 \mod 12$.*

Έστω $\epsilon(x) = \sum_{i \in Q_p} x^i$ και $f(x) = \sum_{i \in N_p} x^i$. Τότε ισχύουν τα ακόλουθα:

i) Υποθέτουμε ότι $p \equiv 1 \mod 12$.

Οι περιτοί τριαδικοί κώδικες τετραγωνικών υπολοίπων $\mathcal{Q}_p$ και $\mathcal{N}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $1 + \epsilon(x)$ και $1 + f(x)$ αντίστοιχα.

Οι άρτιοι τριαδικοί κώδικες τετραγωνικών υπολοίπων $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $-\epsilon(x)$ και $-f(x)$ αντίστοιχα.

ii) Υποθέτουμε ότι $p \equiv -1 \mod 12$.

Οι περιτοί τριαδικοί κώδικες τετραγωνικών υπολοίπων $\mathcal{Q}_p$ και $\mathcal{N}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $-\epsilon(x)$ και $-f(x)$ αντίστοιχα.

Οι άρτιοι τριαδικοί κώδικες τετραγωνικών υπολοίπων $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ έχουν αδύναμους γεννήτορες τα πολυώνυμα $1 + \epsilon(x)$ και $1 + f(x)$ αντίστοιχα.

Απόδειξη. Από την Πρόταση 4.6.5 έχουμε ότι για κάθε έναν από τους τέσσερεις κώδικες $\mathcal{Q}_p$, $\mathcal{N}_p$ και $\overline{\mathcal{Q}}_p$, $\overline{\mathcal{N}}_p$ ο αδύναμος γεννήτορας είναι της μορφής $a_0 + a_1 \sum_{i \in Q_p} x^i + a_2 \sum_{j \in N_p} x^j$, με $a_0, a_1, a_2 \in \mathbb{Z}_3$. Οπότε θα πρέπει σε κάθε περίπτωση να υπολογίσουμε τους συντελεστές a_0, a_1 και a_2.

Υποθέτουμε ότι ο αδύναμος γεννήτορας του κώδικα $\overline{\mathcal{Q}}_p$ είναι το πολυώνυμο $\phi(x) = a_0 + a_1 \sum_{i \in Q_p} x^i + a_2 \sum_{j \in N_p} x^j$. Τότε ο αδύναμος γεννήτορας του $\overline{\mathcal{N}}_p$ είναι το πολυώνυμο $\varrho_b(\phi(x))$, όπου $b \in N_p$. Από το Λήμμα 4.5.19 έχουμε ότι $\varrho_b(\epsilon(x)) = \epsilon(x^b) = f(x)$ και $\varrho_b(f(x)) = f(x^b) = \epsilon(x)$. Συνεπώς, $\varrho_b(\phi(x)) = a_0 + a_2 \sum_{i \in Q_p} x^i + a_1 \sum_{j \in N_p} x^j$.

Θεωρούμε την περίπτωση $p \equiv 1 \mod 12$. Από τον ορισμό των διττών κωδίκων (Ορισμός 4.5.2) έχουμε ότι $\phi(x) + \varrho_b(\phi(x)) = 1 - \vartheta(x) = -x - x^2 - \cdots - x^{p-1}$, όπου $\vartheta(x) = 1 - (1/n) \cdot (x^{n-1} + x^{n-2} + \cdots x + 1)$. Από την τελευταία σχέση έπεται ότι $2a_0 = 0$ και $a_1 + a_2 = -1$. Δηλαδή έχουμε ότι $a_0 = 0$ και είτε $a_1 = a_2 = 1$ είτε $a_1 = 0, a_2 = -1$ (ή $a_1 = -1, a_2 = 0$).

Στην περίπτωση, όπου $a_1 = a_2 = 1$, έχουμε:

$$\phi(x) = \sum_{i \in Q_p} x^i + \sum_{j \in N_p} x^j = -(1 - \vartheta(x)).$$

Άτοπο, από το Λήμμα 4.5.1 και το Θεώρημα 4.5.4. Συνεπώς, έχουμε ότι $a_1 = 0$, $a_2 = -1$ (ή $a_1 = -1$, $a_2 = 0$). Δηλαδή πράγματι οι αδύναμοι γεννήτορες για τους άρτιους κώδικες $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ έχουν πολυώνυμα αδύναμους γεννήτορες τα $-\epsilon(x)$ και $-f(x)$ αντίστοιχα.

Για τους αντίστοιχους περιττούς κώδικες $\mathcal{Q}_p$ και $\mathcal{N}_p$ οι αδύναμοι γεννήτορες προφανώς είναι τα $1+\epsilon(x)$ και $1+f(x)$ (ιδέ τον Ορισμό 4.5.2).

Η περίπτωση, όπου $p \equiv -1 \mod 12$ αντιμετωπίζεται αναλόγως, καθότι στην περίπτωση αυτή έπεται ότι $2a_0 = -1$ και $a_1 + a_2 = 1$. (Να κάνετε τον έλεγχο και να συνεχίσετε.) ό.έ.δ.

Παρατήρηση 4.6.11. Έστω $\mathbb{F}$ ένα σώμα με 3^t το πλήθος στοιχεία. Από το Θεώρημα 4.6.7 έχουμε ότι, αν ο t είναι περιττός, τότε υπάρχουν κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{F}$ μήκους p, αν και μόνο αν ο περιττός πρώτος p είναι της μορφής $p \equiv \pm 1 \mod 12$. Στην περίπτωση αυτή οι αδύναμοι γεννήτορες, που έχουν υπολογισθεί, στην προηγούμενη πρόταση, για τους τέσσερεις κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{Z}_3$ παραμένουν αδύναμα πολυώνυμα αν θεωρηθούν επί του σώματος $\mathbb{F}$. Επομένως, (εξακολουθούν να) αποτελούν τους αδύναμους γεννήτορες για τους τέσσερεις κώδικες τετραγωνικών υπολοίπων επί του σώματος $\mathbb{F}$.

Επίσης, από το Θεώρημα 4.6.7 έχουμε ότι, αν ο t είναι άρτιος, τότε υπάρχουν κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{F}$ μήκους p για οποιονδήποτε περιττό πρώτο ($p \neq 3$). Για $p \equiv \pm 1 \mod 12$ έχουμε τους αδύναμους γεννήτορες που έχουν υπολογισθεί στην προηγούμενη πρόταση. Για $p \equiv \pm 5 \mod 12$ οι αντίστοιχοι αδύναμοι γεννήτορες μπορούν να υπολογισθούν από την Πρόταση 4.6.5 υπολογίζοντας σε κάθε περίπτωση τα αντίστοιχα a_0, a_1 και a_2. (Προσπαθήστε το στην περίπτωση, όπου έχουμε ένα σώμα $\mathbb{F}$ με 3^2 το πλήθος στοιχεία).

Παράδειγμα 4.6.12. Το 2 είναι τετραγωνικό υπόλοιπο $\mod 23$. Στην περίπτωση αυτή έχουμε ότι $Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ και $N_{23} = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$. Οπότε, από την Πρόταση 4.6.8, μπορούμε να υπολογίσουμε τους αδύναμους γεννήτορες και για τους τέσσερεις δυαδικούς κώδικες τετραγωνικών υπολοίπων μήκους 23. Παρατηρήστε ότι οι

κώδικες $\mathcal{Q}_{23}$ και $\mathcal{N}_{23}$ είναι ισοδύναμοι με τον κώδικα Golay $\mathcal{G}_{23}$.

Το 3 είναι τετραγωνικό υπόλοιπο $\mod 11$. Στην περίπτωση αυτή έχουμε ότι $Q_{11} = \{1, 3, 4, 5, 9\}$ και $N_{11} = \{2, 6, 7, 8, 10\}$. Οπότε, από την Πρόταση 4.6.10, μπορούμε να υπολογίσουμε τους αδύναμους γεννήτορες και για τους τέσσερεις τριαδικούς κώδικες τετραγωνικών υπολοίπων μήκους 11. Παρατηρήστε ότι οι κώδικες $\mathcal{Q}_{11}$ και $\mathcal{N}_{11}$ είναι ισοδύναμοι με τον κώδικα Golay $\mathcal{G}_{11}$.

Να συγκρίνετε το προηγούμενο παράδειγμα με το Παράδειγμα $4.6.3_1$. Παρατηρήστε (για άλλη μια φορά) ότι με την χρήση των αδύναμων γεννητόρων μπορούμε να αποφύγουμε την παραγοντοποίηση πολυωνύμων της μορφής $x^n - 1$ για τον υπολογισμό των αντίστοιχων κυκλικών κωδίκων.

Ενδιαφέρον παρουσιάζουν οι κώδικες μηδενικού αθροίσματος, οι οποίοι προέρχονται ως επέκταση κωδίκων τετραγωνικών υπολοίπων.

Ως γνωστόν, αν έχουμε έναν κώδικα $\mathcal{C}$ μήκους n επί ενός πεπερασμένου σώματος $\mathbb{F}$, η μηδενικού αθροίσματος επέκτασή του είναι ο κώδικας $\widehat{\mathcal{C}} = \{\, a_1a_2\cdots a_na_{n+1} \mid a_1a_2\cdots a_n \in \mathcal{C} \text{ και } a_{n+1} = -\sum_{i=1}^{n} a_i \,\}$.

Θεώρημα 4.6.13. *Έστω $\mathcal{Q}_p$ και $\mathcal{N}_p$ οι περιττοί κώδικες τετραγωνικών υπολοίπων με μήκος τον περιττό πρώτο p επί του σώματος $\mathbb{Z}_q$.*

1. *Υποθέτουμε ότι $q = 2$.*

   i) Αν $p \equiv 1 \mod 8$, τότε οι κώδικες $\widehat{\mathcal{Q}_p}$ και $\widehat{\mathcal{N}_p}$ είναι ο ένας δυϊκός του άλλου.

   ii) Αν $p \equiv -1 \mod 8$, τότε οι κώδικες $\widehat{\mathcal{Q}_p}$ και $\widehat{\mathcal{N}_p}$ είναι αυτοδυϊκοί. Επιπλέον ισχύει ότι, και στους δύο κώδικες, το βάρος κάθε κωδικολέξης είναι πολλαπλάσιο του 4.

2. *Υποθέτουμε ότι $q = 3$.*

   i) Αν $p \equiv -1 \mod 12$, τότε οι κώδικες $\widehat{\mathcal{Q}_p}$ και $\widehat{\mathcal{N}_p}$ είναι αυτοδυϊκοί.

   ii) Αν $p \equiv 1 \mod 12$, τότε οι κώδικες $\widehat{\mathcal{Q}_p}$ και $(\widehat{\mathcal{N}_p})_{\mathrm{D}}$ είναι ο ένας δυϊκός του άλλου. Όπου ο D είναι ο διαγώνιος πίνακας με στοιχεία στην κυρία διαγώνιο τα στοιχεία $1, 1, \cdots, 1, -1$.

Απόδειξη. Υπενθυμίζουμε (ιδέ σελίδα 106) ότι, αν P είναι ένας πίνακας ελέγχου ισοτιμίας ενός κώδικα $\mathcal{C}$, τότε ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\widehat{\mathcal{C}}$ είναι ο πίνακας:

$$\widehat{\mathrm{P}} = \begin{pmatrix} \mathbf{1} & 1 \\ \mathrm{P} & \mathbf{0} \end{pmatrix}.$$

1. Έστω $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ οι αντίστοιχοι άρτιοι κώδικες τετραγωνικών υπολοίπων.

   Στο πολυώνυμο $\vartheta(x) = (1/p)(x^{p-1} + x^{p-2} + \cdots x + 1)$ αντιστοιχεί η λέξη $1, 1, \cdots, 1$ μήκους p, οπότε αν την επεκτείνουμε σε μια λέξη μήκους $p+1$ μηδενικού αθροίσματος έχουμε μια λέξη μήκους $p+1$, της οποίας όλα τα στοιχεια είναι ίσα με 1. Η λέξη αυτή, προφανώς, είναι κάθετη προς τον εαυτό της.

   i) Υποθέτουμε ότι $p \equiv 1 \mod 8$. Στην περίπτωση αυτή, προφανώς, το -1 είναι τετραγωνικό υπόλοιπο και επομένως $(\overline{\mathcal{Q}}_p)_{\varrho_{-1}} = \overline{\mathcal{Q}}_p$ και $(\overline{\mathcal{N}}_p)_{\varrho_{-1}} = \overline{\mathcal{N}}_p$. Το αποτέλεσμα έπεται τώρα από το Θεώρημα 4.5.13.

   ii) Υποθέτουμε ότι $p \equiv -1 \mod 8$. Στην περίπτωση αυτή, προφανώς, το -1 δεν είναι τετραγωνικό υπόλοιπο και επομένως $(\overline{\mathcal{Q}}_p)_{\varrho_{-1}} = \overline{\mathcal{N}}_p$ και $(\overline{\mathcal{N}}_p)_{\varrho_{-1}} = \overline{\mathcal{Q}}_p$. Πάλι από το το Θεώρημα 4.5.13 έχουμε οι κώδικες $\widehat{\overline{\mathcal{Q}}_p}$ και $\widehat{\overline{\mathcal{N}}_p}$ είναι αυτοδυϊκοί.

   Θα δείξουμε ότι το βάρος κάθε λέξης είναι πολλαπλασιο του 4. Παρατηρούμε ότι σε καθ' έναν από τους περιττούς κώδικες $\mathcal{Q}_p$ και $\mathcal{N}_p$ ο αδύναμος γεννήτορας έχει βάρος ίσον με $(p-1)/2$ (ιδέ Πρόταση 4.6.8). Από την Πρόταση 3.2.31 έχουμε ότι ένας γεννήτορας πίνακας για τους κώδικες αυτούς προκύπτει από κυκλικές μεταθέσεις των συντελεστών του αντιστοίχου αδυνάμου γεννήτορα. Συνεπώς, οι κώδικες $\widehat{\mathcal{Q}_p}$ και $\widehat{\mathcal{N}_p}$ έχουν γεννήτορες πίνακες των οποίων οι γραμμές έχουν βάρος ίσον με $(p-1)/2 + 1 \equiv 0 \mod 4$.

2. Όπως προηγουμένως, έστω $\overline{\mathcal{Q}}_p$ και $\overline{\mathcal{N}}_p$ οι αντίστοιχοι άρτιοι κώδικες τετραγωνικών υπολοίπων.

   Στο πολυώνυμο $\vartheta(x) = (1/p)(x^{p-1} + x^{p-2} + \cdots x + 1)$ αντιστοιχεί η λέξη $1, 1, \cdots, 1$ μήκους p, οπότε αν την επεκτείνουμε σε μια λέξη μήκους $p+1$

μηδενικού αθροίσματος έχουμε μια λέξη μήκους $p+1$, της οποίας όλα τα στοιχεια είναι ίσα με 1 στην περίπτωση, όπου $p \equiv -1 \mod 12$. Η λέξη αυτή, προφανώς, είναι κάθετη προς τον εαυτό της.

Στην περίπτωση, όπου $p \equiv 1 \mod 12$, η λέξη μηδενικού αθροίσματος μήκους $p+1$ που προκύπτει είναι της μορφής $1, 1, \cdots, 1, -1$. Η λέξη αυτή δεν είναι κάθετη προς τον εαυτό της, αλλά είναι κάθετη προς τη λέξη $(1, 1, \cdots, 1, -1) \cdot \mathrm{D}$

i) Υποθέτουμε ότι $p \equiv -1 \mod 12$. Στην περίπτωση αυτή, προφανώς, το -1 δεν είναι τετραγωνικό υπόλοιπο και επομένως $(\overline{\mathcal{Q}}_p)_{\varrho_{-1}} = \overline{\mathcal{N}}_p$ και $(\overline{\mathcal{N}}_p)_{\varrho_{-1}} = \overline{\mathcal{Q}}_p$. Το αποτέλεσμα έπεται τώρα από το Θεώρημα 4.5.13.

ii) Υποθέτουμε ότι $p \equiv 1 \mod 12$. Στην περίπτωση αυτή, προφανώς, το -1 είναι τετραγωνικό υπόλοιπο και επομένως $(\overline{\mathcal{Q}}_p)_{\varrho_{-1}} = \overline{\mathcal{Q}}_p$ και $(\overline{\mathcal{N}}_p)_{\varrho_{-1}} = \overline{\mathcal{N}}_p$. Το αποτέλεσμα έπεται τώρα πάλι από το Θεώρημα 4.5.13. ό.έ.δ.

Παράδειγμα 4.6.14. Στο Παράδειγμα 4.6.12 είχαμε δει ότι: Οι περιττοί δυαδικοί κώδικες τετραγωνικών υπολοίπων μήκους 23, $\mathcal{Q}_{23}$ και $\mathcal{N}_{23}$, είναι ισοδύναμοι με τον κώδικα Golay $\mathcal{G}_{23}$ και οι περιττοί τριαδικοί κώδικες τετραγωνικών υπολοίπων μήκους 11, $\mathcal{Q}_{11}$ και $\mathcal{N}_{11}$, είναι ισοδύναμοι με τον κώδικα Golay $\mathcal{G}_{11}$.

Από το προηγούμενο θεώρημα έπεται ότι οι κώδικες $\widehat{\mathcal{Q}_{23}}$ και $\widehat{\mathcal{N}_{23}}$ είναι ισοδύναμοι με τον επεκτεταμένο κώδικα Golay $\mathcal{G}_{24}$ και οι κώδικες $\widehat{\mathcal{Q}_{11}}$ και $\widehat{\mathcal{N}_{11}}$ είναι ισοδύναμοι με τον επεκτεταμένο κώδικα Golay $\mathcal{G}_{12}$.

Παρατήρηση 4.6.15. Επισημαίνουμε ότι το Λήμμα 4.2.3, του οποίου η απόδειξη είχε δοθεί με στοιχειώδη επιχειρήματα, απορρέει ως πόρισμα του προηγουμένου Θεωρήματος.

4.6.1 Ασκήσεις

1. Να μελετήσετε τους δυαδικούς κώδικες τετραγωνικών υπολοίπων μήκους 17.

2. Για κάθε περιττό πρώτο $p < 29$ να μελετήσετε τους κώδικες τετραγωνικών υπολοίπων μήκους p επί του σώματος $\mathbb{Z}_3$. (Σε κάθε περίπτωση να υπολογίσετε τους αδύναμους γεννήτορες των κωδίκων αυτών.)

3. Δείξτε ότι για τους δυϊκούς κώδικες τετραγωνικών υπολοίπων επί του $\mathbb{Z}_2$ μήκους p ισχύουν τα εξής:

   Για $p \equiv -1 \mod 8$, έχουμε ότι

   $\mathcal{Q}_p^{\perp} = \overline{\mathcal{Q}}_p$ και $\mathcal{N}_p^{\perp} = \overline{\mathcal{N}}_p$.

   Για $p \equiv 1 \mod 8$, έχουμε ότι

   $\mathcal{Q}_p^{\perp} = \overline{\mathcal{N}}_p$ και $\mathcal{N}_p^{\perp} = \overline{\mathcal{Q}}_p$.

   Συγκρίνατε με το Θεώρημα 4.5.13.

   Υπολογίστε τους αδύναμους γεννήτορες για τους δυϊκούς κώδικες τετραγωνικών υπολοίπων με τη βοήθεια της Πρότασης 4.6.8 και με τη βοήθεια της Πρότασης 3.2.33.

4. *i)* Έστω $\mathbb{F} = \{0, 1, \omega, \omega^2\}$ το σώμα με τέσσερα στοιχεία. Με τη βοήθεια της Πρότασης 4.6.5 να υπολογίσετε τους αδύναμους γεννήτορες για τους κώδικες τετραγωνικών υπολοίπων, μήκους p, επί του $\mathbb{F}$ για κάθε περιττό πρώτο p.

   ii) Δείξτε ότι:

   Για τους περιττούς κώδικες τετραγωνικών υπολοίπων $\mathcal{Q}_5$, $\mathcal{N}_5$ μήκους 5 επί του σώματος $\mathbb{F} = \{0, 1, \omega, \omega^2\}$ οι αδύναμοι γεννήτορες είναι τα πολυώνυμα $1 + \omega(x + x^4) + \omega^2(x^2 + x^3)$ και $1 + \omega^2(x + x^4) + \omega(x^2 + x^3)$ αντίστοιχα.

   Για τους άρτιους κώδικες τετραγωνικών υπολοίπων $\overline{\mathcal{Q}}_5$, $\overline{\mathcal{N}}_5$ μήκους 5 επί του σώματος $\mathbb{F} = \{0, 1, \omega, \omega^2\}$ οι αδύναμοι γεννήτορες είναι τα πολυώνυμα $\omega(x+x^4)+\omega^2(x^2+x^3)$ και $\omega^2(x+x^4)+\omega(x^2+x^3)$ αντίστοιχα.

5. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

Βιβλιογραφία

Berlekamp, E. R. *"Algebraic Coding Theory"*. Laguna Hills, CA: Aegean Park Press, 1984.

Hall, J.I. *Notes on Coding Theory*. (σε ηλεκτρονική μορφή). www.math.msu.edu/~jhall.

Hamming, R. *"Coding and Information Theory"*. Prentice-Hall, Englewood Cliffs 2^{nd} Edition, 1986.

Hill, R. *"A First Course in Coding Theory"*. Oxford University Press, Oxford, 1986.

Huffman, C. W. and Pless, V. . *"Fundamentals of Error-Correcting Codes"*. Cambridge University Press, 2003.

Lidl, R. and Niederreiter H. . *"Introduction to finite fields and their applications"*. Cambridge University Prees, 2000.

MacWilliams, F.J. and Sloane, N.J.A. *"The Theory of Error-correcting Codes"*. North-Holland, Amsterdam, 1977.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*. Wiley, New York, 1998.

Walker, J. L. *"Codes and Curves"*, volume 7 of *Student Mathematical Library*. AMS, 2000.

Δ. Βάρσος. *Στοιχεία Αλγεβρικής Θεωρίας Κωδίκων*. Εκδόσεις Σοφία, 2005.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

Δ. Πουλάκης. *Αλγεβρικοί Κώδικες*. Εκδόσεις ΖΗΤΗ, 2010.

ΚΕΦΑΛΑΙΟ 5

Κώδικες Reed-Solomon και συναφείς κώδικες

Το 1959 ο Hocquenghen και, ανεξάρτητα, το 1960 οι Bose Ray-Chaudhuri επινόησαν μια κατηγορία κωδίκων τους λεγόμενους BCH κώδικες. Οι κώδικες αυτοί είναι πολύ σημαντικοί για πολλούς λόγους. Για παράδειγμα, έχουν ικανότητα διόρθωσης μεγάλου αριθμού λαθών ακόμη και αν το μήκος τους είναι σχετικά μικρό. Η κωδικοποίηση και αποκωδικοποίση γίνεται σχετικά εύκολα. Αποτελούν την βάση για κατασκευή άλλων κωδίκων. Το σπουδαιότερο όμως είναι ότι μπορούν να κατασκευασθούν επί ενός πεπερασμένου σώματος με *επιθυμητή* ελάχιστη απόσταση (κώδικες προσχεδιασμένης απόστασης).

Το μόνο, ίσως, μειονέκτημά τους είναι ότι το μήκος τους υπόκειται σε περιορισμό από το πλήθος των στοιχείων του σώματος επί του οποίου ορίζονται.

Αν και αρχικά είχαν επινοηθεί και μελετηθεί επί ενός πεπερασμένου σώματος χαρακτηριστικής 2 (και μάλιστα μόνον ορισμένες ειδικές περιπτώσεις), σχεδόν αμέσως η μελέτη τους γενικεύθηκε το 1961, από τους Gorenstein και Zierler, επί πεπερασμένων σωμάτων οποιασδήποτε χαρακτηριστικής p.

5.1 BCH Κώδικες

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Έστω n, δ θετικοί ακέραιοι με $2 \leq \delta \leq n$ και b ένας μη αρνητικός ακέραιος. Θα κατασκευάσουμε έναν πολυωνυμικό κώδικα επί του $\mathbb{F}$ με μήκος n και ελάχιστη απόσταση τουλάχιστον ίση με δ.

Επιλέγουμε τον ελάχιστο θετικό ακέραιο s με την ιδιότητα $q^s \geq n+1$.[1] Έστω $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ βαθμού s και α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Για κάθε $0 \leq i \leq \delta-2$ έστω $m_{i+1}(x)$ το ελάχιστο πολυώνυμο του α^{b+i} επί του $\mathbb{F}$ και $\gamma(x) = \varepsilon\kappa\pi(\, m_{i+1}(x),\ 0 \leq i \leq \delta-2\,)$. Δηλαδή το πολυώνυμο $\gamma(x)$ είναι το μικροτέρου βαθμού μονικό πολυώνυμο επί του $\mathbb{F}$, το οποίο έχει ως ρίζες τα στοιχεία $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$. (Παρατηρήστε ότι οι εκθέτες του α στις ρίζες του πολυωνύμου $\gamma(x)$ είναι διαδοχικοί ακέραιοι).

Ορισμός 5.1.1. *Ο πολυωνυμικός κώδικας (ιδέ τον Ορισμό 3.1.3) $\mathcal{BCH} = \mathcal{BCH}(n, \delta, \alpha, b)$ μήκους n με γεννήτορα πολυώνυμο το πολυώνυμο $\gamma(x) \in \mathbb{F}[x]$ ονομάζεται* ***BCH κώδικας*** *προσχεδιασμένης απόστασης δ επί του σώματος $\mathbb{F}$.*

Διαφορετικά θα μπορούσαμε να ορίσουμε έναν BCH κώδικα ως εξής:

$$\begin{aligned}\mathcal{BCH}(n, \delta, \alpha, b) &= \{\, f(x) \in \mathbb{F}_{n-1}[x] \mid \alpha^{b+i} \text{ είναι ρίζα του } f(x) \\ &\qquad\qquad \text{για όλα τα } 0 \leq i \leq \delta-2\,\} \\ &= \{\mathbf{r} = r_0 r_1 \cdots r_{n-1} \mid \text{το πολυώνυμο} \\ &\qquad r_0 + r_1 x + \cdots + r_{n-1}x^{n-1} \in \mathbb{F}_{n-1}[x] \text{ έχει ως ρίζες τα} \\ &\qquad\qquad \alpha^{b+i} \text{ για όλα τα } 0 \leq i \leq \delta-2\,\}.\end{aligned}$$

Παρατηρήσεις 5.1.2. 1. Έστω k ο βαθμός του πολυωνύμου $\gamma(x)$, τότε, επειδή κάθε πολυώνυμο $m_i(x)$ διαιρεί το πολυώνυμο $x^{q^s-1}-1$ (γιατί;), έχουμε ότι $k \leq q^s-1$. Αυτό δεν είναι αρκετό για να μπορεί να ορισθεί ένας BCH κώδικας. Αναγκαστικά θα πρέπει να ισχύει $k \leq n-1 \leq q^s-2$.

[1] Στην πράξη οι πλέον ενδιαφέρουσες περιπτώσεις είναι όταν ο n είναι διαιρέτης του q^s-1. Για τον λόγο αυτόν πολλοί συγγραφείς θέτουν αυτή την υπόθεση στον ορισμό.

Θα δούμε στα επόμενα ικανές συνθήκες (ως προς τα n, δ, και b) ώστε πράγματι να μπορεί να ορισθεί ένας BCH κώδικας. (Πρόταση 5.1.7).

2. Στην πράξη ο μη αρνητικός ακέραιος b δεν χρειάζεται να υπερβαίνει τον q^s-1 (γιατί;). Όπως επίσης δεν είναι ανάγκη να υποτεθεί μη αρνητικός (γιατί;).

3. Όπως έχουμε επισημάνει πολλοί θέτουν τον περιορισμό, από την αρχή, ο n να διαιρεί τον q^s-1. Άλλοι δεν απαιτούν το στοιχείο α να είναι πρωταρχικό στοιχείο του σώματος $\mathbb{K}$, αλλά να είναι ένα στοιχείο τάξης n. Στην περίπτωση αυτή έπεται ότι, αφ' ενός μεν ο n διαιρεί τον q^s-1, αφ' ετέρου δε ότι ο κώδικας είναι κυκλικός (γιατί;). Οι περιπτώσεις αυτές αποτελούν τις πλέον ενδιαφέρουσες και στα επόμενα θα επισημαίνεται αυτό.

4. Από τον τρόπο ορισμού ενός BCH κώδικα $\mathcal{BCH}(n,\,\delta,\,\alpha,\,b)$ ο κώδικας αυτός εξαρτάται (και) από την επιλογή του πρωταρχικού στοιχείου α. Επομένως γεννάται το ερώτημα, αν επιλέξουμε ένα άλλο πρωταρχικό στοιχείο β, τί σχέση έχουν οι δύο κώδικες:

$$\mathcal{BCH}(n,\,\delta,\,\alpha,\,b) \quad \text{και} \quad \mathcal{BCH}(n,\,\delta,\,\beta,\,b);$$

(βλέπε την άσκηση 2 στο τέλος της παραγράφου).

Στην ειδική περίπτωση όπου $b=1$ ο κώδικας:

$$\mathcal{BCH}(n,\,\delta,\,\alpha,\,1) = \mathcal{BCH}(n,\,\delta,\,\alpha)$$

ονομάζεται *υπό την στενή έννοια* BCH κώδικας.

Στην ειδική περίπτωση όπου $q^s = n+1$, ο κώδικας $\mathcal{BCH}(q^s-1,\,\delta,\,\alpha,\,b)$ ονομάζεται *πρωταρχικός* BCH κώδικας.

Στην πλέον δε ειδική περίπτωση, όπου $s=1$, δηλαδή $n=q-1$ ο κώδικας $\mathcal{BCH}(q-1,\,\delta,\,\alpha,\,b)$ ονομάζεται κώδικας **Reed-Solomon**.

Οι ειδικές αυτές περιπτώσεις παρουσιάζουν μεγαλύτερο πρακτικό ενδιαφέρον και είχαν μελετηθεί πριν από την γενική περίπτωση των BCH κωδίκων.

Στην περίπτωση ενός πρωταρχικού BCH κώδικα ($n=q^s-1$) το πρωταρχικό στοιχείο α του σώματος $\mathbb{K}$ είναι μια n-οστη πρωταρχική ρίζα της μονάδας

και ο αντίστοιχος (πρωταρχικός) BCH κώδικας είναι κυκλικός (βλέπε και την τελευταία από τις προηγούμενες παρατηρήσεις).

Θεώρημα 5.1.3. *Σε έναν BCH κώδικα $\mathcal{BCH}(n,\, \delta,\, \alpha,\, b)$ με γεννήτορα πολυώνυμο $\gamma(x)$ για την ελάχιστη απόστασή του, έστω d, ισχύει $deg(\gamma(x)) + 1 \geq d \geq \delta$.*

Απόδειξη. Θεωρούμε τον $\delta - 1 \times n$ πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & \alpha^b & (\alpha^b)^2 & \cdots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \cdots & (\alpha^{b+1})^{n-1} \\ 1 & \alpha^{b+2} & (\alpha^{b+2})^2 & \cdots & (\alpha^{b+2})^{n-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & \cdots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix}.$$

Παρατηρούμε ότι κάθε $\delta - 1 \times \delta - 1$ υποπίνακας του πίνακα H είναι ο ανάστροφος πίνακας ενός πίνακα Vandermonde, άρα αντιστρέψιμος. Επομένως κάθε $\delta - 1$ το πλήθος στήλες του πίνακα H είναι γραμμικά ανεξάρτητες, ενώ κάθε δ το πλήθος στήλες είναι γραμμικά εξαρτημένες. Υποθέτουμε ότι υπάρχει ένα στοιχείο $\mathbf{c} = c_0\, c_1\, c_2 \cdots c_{n-1}$ του κώδικα με βάρος w μικρότερο από δ. Από τον τρόπο ορισμού του κώδικα $\mathcal{BCH}(n,\, \delta,\, \alpha,\, b)$ έχουμε ότι το στοιχείο $\mathbf{c} = c_0\, c_1 \cdots c_{n-1}$ ανήκει στον κώδικα αν και μόνο αν $(c_0,\, c_1,\, \ldots,\, c_{n-1}) \cdot \mathrm{H}^t = \mathbf{0}$. Από την σχέση αυτή βλέπουμε ότι οι w το πλήθος στήλες του πίνακα H που αντιστοιχούν στα μη μηδενικά στοιχεία της (κωδικο)λέξης $\mathbf{c}$ είναι γραμμικά εξαρτημένες, άτοπο. Άρα $d \geq \delta$.

Διαφορετικά θα μπορούσαμε να επιχειρηματολογίσουμε ως εξής: Αν $\mathbf{c}$ ήταν μια (κωδικο)λέξη με βάρος ίσο με την ελάχιστη απόσταση d του κώδικα, τότε πάλι από την σχέση $\mathbf{c}\mathrm{H}^t = \mathbf{0}$, έχουμε ότι d το πλήθος στήλες του πίνακα που αντιστοιχούν στα μη μηδενικά στοιχεία της $\mathbf{c}$ είναι γραμμικά εξαρτημένες, δηλαδή $\delta \leq d$.

Ο κώδικας $\mathcal{BCH}(n,\, \delta,\, \alpha,\, b)$ είναι πολυωνυμικός με γεννήτορα πολυώνυμο το $\gamma(x)$. Από την Παρατήρηση 3.1.5 έχουμε ότι η διάσταση του κώδικα είναι ίση με $n - deg(\gamma(x))$. Γνωρίζουμε όμως ότι $d \leq n - (n - deg(\gamma(x))) + 1 = deg(\gamma(x)) + 1$ (φράγμα του Singleton για γραμμικούς κώδικες Πρόταση 2.1.13).

ό.έ.δ.

Παρατηρήσεις 5.1.4. 1. Η σχέση $d \geq \delta$ δικαιολογεί την ονομασία *προσχεδιασμένη απόσταση*. Στα επόμενα θα δούμε περιπτώσεις, όπου έχουμε ισότητα και περιπτώσεις όπου έχουμε γνήσια ανισότητα.

2. Η απόδειξη του προηγουμένου θεωρήματος είναι στην πραγματικότητα η απόδειξη της Πρότασης 2.2.25.

   Εκεί είχαμε έναν πίνακα ελέγχου ισοτιμίας του κώδικα. Εδώ ο πίνακας H **δεν** είναι πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{BCH}(n, \delta, \alpha, b)$. Περισσότερα επ' αυτού στα επόμενα.

3. Υπάρχουν περιπτώσεις όπου $d = deg(\gamma(x)) + 1$. Δηλαδή υπάρχουν BCH κώδικες, οι οποίοι είναι μέγιστης απόστασης.

Στο προηγούμενο θεώρημα, για να δείξουμε ότι η ελάχιστη απόσταση του κώδικα φράσσεται (από κάτω) από την προσχεδιασμένη τιμή δ, κρίσιμο σημείο ήταν η ύπαρξη πινάκων Vandermonde. Αυτό οφείλεται στο ότι οι ρίζες του γεννήτορα πολυωνύμου είναι τα στοιχεία $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$, τα οποία είναι δυνάμεις του ίδιου στοιχείου α με εκθέτες διαδοχικούς ακεραίους.

Επομένως θα μπορούσαμε να γενικεύσουμε σε τυχαίους κυκλικούς κώδικες.

Πρόταση 5.1.5. ***(Το φράγμα BCH)*** *Έστω ω μια πρωταρχική n-οστή ρίζα της μονάδας επί του πεπερασμένου σώματος $\mathbb{F}$ και $\mathcal{C}$ ένας κυκλικός κώδικας μήκους n με γεννήτορα πολυώνυμο $g(x) \in \mathbb{F}[x]$. Υποθέτουμε ότι μεταξύ των ριζών του $g(x)$ είναι και τα $\delta - 1$ το πλήθος στοιχεία $\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$, όπου $b \geq 0$. Τότε η ελάχιστη απόσταση του κώδικα $\mathcal{C}$ είναι τουλάχιστον ίση με δ.*

Απόδειξη. Η απόδειξη είναι ακριβώς η ίδια με το πρώτο μέρος της απόδειξης του προηγουμένου θεωρήματος. ό.έ.δ.

Παραδείγματα 5.1.6. 1. Θα κατασκευάσουμε έναν δυαδικό υπό την στενή έννοια BCH κώδικα ($b = 1$) μήκους $n = 7$ και προσχεδιασμένης απόστασης $\delta = 3$.

Σύμφωνα με τον ορισμό 5.1.1 θα πρέπει να κατασκευάσουμε μια επέκταση $\mathbb{K}$ του σώματος $\mathbb{Z}_2$ βαθμού $s = 3$ (καθότι πρέπει να ισχύει $2^3 \geq 7 + 1 = 8$). Δηλαδή θα έχουμε έναν πρωταρχικό κώδικα.

Το πολυώνυμο $x^3 + x + 1 \in \mathbb{Z}_2[x]$ είναι ανάγωγο επί του $\mathbb{Z}_2$, οπότε έχουμε το σώμα $\mathbb{K} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$, το οποίο είναι μια επέκταση του $\mathbb{Z}_2$ βαθμού 3. Το στοιχείο $\alpha = x + \langle x^3 + x + 1\rangle$ είναι πρωταρχικό στοιχείο του σώματος $\mathbb{K}$ (γιατί;) με ελάχιστο πολυώνυμο (επί του $\mathbb{Z}_2$) το $m_1(x) = x^3 + x + 1$, αλλά και το στοιχείο α^2 έχει το ίδιο ελάχιστο πολυώνυμο (γιατί;). Συνεπώς το πολυώνυμο γεννήτορας του BCH κώδικα που αναζητούμε είναι το πολυώνυμο $\gamma(x) = x^3 + x + 1$.

Οπότε η διάσταση του κώδικα είναι ίση με $n - deg(\gamma(x)) = 7 - 3 = 4$ και σύμφωνα με το προηγούμενο θεώρημα έχουμε ότι η ελάχιστη απόσταση ικανοποιεί την σχέση $4 \geq d \geq 3$. Επειδή το πολυώνυμο γεννήτορας έχει τρεις μη μηδενικούς όρους, η ελάχιστη απόσταση του κώδικα ισούται με τρία.

Αν θελήσουμε να περιγράψουμε τα στοιχεία του κώδικα, έχουμε:

$$\begin{aligned}\mathcal{BCH} &= \{\, f(x) \cdot x^3 + x + 1 \mid f(x) = a_3x^3 + a_2x^2 + a_1x + a_0, \quad a_i \in \mathbb{Z}_2 \,\} \\ &= \{\, (a_0, a_1 + a_0, a_2 + a_1, a_3 + a_2 + a_0, a_3 + a_1, a_2, a_3) \mid a_i \in \mathbb{Z}_2 \,\}.\end{aligned}$$

2. Θα κατασκευάσουμε έναν δυαδικό υπό την στενή έννοια BCH κώδικα ($b = 1$) μήκους $n = 15$, ο οποίος θα διορθώνει (τουλάχιστον) 2 λάθη.

   Θα πρέπει να κατασκευάσουμε μια επέκταση $\mathbb{K}$ του σώματος $\mathbb{Z}_2$ βαθμού $s = 4$ (καθότι πρέπει να ισχύει $2^4 \geq 15 + 1 = 16$). Δηλαδή θα έχουμε έναν πρωταρχικό κώδικα. Επίσης, επειδή θέλουμε να διορθώνει (τουλάχιστον) 2 λάθη, η προσχεδιασμένη απόσταση θα είναι ίση $\delta = 5$.

   Όπως στο προηγούμενο παράδειγμα το πολυώνυμο $x^4 + x + 1 \in \mathbb{Z}_2[x]$ είναι ανάγωγο επί του $\mathbb{Z}_2$, οπότε έχουμε το σώμα $\mathbb{K} = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$, το οποίο είναι μια επέκταση του $\mathbb{Z}_2$ βαθμού 4. Το στοιχείο $\alpha = x + \langle x^4 + x + 1\rangle$ είναι πρωταρχικό στοιχείο του σώματος $\mathbb{K}$ (γιατί;) με ελάχιστο πολυώνυμο (επί του $\mathbb{Z}_2$) το $m_1(x) = x^4 + x + 1$.

Το πολυώνυμο γεννήτορας του BCH κώδικα που αναζητούμε, το πολυώνυμο $\gamma(x)$, είναι το μικροτέρου βαθμού μονικό πολυώνυμο επί του $\mathbb{Z}_2$, το οποίο έχει ως ρίζες τα στοιχεία $\alpha, \alpha^2, \alpha^3, \alpha^4$. Αλλά τα στοιχεία α^2, α^4 έχουν το ίδιο ελάχιστο πολυώνυμο με το στοιχείο α (γιατί;). Συνεπώς $\gamma(x) = m_1(x)m_3(x)$. Επομένως πρέπει να υπολογίσουμε το $m_3(x)$, το ελάχιστο πολυώνυμο του α^3. Έχουμε $m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})$. Το στοιχείο α ικανοποιεί τις σχέσεις $\alpha^{15} = 1$ και $\alpha^4 + \alpha + 1 = 0$. Οπότε κάνοντας τις πράξεις στο δεξιό μέρος της σχέσης $m_3(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^9)(x-\alpha^{12})$ καταλήγουμε ότι $m_3(x) = x^4 + x^3 + x^2 + x + 1$ (να κάνετε τις πράξεις και να επιβεβαιώσετε το αποτέλεσμα). Άρα $\gamma(x) = m_1(x)m_3(x) = (x^4+x+1)(x^4+x^3+x^2+x+1) = x^8 + x^7 + x^6 + x^4 + 1$.

Οπότε η διάσταση του κώδικα είναι ίση με $n-deg(\gamma(x)) = 15-8 = 7$ και σύμφωνα με το προηγούμενο θεώρημα έχουμε ότι η ελάχιστη απόσταση ικανοποιεί την σχέση $9 \geq d \geq 5$. Επειδή το πολυώνυμο γεννήτορας έχει πέντε μη μηδενικούς όρους, η ελάχιστη απόσταση του κώδικα ισούται με πέντε.

Άρα ο κώδικας που κατασκευάσαμε μπορεί να περιγρφεί ως εξής:

$$\begin{aligned}\mathcal{BCH}(15,\,5,\,\alpha) = \{\, f(x) \in (\mathbb{Z}_2)_{14}[x] \mid \\ \alpha^{1+i} \text{ είναι ρίζα του } f(x) \text{ για όλα τα } 0 \leq i \leq 3\,\} \\ = \{\, (a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6) \\ (x^8 + x^7 + x^6 + x^4 + 1) \mid a_0, a_1, a_2, a_3, a_4, a_5, a_6 \in \mathbb{Z}_2\} \\ = \{\, \mathbf{r} = r_0\, r_1 \cdots r_{14} \mid \text{το πολυώνυμο} \\ r_0 + r_1x + \cdots + r_{14}x^{14} \in (\mathbb{Z}_2)_{14}[x] \text{ έχει ως ρίζες τα} \\ \alpha^{1+i} \text{ για όλα τα } 0 \leq i \leq 3\,\}.\end{aligned}$$

3. Θα κατασκευάσουμε έναν τριαδικό υπό την στενή έννοια BCH κώδικα ($b = 1$) μήκους $n = 8$, ο οποίος θα διορθώνει (τουλάχιστον) 2 λάθη.

   Θα πρέπει να κατασκευάσουμε μια επέκταση $\mathbb{K}$ του σώματος $\mathbb{Z}_3$ βαθμού $s = 2$ (καθότι πρέπει να ισχύει $3^2 \geq 8+1 = 9$). Δηλαδή θα έχουμε

έναν πρωταρχικό κώδικα. Επίσης, επειδή θέλουμε να διορθώνει (τουλάχιστον) 2 λάθη, η προσχεδιασμένη απόσταση θα είναι ίση $\delta = 5$.

Όπως στα προηγούμενα παραδείγματα επιλέγουμε το πολυώνυμο $x^2 + x + 2 \in \mathbb{Z}_3[x]$, το οποίο είναι ανάγωγο επί του $\mathbb{Z}_3$, οπότε έχουμε το σώμα $\mathbb{K} = \mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$, το οποίο είναι μια επέκταση του $\mathbb{Z}_3$ βαθμού 2. Το στοιχείο $\alpha = x + \langle x^2 + x + 2\rangle$ είναι πρωταρχικό στοιχείο του σώματος $\mathbb{K}$ (γιατί;) με ελάχιστο πολυώνυμο (επί του $\mathbb{Z}_3$) το $m_1(x) = x^2 + x + 2$.

Το πολυώνυμο γεννήτορας του BCH κώδικα που αναζητούμε, το πολυώνυμο $\gamma(x)$, είναι το μικροτέρου βαθμού μονικό πολυώνυμο επί του $\mathbb{Z}_3$, το οποίο έχει ως ρίζες τα στοιχεία α, α^2, α^3, α^4. Αλλά το στοιχείο α^3 έχει το ίδιο ελάχιστο πολυώνυμο με το στοιχείο α (γιατί;), όπως επίσης τα στοιχεία α^2 και α^6. Συνεπώς $\gamma(x) = m_1(x)m_2(x)m_4(x)$. Επομένως πρέπει να υπολογίσουμε τα $m_2(x)$ και $m_4(x)$.

Το στοιχείο α ικανοποιεί τη σχέση $\alpha^8 = 1$. Επομένως εύκολα βλέπουμε ότι $\alpha^4 = 2$. Συνεπώς:

$$\begin{aligned} m_2(x) &= (x - \alpha^2)(x - \alpha^6) \\ &= (x - \alpha^2)(x - 2\alpha^2) \\ &= x^2 + 2\alpha^4 = x^2 + 1. \end{aligned}$$

Επίσης $m_4(x) = x - \alpha^4 = x - 2 = x + 1$. Άρα:

$$\begin{aligned} \gamma(x) &= m_1(x)m_2(x)m_4(x) \\ &= (x^2 + x + 2)(x^2 + 1)(x + 1) \\ &\vdots \\ &= x^5 + 2x^4 + x^3 + x^2 + 2. \end{aligned}$$

Οπότε η διάσταση του κώδικα είναι ίση με $n - deg(\gamma(x)) = 8 - 5 = 3$ και σύμφωνα με το προηγούμενο θεώρημα έχουμε ότι η ελάχιστη απόσταση ικανοποιεί την σχέση $5 + 1 \geq d \geq 5$. Επειδή το πολυώνυμο γεννήτορας έχει πέντε μη μηδενικούς όρους, η ελάχιστη απόσταση του κώδικα ισούται με πέντε.

Άρα ο κώδικας που κατασκευάσαμε μπορεί να περιγραφεί ως εξής:

$$\begin{aligned}\mathcal{BCH}(8,\,5,\,\alpha) &= \{\, f(x) \in (\mathbb{Z}_3)_7[x] \mid \alpha^{1+i} \text{ είναι ρίζα του } f(x) \\ &\qquad\qquad \text{για όλα τα } 0 \le i \le 3 \,\} \\ &= \{\, (a_0 + a_1 x + a_2 x^2)(x^5 + 2x^4 + x^3 + x^2 + 2) \mid \\ &\qquad\qquad a_0,\, a_1,\, a_2 \in \mathbb{Z}_2 \,\} \\ &= \{\, \mathbf{r} = r_0\, r_1 \cdots r_7 \mid \text{το πολυώνυμο} \\ &\qquad\qquad r_0 + r_1 x + \cdots + r_7 x^7 \in (\mathbb{Z}_2)_7[x] \text{ έχει ως ρίζες τα} \\ &\qquad\qquad \alpha^{1+i} \text{ για όλα τα } 0 \le i \le 3 \,\}.\end{aligned}$$

4. Έστω $r \ge 2$ ένας ακέραιος. Θα κατασκευάσουμε έναν πρωταρχικό, υπό την στενή έννοια, δυαδικό BCH κώδικα προσχεδιασμένης απόστασης $\delta = 3$. Έστω $n = 2^r - 1$ και $\mathbb{K}$ μια επέκταση του $\mathbb{Z}_2$ βαθμού r, επιλέγουμε ένα πρωταρχικό στοιχείο α του σώματος $\mathbb{K}$ (δηλαδή μια πρωταρχική n-οστή ρίζα της μονάδος). Σύμφωνα με τον Ορισμό 5.1.1 ο πρωταρχικός ($n = 2^r - 1$), υπό την στενή έννοια ($b = 1$) BCH κώδικας έχει γεννήτορα πολυώνυμο το $\gamma(x) = \varepsilon\kappa\pi(\, m_{i+1}(x),\ 0 \le i \le \delta - 2\,)$, όπου, για κάθε $0 \le i \le \delta - 2$, το $m_{i+1}(x)$ είναι το ελάχιστο πολυώνυμο του α^{b+i} επί του $\mathbb{Z}_2$. Αλλά $b = 1$ και $\delta = 3$, οπότε $\gamma(x) = \varepsilon\kappa\pi(\, m_1(x), m_2(x)\,)$. Τα στοιχεία όμως α και α^2 έχουν το ίδιο ελάχιστο πολυώνυμο. Συνεπώς έχουμε κατασκευάσει τον κώδικα $\mathcal{BCH}(n = 2^r - 1, \delta = 3, \alpha)$ με γεννήτορα πολυώνυμο $\gamma(x) = m_1(x) = m_\alpha(x)$.

Θα δούμε την σχέση αυτού του κώδικα με τους δυαδικούς Hamming κώδικες.

Έστω $\mathcal{H}(r,\,2)$ ο δυαδικός Hamming κώδικας με παραμέτρους:

$$[n = 2^r - 1,\, k = 2^r - 1 - r,\, d = 3].$$

Στο Θεώρημα 4.1.9 είχαμε δεί ότι ο κώδικας $\mathcal{H}(r,\,2)$ είναι ισοδύναμος με τον κυκλικό κώδικα που έχει γεννήτορα πολυώνυμο το ελάχιστο πολυώνυμο $m_\omega(x)$, όπου ω είναι μια πρωταρχική n-οστη ρίζα της μονάδος επί του $\mathbb{Z}_2$.

Άρα αποδείξαμε ότι οι δυαδικοί Hamming κώδικες αποτελούν μια ειδική περίπτωση των δυαδικών BCH κωδίκων.

Πρόταση 5.1.7. *Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία. Έστω $n = q^s - 1$, $\delta = qt + 1$ θετικοί ακέραιοι με $2 \leq \delta \leq n$. Πάντα μπορούμε να κατασκευάσουμε επί του $\mathbb{F}$ έναν BCH (υπό την στενή έννοια) κώδικα μήκους n και προσχεδιασμένης απόστασης δ με γεννήτορα πολυώνυμο $\gamma(x)$ βαθμού το πολύ $(q-1)ts$.*

Απόδειξη. Έστω $\mathbb{K}$ μια επέκταση του $\mathbb{F}$ βαθμού s και α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Για κάθε $1 \leq i \leq \delta - 1 = qt$ έστω $m_i(x)$ το ελάχιστο πολυώνυμο του α^i επί του $\mathbb{F}$ και $\gamma(x) = \varepsilon\kappa\pi(\, m_i(x),\ 1 \leq i \leq \delta - 1 = qt\,)$. Όπως στον ορισμό, κατασκευάζουμε τον BCH κώδικα $\mathcal{BCH}(n,\, \delta,\, \alpha)$.

Κάθε πολυώνυμο $m_i(x)$ έχει βαθμό s, άρα το πολυώνυμο γεννήτορας $\gamma(x)$ έχει βαθμό το πολύ $(qt)s$. Γνωρίζουμε ότι οι ρίζες α και α^q έχουν το ίδιο ελάχιστο πολυώνυμο και γενικά οι ρίζες α^i και $(\alpha^i)^q$ έχουν το ίδιο ελάχιστο πολυώνυμο. Επομένως τα t το πλήθος πολυώνυμα $m_q(x), m_{2q}(x), \ldots, m_{tq}(x)$ δεν χρειάζεται να συμπεριληφθούν στον υπολογισμό του ε.κ.π. των $m_i(x)$, $1 \leq i \leq \delta - 1 = qt$. Συνεπώς για το $\varepsilon\kappa\pi(\, m_i(x),\ 1 \leq i \leq \delta - 1 = qt\,)$ αρκούν $qt - t$ το πλήθος πολυώνυμα, δηλαδή το πολυώνυμο γεννήτορας $\gamma(x)$ έχει βαθμό το πολύ $(q-1)ts$. ό.έ.δ.

Παρατήρηση 5.1.8. Στην ειδική περίπτωση των δυαδικών κωδίκων, αν υποθέσουμε ότι έχουμε περιττή προσχεδιασμένη απόσταση, $\delta = 2t+1$, όπως στην προηγούμενη πρόταση, έχουμε ότι $m_1(x) = m_{\delta-1}(x)$, καθότι οι ρίζες α και α^{2t} έχουν το ίδιο ελάχιστο πολυώνυμο. Επομένως $\gamma(x) = \varepsilon\kappa\pi(\, m_i(x),\ 1 \leq i \leq \delta - 1 = 2t\,) = \varepsilon\kappa\pi(\, m_i(x),\ 1 \leq i \leq \delta - 2 = 2t - 1\,)$. Συνεπώς οι κώδικες $\mathcal{C}(n,\, \delta,\, \alpha)$ και $\mathcal{C}(n,\, \delta - 1,\, \alpha)$ συμπίπτουν.

Η παρατήρηση αυτή μας επιτρέπει (άνευ βλάβης) να υποθέτουμε πάντα ότι οι, υπό την στενή έννοια, δυαδικοί BCH κώδικες έχουν περιττή προσχεδιασμένη απόσταση.

Έστω $\mathcal{BCH}(n,\, \delta,\, \alpha,\, b)$ ένας BCH κώδικας επί ενός σώματος $\mathbb{F}$.

Στο Θεώρημα 5.1.3 για να αποδείξουμε ότι ο αριθμός δ αποτελεί ένα κάτω φράγμα για την ελάχιστη απόσταση του κώδικα είχαμε χρησιμοποιήσει

τον $(\delta-1)\times n$ πίνακα:

$$\mathrm{H}=\begin{pmatrix} 1 & \alpha^{b} & (\alpha^{b})^{2} & \cdots & (\alpha^{b})^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^{2} & \cdots & (\alpha^{b+1})^{n-1} \\ 1 & \alpha^{b+2} & (\alpha^{b+2})^{2} & \cdots & (\alpha^{b+2})^{n-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^{2} & \cdots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix}.$$

Αν και ο πίνακας H δεν είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{BCH}$ (Παρατήρηση 5.1.4), στην απόδειξη επικαλεσθήκαμε επιχειρήματα που σχετίζονται με ιδιότητες ενός πίνακα ελέγχου ισοτιμίας του κώδικα.

Θα κατασκευάσουμε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{BCH}$ με την βοήθεια του πίνακα H.

Στην θέση $(i,\,j)$ αντιστοιχεί το στοιχείο $h_{ij}=(\alpha^{b+i-1})^{j-1}$. Το στοιχείο αυτό ανήκει στο σώμα $\mathbb{K}$, το οποίο είναι μια επέκταση του σώματος $\mathbb{F}$ βαθμού s. Θεωρούμε το σώμα $\mathbb{K}$ ως διανυσματικό χώρο επί του $\mathbb{F}$, επιλέγουμε και σταθεροποιούμε μια διατεταγμένη βάση του $\mathbf{B}=\{e_1,\,e_2,\,\ldots,\,e_s\}$. Κάθε h_{ij} το εκφράζουμε ως γραμμικό συνδυασμό των διανυσμάτων της βάσης που επιλέξαμε και με $[r_i^j]$ συμβολίζουμε το διάνυσμα στήλη των συντελεστών στην έκφραση αυτή. Δηλαδή $h_{ij}=[r_i^j]^t\cdot(e_1,\,e_2,\,\ldots,\,e_s)^t$.

Από τον τρόπο ορισμού του κώδικα $\mathcal{BCH}(n,\,\delta,\,\alpha,\,b)$ έχουμε ότι το στοιχείο $\mathbf{c}=c_1\,c_2\cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1,\,c_2,\,\ldots,\,c_n)\cdot\mathrm{H}^t=\mathbf{0}$.

Οπότε, σε συνδυασμό με την προηγούμενη σχέση έχουμε ότι το $\mathbf{c}=c_1\,c_2\cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $c_1[r_i^1]+c_2[r_i^2]+\cdot c_n[r_i^n]=\mathbf{0}$ για κάθε $i=1,\,2,\,\ldots,\,\delta-1$.

Κατασκευάζουμε τον πίνακα:

$$\mathrm{P}=\begin{pmatrix} [r_1^1] & [r_1^2] & [r_1^3] & \cdots & [r_1^n] \\ [r_2^1] & [r_2^2] & [r_2^3] & \cdots & [r_2^n] \\ [r_3^1] & [r_3^2] & [r_3^3] & \cdots & [r_3^n] \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ [r_{\delta-1}^1] & [r_{\delta-1}^2] & [r_{\delta-1}^3] & \cdots & [r_{\delta-1}^n] \end{pmatrix},$$

ο οποίος προκύπτει από τον πίνακα H με την αντικατάσταση κάθε h_{ij} με το διάνυσμα στήλη $[r_i^j]$ των συντελεστών του στην έκφρασή του ως γραμμικό

συνδυασμό των διανυσμάτων της βάσης **B**. Προφανώς από τα προηγούμενα έπεται ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1, c_2, \ldots, c_n) \cdot \mathrm{P}^t = \mathbf{0}$.

Στον πίνακα P, αν αναπτύξουμε κάθε στήλη $[r_i^j]$, η οποία περιλαμβάνει s το πλήθος στοιχεία, τότε προκύπτει ένας $(\delta - 1)s \times n$ πίνακας $\overline{\mathrm{H}}$, του οποίου τα στοιχεία είναι από το σώμα $\mathbb{F}$ και για τον οποίο ισχύει ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1, c_2, \ldots, c_n) \cdot \overline{\mathrm{H}}^t = \mathbf{0}$.

Συνεπώς με την διαδικασία αυτή κατασκευάσαμε έναν πίνακα ελέγχου ισοτιμίας για τον BCH κώδικα $\mathcal{BCH}(n, \delta, \alpha, b)$ επί του σώματος $\mathbb{F}$.

Παρατήρηση 5.1.9. Η διαδικασία, που περιγράψαμε για την κατασκευή ενός πίνακα ελέγχου ισοτιμίας για τον BCH κώδικα $\mathcal{BCH}(n, \delta, \alpha, b)$, είναι η ίδια που παρουσιάσαμε στην σελίδα 191 για την κατασκευή ενός πίνακα ελέγχου ισοτιμίας σε έναν κυκλικό κώδικα.

Παράδειγμα 5.1.10. Στο Παράδειγμα $5.1.6_1$ είχαμε κατασκευάσει έναν, υπό την στενή έννοια ($b = 1$), δυαδικό BCH κώδικα $\mathcal{BCH}$ μήκους $n = 7$ και προσχεδιασμένης απόστασης $\delta = 3$, του οποίου το πολυώνυμο γεννήτορας ήταν το $\gamma(x) = x^3 + x + 1$. Λαμβάνοντας το στοιχείο $\alpha = x + \langle x^3 + x + 1 \rangle$ στην επέκταση $\mathbb{K} = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ κατασκευάζουμε τον 2×7 πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & (\alpha^2)^4 & (\alpha^2)^5 & (\alpha^2)^6 \end{pmatrix},$$

ο οποίος δεν είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{BCH}$. Θα κατασκευάσουμε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα με την βοήθεια του πίνακα H.

Η επέκταση $\mathbb{K}$ είναι βαθμού 3 επί του $\mathbb{Z}_2$. Επιλέγουμε και σταθεροποιούμε την διατεταγμένη βάση $\mathbf{B} = \{1, \alpha, \alpha^2\}$. Κάθε στοιχείο του πίνακα το εκφράζουμε ως γραμμικό συνδυασμό των διανυσμάτων της βάσης που επιλέξαμε και με $[r_i^j]$ συμβολίζουμε το διάνυσμα στήλη των συντελεστών του στοιχείου στη θέση (i, j) στην έκφραση αυτή. Για παράδειγμα:

$$1 = [r_1^1]^t \cdot (1, \alpha, \alpha^2)^t = (1, 0, 0) \cdot (1, \alpha, \alpha^2)^t,$$
$$\alpha^6 = [r_2^4]^t \cdot (1, \alpha, \alpha^2)^t = (1, 0, 1) \cdot (1, \alpha, \alpha^2)^t.$$

Τελικά ο $(2 \cdot 3) \times 7$ πίνακας:

$$\overline{\mathrm{H}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ - & - & - & - & - & - & \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

ο οποίος κατασκευάστηκε με την διαδικασία που περιγράψαμε (να κάνετε τον έλεγχο των πράξεων), είναι ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{C}$, καθότι τα στοιχεία είναι από το σώμα $\mathbb{Z}_2$ και ισχύει ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1, c_2, \ldots, c_n) \cdot \overline{\mathrm{H}}^t = \mathbf{0}$.

5.1.1 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;* αυτής της παραγράφου.

2. Έστω ένας $\mathcal{BCH}$ κώδικας. Κατά πόσον η δομή του κώδικα αυτού εξαρτάται από την επιλογή του πρωταρχικού στοιχείου α; Δηλαδή, αν επιλέξουμε ένα άλλο πρωταρχικό στοιχείο β, τί σχέση έχουν οι δύο κώδικες $\mathcal{BCH}(n, \delta, \alpha, b)$ και $\mathcal{BCH}(n, \delta, \beta, b)$;

   (Εξετάστε πρώτα την περίπτωση, όπου οι κώδικες είναι υπό την στενή έννοια πρωταρχικοί κώδικες).

3. Να προσδιορίσετε όλους τους δυαδικούς BCH κώδικες μήκους 15.

4. Να κατασκευάσετε έναν υπό την στενή έννοια τριαδικό BCH κώδικα $\mathcal{BCH}(26, 5, \alpha)$.

5. Ως γνωστόν ένας κώδικας $\mathcal{C}$ ονομάζεται αυτο-ορθογώνιος αν ισχύει $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. Να βρεθεί ένας αυτο-ορθογώνιος δυαδικός BCH κώδικας μήκους $n = 7$.

   (βλέπε Ασκήσεις 3.2.5$_{14,\,15,\,16}$).

6. Ποίος είναι ο λόγος πληροφορίας ενός υπό την στενή έννοια BCH κώδικα μήκους 31, ο οποίος διορθώνει δύο λάθη;

   (α) Επί του σώματος $\mathbb{Z}_2$.

   (β) Επί του σώματος $\mathbb{Z}_3$.

7. Να υπολογίσετε το πολυώνυμο γεννήτορα και το πολυώνυμο ελέγχου ισοτιμίας για έναν δυαδικό BCH κώδικα, ο οποίος διορθώνει τρία λάθη.

   (α) Μήκους 15.

   (β) Μήκους 31.

   (γ) Με τον κώδικα αυτό κωδικοποιήστε την πληροφορία, της οποίας όλοι οι χαρακτήρες είναι ίσοι με το 1.

5.2 Συμβατικοί Κώδικες Reed-Solomon

Στην προηγουμένη παράγραφο αναφερθήκαμε στην κατασκευή των BCH κωδίκων επί ενός σώματος $\mathbb{F}$ χρησιμοποιώντας μια επέκταση $\mathbb{K}$ του $\mathbb{F}$. Εδώ θα γενικεύσουμε την προηγουμένη κατασκευή και θα λάβουμε τους BCH κώδικες ως υποκώδικες άλλων κωδίκων.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Έστω n, δ θετικοί ακέραιοι με $2 \leq \delta \leq n$ και b ένας μη αρνητικός ακέραιος. Έστω $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ βαθμού s με την ιδιότητα $\mid \mathbb{K} \mid = q^s \geq n+1$ και α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Ορίζουμε το πολυώνυμο:

$$\hat{\gamma}(x) = (x-\alpha^b)(x-\alpha^{b+1})(x-\alpha^{b+2}) \cdots (x-\alpha^{b+\delta-2}) \in \mathbb{K}[x].$$

Ορισμός 5.2.1. *Ο πολυωνυμικός κώδικας $CRS = CRS(n, \delta, \alpha, b)$[2] μήκους n με πολυώνυμο γεννήτορα το πολυώνυμο $\hat{\gamma}(x) \in \mathbb{K}[x]$ ονομάζεται* ***Συμβατικός κώδικας Reed-Solomon*** *προσχεδιασμένης απόστασης δ (με σώμα βάσης το $\mathbb{F}$).*

[2] Ο συμβολισμός CRS προέρχεται από την διεθνή ονομασία Convensional Reed-Solomon code.

Διαφορετικά θα μπορούσαμε να ορίσουμε έναν συμβατικό κώδικα Reed-Solomon ως εξής:

$$\begin{aligned} \mathcal{CRS}(n,\,\delta,\,\alpha,\,b) &= \{\, f(x) \in \mathbb{K}_{n-1}[x] \mid \alpha^{b+i} \text{ είναι ρίζα του } f(x) \\ &\qquad\qquad \text{για όλα τα } 0 \le i \le \delta - 2 \,\} \\ &= \{\mathbf{r} = r_0\, r_1 \cdots r_{n-1} \mid \text{το πολυώνυμο} \\ &\qquad r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} \in \mathbb{K}_{n-1}[x] \text{ έχει ως ρίζες τα} \\ &\qquad\qquad \alpha^{b+i} \text{ για όλα τα } 0 \le i \le \delta - 2 \,\}. \end{aligned}$$

Παρατηρήσεις 5.2.2. 1. Αν και ξεκινήσαμε με αφετηρία το σώμα $\mathbb{F}$, ο κώδικας $\mathcal{CRS}$ που κατασκευάσαμε έχει ως αλφάβητο τα στοιχεία μιας επέκτασης $\mathbb{K}$ του σώματος $\mathbb{F}$.

Ο μόνος λόγος που κάνουμε αυτό είναι να επανέλθουμε στα επόμενα για να δούμε τους BCH κώδικες ως (υπο)κώδικες των συμβατικών κωδίκων Reed-Solomon.

Συνεπώς θα μπορούσαμε να ορίσουμε τους συμβατικούς κώδικες Reed-Solomon ως εξής:

Έστω $\mathbb{K}$ ένα πεπερασμένο σώμα n, δ θετικοί ακέραιοι με $2 \le \delta \le n \le |\,\mathbb{K}\,| - 1$ και b ένας μη αρνητικός ακέραιος. Έστω α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Ορίζουμε το πολυώνυμο $\hat{\gamma}(x) = (x-\alpha^b)(x-\alpha^{b+1})(x-\alpha^{b+2}) \cdots (x-\alpha^{b+\delta-2}) \in \mathbb{K}[x]$.

Ο πολυωνυμικός κώδικας $\mathcal{CRS} = \mathcal{CRS}(n,\,\delta,\,\alpha,\,b)$ μήκους n με πολυώνυμο γεννήτορα το πολυώνυμο $\hat{\gamma}(x) \in \mathbb{K}[x]$ ονομάζεται **συμβατικός κώδικας Reed-Solomon** .

Η πλέον ενδιαφέρουσα κατηγορία συμβατικώνν κωδίκων Reed-Solomon είναι οι πρωταρχικοί συμβατικοί κώδικες Reed-Solomon (στο εξής θα αναφέρονται απλά ως κώδικες Reed-Solomon), όπου το μήκος τους n ισούται με το πλήθος των μη μηδενικών στοιχείων του σώματος $\mathbb{K}$ ($n = |\,\mathbb{K}\,| - 1$) που αποτελεί το αλφάβητο του κώδικα.

Μάλιστα δε οι κώδικες αυτοί είναι κυκλικοί, καθότι το πολυώνυμο $\hat{\gamma}(x) = (x-\alpha^b)(x-\alpha^{b+1})(x-\alpha^{b+2}) \cdots (x_\alpha^{b+\delta-2}) \in \mathbb{K}[x]$ διαιρεί το $x^n - 1$,

αφού κάθε στοιχείο c του σώματος $\mathbb{K}$ ικανοποιεί την σχέση $c^n = 1$.

2. Θεωρούμε τον $(\delta - 1) \times n$ πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & \alpha^b & (\alpha^b)^2 & \cdots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \cdots & (\alpha^{b+1})^{n-1} \\ 1 & \alpha^{b+2} & (\alpha^{b+2})^2 & \cdots & (\alpha^{b+2})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & \cdots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix}.$$

Εύκολα βλέπουμε ότι ο πίνακας H είναι ένας πίνακας ελέγχου ισοτιμίας για τον συμβατικό κώδικα Reed-Solomon καθότι, από τον τρόπο ορισμού του κώδικα $\mathcal{CRS}(n, \delta, \alpha, b)$, έχουμε ότι το στοιχείο $\mathbf{c} = c_0\, c_1 \cdots c_{n-1}$ ανήκει στον κώδικα αν και μόνο αν $(c_0, c_1, \ldots, c_{n-1}) \cdot \mathrm{H}^t = \mathbf{0}$.

Μπορούμε να αποδείξουμε ένα θεώρημα ανάλογο με το Θεώρημα 5.1.3.

Θεώρημα 5.2.3. *Ένας συμβατικός κώδικας Reed-Solomon $\mathcal{CRS}(n, \delta, \alpha, b)$ με πολυώνυμο γεννήτορα $\hat{\gamma}(x)$ είναι κώδικας μέγιστης (ελάχιστης) απόστασης (MDS κώδικας). Μάλιστα δε για την ελάχιστη απόστασή του, έστω d, ισχύει $deg(\hat{\gamma}(x)) + 1 = d = \delta$.*

Απόδειξη. Από την προηγουμένη παρατήρηση, ο πίνακας H είναι ένας πίνακας ελέγχου ισοτιμίας του οποίου η τάξη ισούται με το πλήθος γραμμών του $\delta - 1$. Επομένως, σύμφωνα με την Πρόταση 2.2.25, έχουμε ότι η ελάχιστη απόστασή του είναι ίση με $d = \delta$.

Από το δεύτερο μέρος της απόδειξης του Θεωρήματος 5.1.3 έχουμε ότι ο κώδικας είναι MDS. ό.έ.δ.

Παράδειγμα 5.2.4. Θα κατασκευάσουμε,τώρα, έναν κώδικα Reed-Solomon $\mathcal{CRS}(7, 3, \alpha)$ μήκους $n = 7$, προσχεδιασμένης απόστασης $\delta = 3$ $(b = 1)$, όπου $\alpha = x + \langle x^3 + x + 1 \rangle$ είναι ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K} = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$. Κατασκευάζουμε τον 2×6 πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & (\alpha^2)^2 & (\alpha^2)^3 & (\alpha^2)^4 & (\alpha^2)^5 \end{pmatrix}.$$

Ο κώδικας που αναζητούμε έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα H και ως γεννήτορα πολυώνυμο το πολυώνυμο $\hat{\gamma}(x) = (x-\alpha)(x-\alpha^2) \in \mathbb{K}[x]$. Δηλαδή

$$\begin{aligned}\widehat{\mathcal{C}}(7,\,3,\,\alpha) &= \{\, f(x) \in \mathbb{K}_6[x] \mid \alpha,\, \alpha^2 \text{ είναι ρίζες του } f(x) \,\} \\ &= \{\mathbf{r} = r_0\, r_1 \cdots r_6 \mid \text{το πολυώνυμο } r_0 + r_1 x + \cdots + r_6 x^6 \in \mathbb{K}_6[x] \\ &\qquad\qquad \text{έχει ως ρίζες τα } \alpha,\, \alpha^2 \,\} \\ &= \{\mathbf{r} = r_0\, r_1 \cdots r_6 \in \mathbb{K}^7 \mid \mathbf{r}\mathrm{H}^t = \mathbf{0}\}.\end{aligned}$$

5.2.1 Οι BCH κώδικες ως υποκώδικες των συμβατικών κωδίκων Reed-Solomon

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Έστω n, δ θετικοί ακέραιοι με $2 \leq \delta \leq n$ και b ένας μη αρνητικός ακέραιος. Έστω $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ βαθμού s με την ιδιότητα $q^s \geq n+1$ και α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Έστω $C\mathcal{RS} = C\mathcal{RS}(n,\, \delta,\, \alpha,\, b)$ ο συμβατικός κώδικας Reed-Solomon μήκους n με πολυώνυμο γεννήτορα το πολυώνυμο $\hat{\gamma}(x) = (x-\alpha^b)(x-\alpha^{b+1})(x-\alpha^{b+2}) \cdots (x-\alpha^{b+\delta-2}) \in \mathbb{K}[x]$.

Από τον κώδικα $C\mathcal{RS}$ επιλέγουμε μόνο τις (κωδικο)λέξεις, των οποίων τα γράμματα (οι χαρακτήρες) ανήκουν στο (αρχικό) σώμα $\mathbb{F}$. Δηλαδή παίρνουμε την τομή $\mathcal{A} = \mathbb{F}^n \cap C\mathcal{RS}$.

Το σύνολο $\mathcal{A}$ είναι ένας (υπο)κώδικας του κώδικα $C\mathcal{RS}$ και μάλιστα γραμμικός (ως τομή διανυσματικών χώρων επί του ιδίου σώματος $\mathbb{F}$). Μάλιστα δε ως υποκώδικας του $C\mathcal{RS}$ είναι *αραιώτερος*, δηλαδή η ελάχιστη απόστασή του είναι τουλάχιστον ίση με δ.

Θα περιγράψουμε τα στοιχεία του κώδικα $\mathcal{A}$. Για κάθε $0 \leq i \leq \delta-2$ έστω $m_i(x)$ το ελάχιστο πολυώνυμο του α^{b+i} επί του $\mathbb{F}$ και $\gamma(x) = \varepsilon\kappa\pi(\, m_i(x),\ 0 \leq i \leq \delta-2\,)$. Δηλαδή το πολυώνυμο $\gamma(x)$ είναι το μικροτέρου βαθμού μονικό πολυώνυμο επί του $\mathbb{F}$, το οποίο έχει ως ρίζες τα στοιχεία α^b, α^{b+1}, ..., $\alpha^{b+\delta-2}$. Από την άλλη πλευρά το πολυώνυμο $\hat{\gamma}(x) = (x-\alpha^b)(x-\alpha^{b+1})(x-\alpha^{b+2}) \cdots (x-\alpha^{b+\delta-2}) \in \mathbb{K}[x]$ έχει ακριβώς τα στοιχεία α^b, α^{b+1}, ..., $\alpha^{b+\delta-2}$ ως ρίζες. Δη-

λαδή το πολυώνυμο $\hat{\gamma}(x)$ διαιρεί το πολυώνυμο $\gamma(x)$ (η διαίρεση γίνεται στο δακτύλιο $\mathbb{K}[x]$).

Έστω $\mathbf{r} = r_0 r_1 \cdots r_{n-1}$ ένα στοιχείο του κώδικα $\mathcal{A}$, δηλαδή το πολυώνυμο $r_0+r_1x+\cdots+r_{n-1}x^{n-1} \in \mathbb{F}_{n-1}[x]$ έχει ως ρίζες τα α^{b+i} για όλα τα $0 \leq i \leq \delta-2$. Από τον ορισμό του πολυωνύμου $\gamma(x)$, το $\gamma(x)$ διαιρεί το πολυώνυμο $r_0+r_1x+\cdots+r_{n-1}x^{n-1} \in \mathbb{F}_{n-1}[x]$. Αυτό σημαίνει ότι το στοιχείο $\mathbf{r} = r_0 r_1 \cdots r_{n-1}$ ανήκει στον BCH κώδικα $\mathcal{BCH} = \mathcal{BCH}(n, \delta, \alpha, b)$.

Προφανώς ισχύει ότι $\mathcal{BCH} = \mathcal{BCH}(n, \delta, \alpha, b) \subseteq \mathcal{A}$.

Ανακεφαλαιώνοντας έχουμε:

Θεώρημα 5.2.5. *Κάθε BCH κώδικας $\mathcal{BCH} = \mathcal{BCH}(n, \delta, \alpha, b)$ επί ενός πεπερασμένου σώματος $\mathbb{F}$ προέρχεται από την αποδελτίωση (σμίκρυνση) ενός συμβατικού κώδικα Reed-Solomon.*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Πόρισμα 5.2.6. *Έστω $\mathbb{K}$ ένα πεπερασμένο σώμα και $\mathcal{CRS}$ ένας συμβατικός κώδικας Reed-Solomon μήκους n (επί του $\mathbb{K}$). Για κάθε υπόσωμα $\mathbb{F}$ του $\mathbb{K}$ ορίζεται ένας BCH κώδικας $\mathcal{BCH}_{\mathbb{F}} = \mathcal{CRS} \cap \mathbb{F}^n$.*

Αντίστροφα, έστω $\mathbb{F}$ ένα πεπερασμένο σώμα και $\mathcal{BCH}$ ένας BCH κώδικας. Τότε υπάρχει μια επέκταση $\mathbb{K}$ του σώματος $\mathbb{F}$ επί του οποίου ορίζεται ένας συμβατικός κώδικας Reed-Solomon $\mathcal{CRS}$.

Παράδειγμα 5.2.7. Στο Παράδειγμα 5.2.4 είχαμε κατασκευάσει έναν κώδικα Reed-Solomon $\mathcal{RS}(7, 3, \alpha)$ επί του αλφαβήτου $\mathbb{K} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$.

Στο Παράδειγμα $5.1.6_1$ είχαμε κατασκευάσει έναν δυαδικό BCH κώδικα $\mathcal{BCH}(7, 3, \alpha)$.

Προφανώς ισχύει ότι $\mathcal{BCH} = \mathcal{RS} \cap \mathbb{Z}_2^7$. Δηλαδή ο BCH κώδικας $\mathcal{BCH}$ επί του σώματος $\mathbb{Z}_2$ προέρχεται από την αποδελτίωση (σμίκρυνση) του κώδικα Reed-Solomon $\mathcal{RS}(7, 3, \alpha)$ επί του αλφαβήτου $\mathbb{K}$.

Σχόλιο 5.2.8. Είδαμε ότι ένας BCH κώδικας μπορεί να προέλθει ως υποκώδικας ενός συμβατικού κώδικα Reed-Solomon. Από την άλλη πλευρά έχουμε ορίσει τους κώδικες Reed-Solomon ως πρωταρχικούς συμβατικούς κώδικες Reed-Solomon.

Οι έννοιες πρωταρχικός BCH κώδικας και κώδικας Reed-Solomon ταυτίζονται υπό την εξής έννοια: Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathbb{K}$ μια επέκτασή του βαθμού $s = 1$ ($\mathbb{F} = \mathbb{K}$). Σύμφωνα με τον Ορισμό 5.1.1 ορίζεται ο πρωταρχικός BCH κώδικας $\mathcal{BCH} = \mathcal{BCH}(n, \delta, \alpha, b)$ μήκους $n = q - 1$ επί του σώματος $\mathbb{F} = \mathbb{K}$.

Στην Παρατήρηση $5.2.2_1$ όμως, όπως και στη σελίδα 5.1, είδαμε ότι αυτός ειναι και ο ορισμός ενός κώδικα Reed-Solomon.

5.2.2 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;* αυτής της παραγράφου.

2. Έστω $\mathbb{F} = \mathbb{Z}_{13}$.

   (α′) Να κατασκευάσετε έναν υπό την στενή έννοια συμβατικό κώδικα Reed-Solomon (με σώμα βάσης το $\mathbb{Z}_2$) μήκους 15 και διάστασης 11. Ποιά είναι η ελάχιστη απόστασή του;

   (β′) Να κατασκευάσετε έναν υπό τη στενή έννοια κώδικα Reed-Solomon $\mathcal{RS}(n, \delta, \alpha)$ επί του $\mathbb{F}$ μήκους $n = 12$, προσχεδιασμένης απόστασης $\delta = 5$ και με πρωταρχικό στοιχείο $\alpha = 2$.

   Συγκεκριμμένα να υπολογίσετε το πολυώνυμο γεννήτορα και έναν πίνακα ελέγχου ισοτιμίας.

   (γ′) Να μελετήσετε τον δυϊκό κώδικα του $\mathcal{RS}(n, \delta, \alpha)$. Συγκεκριμμένα να υπολογίσετε το πολυώνυμο γεννήτορα και έναν πίνακα ελέγχου ισοτιμίας. Επίσης να υπολογίσετε την ελάχιστη απόστασή του.

   (δ′) Έστω $\gamma(x)$ το πολυώνυμο γεννήτορας του κώδικα $\mathcal{RS}(n, \delta, \alpha)$. Να μελετήσετε το κυκλικό συμπλήρωμά του. Δηλαδή τον κυκλικό κώδικα που έχει ως πολυώνυμο γεννήτορα το πολυώνυμο $g(x)$ με την ιδιότητα $x^{12} - 1 = \gamma(x) \cdot g(x)$. δείξτε ότι και αυτός ο κώδικας είναι ένας κώδικας Reed-Solomon.

3. Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία και α ένα πρωταρχικό στοιχείο του. Έστω k ένας ακέραιος με $1 \leq k \leq n = q - 1$.

Ορίζουμε έναν κώδικα ως εξής:

$$\mathcal{C} = \{ (\varphi(1), \varphi(\alpha), \varphi(\alpha^2), \dots, \varphi(\alpha^{q-2})) \mid \varphi(x) \in \mathbb{F}_{k-1}[x] \}.$$

Δείξτε ότι ο κώδικας αυτός είναι ένας, υπό την στενή έννοια, κώδικας Reed-Solomon επί του $\mathbb{F}$. Υπολογίστε το πολυώνυμο γεννήτορα και έναν πίνακα ελέγχου ισοτιμίας.

(Η άσκηση αυτή αποτελεί έναν ισοδύναμο ορισμό ενός, υπό την στενή έννοια, κώδικα Reed-Solomon. Βλέπε και την Παρατήρηση 5.3.7).

4. (Συνέχεια της προηγουμένης άσκησης) Έστω ότι έχουμε τον κώδικα:

$$\mathcal{C} = \{ (\varphi(1), \varphi(\alpha), \varphi(\alpha^2), \dots, \varphi(\alpha^{q-2})) \mid \varphi(x) \in \mathbb{F}_{k-1}[x] \}.$$

Επιλέγουμε ως πηγή πληροφοριών το $\mathbb{F}^k$ και ως συνάρτηση κωδικοποίησης την $f : \mathbb{F}^k \longrightarrow \mathcal{C}$ με:

$$f(r_0, r_1, \dots, r_{k-1}) = (\varphi(1), \varphi(\alpha), \varphi(\alpha^2), \dots, \varphi(\alpha^{q-2})),$$

όπου $\varphi(x) = r_0 + r_1 x +, \cdots + r_{k-1} x^{k-1}$.

Δείξτε ότι η f είναι πράγματι συνάρτηση κωδικοποίησης.

Να κωδικοποιήσετε την λέξη $(1, 1, \dots, 1)$.

5. Έστω $\mathcal{CRS}(n = 9, \delta = 4, \alpha, b = 0)$ ένας συμβατικός κώδικας Reed-Solomon επί ενός σώματος $\mathbb{F}$ με 2^6 το πλήθος στοιχεία, και το $\alpha \in \mathbb{F}$ να είναι τάξης 9.

   (α΄) Δείξτε ότι ο κώδικας αυτός είναι κυκλικός.

   (β΄) Υπολογίστε έναν γεννήτορα πίνακά του.

   (γ΄) Δείξτε ότι το στοιχείο:

$$(1, \alpha^3, \alpha^{-3}, 1, \alpha^3, \alpha^{-3}, 1, \alpha^3, \alpha^{-3}) \in \mathbb{F}$$

   αποτελεί (κωδικο)λέξη.

5.3 Γενικευμένοι κώδικες Reed-Solomon

Στην προηγουμένη παράγραφο ορίσαμε τους συμβατικούς κώδικες Reed-Solomon μήκους n και προσχεδιασμένης απόστασης δ επί ενός σώματος με την βοήθεια ενός πρωταρχικού στοιχείου α του σώματος, λαμβάνοντας ως πίνακα ελέγχου ισοτιμίας του κώδικα τον $(\delta-1)\times n$ πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & \alpha^b & (\alpha^b)^2 & \cdots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \cdots & (\alpha^{b+1})^{n-1} \\ 1 & \alpha^{b+2} & (\alpha^{b+2})^2 & \cdots & (\alpha^{b+2})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & \cdots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix},$$

όπου b είναι ένας μη αρνητικός ακέραιος.

Θα δούμε πώς μπορούμε να γενικεύσουμε την ανωτέρω κατασκευή.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\alpha_1, \alpha_2, \ldots, \alpha_n$ διακεκριμένα μη μηδενικά στοιχεία του $\mathbb{F}$. Επίσης έστω $u_1, u_2, \ldots, u_n$ μη μηδενικά (όχι κατ' ανάγκη διακεκριμένα) στοιχεία του $\mathbb{F}$ και δ ένας ακέραιος με $2 \le \delta \le n$.

Ο γραμμικός κώδικας $\mathcal{GRS}$ που ορίζεται έχοντας ως πίνακα ελέγχου ισοτιμίας τον πίνακα $\mathrm{H} =$

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ (\alpha_1)^{\delta-2} & (\alpha_2)^{\delta-2} & (\alpha_3)^{\delta-2} & \cdots & (\alpha_n)^{\delta-2} \end{pmatrix} \cdot \begin{pmatrix} u_1 & 0 & 0 & \cdots & 0 \\ 0 & u_2 & 0 & \cdots & 0 \\ 0 & 0 & u_3 \cdots & 0 & \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & u_n \end{pmatrix}$$

με στοιχεία από το αλφάβητο $\mathbb{F}$ ονομάζεται **Γενικευμένος κώδικας Reed-Solomon** επί του σώματος $\mathbb{F}$ και ο πίνακας H ο *κανονικός* πίνακας ελέγχου ισοτιμίας του.

Από τον ορισμό απαιτήται το μήκος n του κώδικα να μην υπερβαίνει το πλήθος των μη μηδενικών στοιχείων του σώματος επί του οποίου ορίζεται. Αν κάνουμε τον πολλαπλασιασμό των δύο ανωτέρω πινάκων βλέπουμε ότι η i-στήλη του πρώτου πίνακα πολλαπλασιάζεται με το στοιχείο u_i. Για τον

λόγο αυτό τα στοιχεία u_i, $i = 1, \dots, n$ ονομάζονται *συντελεστές στηλών* ενώ τα στοιχεία α_i, $i = 1, \dots, n$ ονομάζονται *εντοπισμοί* του κώδικα.

Πριν προχωρήσουμε ας δούμε ένα παράδειγμα. Έστω α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{F}$ και b ένας μη αρνητικός ακέραιος. Θέτουμε $\alpha_i = \alpha^{i-1}$ και $u_i = \alpha^{b(i-1)}$, $i = 1, \dots, n$. Στην περίπτωση αυτή έχουμε ότι:

$$\mathrm{H} = \begin{pmatrix} 1 & \alpha^b & (\alpha^b)^2 & \cdots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & \cdots & (\alpha^{b+1})^{n-1} \\ 1 & \alpha^{b+2} & (\alpha^{b+2})^2 & \cdots & (\alpha^{b+2})^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & \cdots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix}.$$

Παρατηρούμε ότι ο πίνακας H είναι ο πίνακας ελέγχου ισοτιμίας ενός συμβατικού κώδικα Reed-Solomon. Το γεγονός αυτό δικαιολογεί την ονομασία γενικευμένοι κώδικες Reed-Solomon.

Θέτουμε $k = n - \delta + 1$.

Θεώρημα 5.3.1. *Ένας γενικευμένος κώδικας Reed-Solomon $\mathcal{GRS}$ είναι ένας κώδικας με παραμέτρους $[n, k, d = n - k + 1]$, δηλαδή ένας μέγιστης (ελάχιστης) απόστασης (MDS κώδικας).*

Απόδειξη. Ο πίνακας ελέγχου ισοτιμίας H του κώδικα έχει $\delta - 1 = n - k$ το πλήθος γραμμές. Η απόδειξη είναι παρόμοια με την απόδειξη του Θεωρήματος 5.2.3 με μόνη παρατήρηση ότι ο πολλαπλασιασμός των στηλών ενός πίνακα Vandermonde με μη μηδενικά στοιχεία δεν αλλάζει την τάξη του. (Βλέπε και Θεώρημα 2.6.6). ό.έ.δ.

Έστω ένας γενικευμένος κώδικας Reed-Solomon $\mathcal{GRS}$. Όπως προηγουμένως, αν ο κώδικας έχει μήκος $n = q - 1$ θα ονομάζεται *πρωταρχικός*.

Στην περίπτωση, όπου οι συντελεστές στηλών είναι ίσοι με τους αντιστοίχους εντοπισμούς του κώδικα ($u_i = \alpha_i$, $1 \le i \le n$), ο κώδικας θα ονομάζεται *υπό την στενή έννοια* γενικευμένος κώδικας Reed-Solomon. (Στους συμβατικούς κώδικες Reed-Solomon αυτό ισχύει όταν $b = 1$) .

Στην περίπτωση, όπου όλοι οι συντελεστές στηλών είναι ίσοι με 1 ($u_i = 1$, $1 \le i \le n$), ο κώδικας θα ονομάζεται *κανονικοποιημένος*. (Στους συμβατικούς κώδικες Reed-Solomon αυτό ισχύει όταν $b = 0$).

5.3.1 Μια άλλη παρουσίαση των γενικευμένων κωδίκων Reed-Solomon

Στο παρόν εδάφιο θα δούμε τους γενικευμένους κώδικες Reed-Solomon υπό άλλη οπτική γωνία.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathcal{GRS}$ ένας γενικευμένος κώδικας Reed-Solomon με παραμέτρους $[n,\, k,\, d = n-k+1]$ και πίνακα ελέγχου ισοτιμίας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \alpha_3^{n-k-1} & \cdots & \alpha_n^{n-k-1} \end{pmatrix} \cdot \begin{pmatrix} u_1 & 0 & 0 & \cdots & 0 \\ 0 & u_2 & 0 & \cdots & 0 \\ 0 & 0 & u_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & u_n \end{pmatrix}$$

(Δεν ξεχνάμε ότι έχουμε θέσει $k = n-\delta+1$, οπότε $\delta - 2 = n-k-1$).

Ως γνωστόν (Θεώρημα 2.6.3), ο δυϊκός κώδικας $\mathcal{GRS}^{\perp}$ είναι και αυτός ένας MDS κώδικας. Θα δείξουμε επιπλέον ότι **και** αυτός ο κώδικας είναι ένας γενικευμένος κώδικας Reed-Solomon.

Θεωρούμε τον $k \times n$ πίνακα:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}.$$

Θα δείξουμε ότι υπάρχουν $v_1, v_2, \ldots, v_n$ μη μηδενικά στοιχεία του $\mathbb{F}$ με την ιδιότητα:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} v_1 & 0 & 0 & \cdots & 0 \\ 0 & v_2 & 0 & \cdots & 0 \\ 0 & 0 & v_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & v_n \end{pmatrix} \cdot \mathrm{H}^t = \mathbf{0} \quad (*)$$

Αν αποδείξουμε τη σχέση αυτή θα έχουμε αποδείξει ότι ο πίνακας:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} v_1 & 0 & 0 & \cdots & 0 \\ 0 & v_2 & 0 & \cdots & 0 \\ 0 & 0 & v_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & v_n \end{pmatrix}$$

είναι γεννήτορας πίνακας του κώδικα $\mathcal{GRS}$ και ταυτόχρονα πίνακας ελέγχου ισοτιμίας του δυϊκού κώδικα $\mathcal{GRS}^{\perp}$ (Πρόταση 2.2.12).

Κάνοντας τις πράξεις στην σχέση $(*)$, έπεται ότι αναζητούμε μη μηδενικά στοιχεία $v_1, v_2, \ldots, v_n \in \mathbb{F}$ έτσι ώστε ο $k \times (n-k)$ πίνακας $\left(\sum_{r=1}^{n} u_r v_r \alpha_r^{i+j} \right)$ να είναι ο μηδενικός πίνακας, όπου τα $i = 0, 1, 2, \ldots, k-1$ και $j = 0, 1, 2, \ldots, n-k-1$ διατρέχουν τις γραμμές και στήλες αντίστοιχα του πίνακα αυτού. Δηλαδή αναζητούμε μη μηδενικά στοιχεία $v_1, v_2, \ldots, v_n \in \mathbb{F}$, τα οποία να αποτελούν λύση του εξής γραμμικού συστήματος:

$$\begin{pmatrix} u_1 & u_2 & u_3 & \cdots & u_n \\ u_1\alpha_1 & u_2\alpha_2 & u_3\alpha_3 & \cdots & u_n\alpha_n \\ u_1\alpha_1^2 & u_2\alpha_2^2 & u_3\alpha_3^2 & \cdots & u_n\alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ u_1\alpha_1^{n-2} & u_2\alpha_2^{n-2} & u_3\alpha_3^{n-2} & \cdots & u_n\alpha_n^{n-2} \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_n \end{pmatrix} = \mathbf{0}.$$

Το σύστημα αυτό έχει ως πίνακα συντελεστών έναν $(n-1) \times n$ πίνακα με τάξη ίση με $n-1$ (γιατί;). Συνεπώς ο χώρος λύσεων του συστήματος αυτού είναι διανυσματικός υπόχωρος διάστασης ίσης με 1 και για κάθε (μη μηδενική) λύση του $v_1, v_2, \ldots, v_n$ ισχύει ότι $v_i \neq 0$ για όλα τα $i = 1, 2, \ldots, n$ (γιατί;).

Συνεπώς ανακεφαλαιώνοντας έχουμε:

Θεώρημα 5.3.2. *Έστω $\mathcal{GRS}$ ένας $[n, k, n-k+1]$ γενικευμένος κώδικας Reed-Solomon επί ενός πεπερασμένου σώματος $\mathbb{F}$. Τότε ο δυϊκός κώδικας $\mathcal{GRS}^{\perp}$ είναι επίσης ένας $[n, n-k, k+1]$ γενικευμένος κώδικας Reed-Solomon. Μάλιστα δε και οι δύο κώδικες μπορούν να ορισθούν επί των ιδίων εντοπισμών α_i, $i = 1, \ldots, n$.*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Παρατηρήσεις 5.3.3. 1. Το προηγούμενο σύστημα έχει πολλές λύσεις, που σημαίνει ότι ένας γενικευμένος κώδικας Reed-Solomon μπορεί να ορισθεί με διαφορετικούς συντελεστές στηλών. (Βλέπε και την Άσκηση 2 στο τέλος της παραγράφου).

2. Σύμφωνα με τον ορισμό ενός γενικευμένου κώδικα Reed-Solomon και το Θεώρημα 5.3.1, ο πίνακας:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \alpha_3^{n-2} & \cdots & \alpha_n^{n-2} \end{pmatrix} \cdot \begin{pmatrix} u_1 & 0 & 0 & \cdots & 0 \\ 0 & u_2 & 0 & \cdots & 0 \\ 0 & 0 & u_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & u_n \end{pmatrix}$$

του προηγουμένου συστήματος είναι ο πίνακας ελέγχου ισοτιμίας ενός (άλλου) γενικευμένου κώδικα Reed-Solomon με παραμέτρους $[n, 1, n]$. Επειδή η ελάχιστη απόσταση στον κώδικα αυτόν είναι ίση με το μήκος του κώδικα, έπεται ότι όλα τα στοιχεία του έχουν βάρος ίσον με n. Άρα, πράγματι για κάθε μη μηδενική λύση $v_1, v_2, \ldots, v_n$ ισχύει ότι $v_i \neq 0$ για όλα τα $i = 1, 2, \ldots, n$.

3. Στο προηγούμενο θεώρημα είδαμε ότι ο δυϊκός κώδικας ενός γενικευμένου κώδικα Reed-Solomon είναι και αυτός γενικευμένος κώδικας Reed-Solomon. Στην περίπτωση των BCH κωδίκων αυτό δεν ισχύει γενικά.

Πράγματι, στο Παράδειγμα 5.1.6 $_2$ είχαμε κατασκευάσει έναν πρωταρχικό υπο την στενή έννοια BCH κώδικα $\mathcal{BCH}$ επί του $\mathbb{Z}_2$ μήκους 15. Ο κώδικας αυτός είναι κυκλικός και έχει πολυώνυμο γεννήτορα το $\gamma(x) = x^8+x^7+x^6+x^4+1 \in \mathbb{Z}_2[x]$. Το σύνολο ριζών του πολυωνύμου αυτού είναι το $\{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^8, \alpha^9, \alpha^{12}\}$, όπου $\alpha = x+\langle x^4+x+1\rangle \in \mathbb{K} = \mathbb{Z}_2[x]/\langle x^4+x+1\rangle$.

Από την σχέση $x^{15}-1 = (x^8+x^7+x^6+x^4+1)(x^7+x^6+x^4+1)$ έχουμε ότι το πολυώνυμο γεννήτορας του δυϊκού κώδικα $\mathcal{BCH}^\perp$ είναι το πολυώνυμο $d(x) = x^7+x^3+x+1$ (γιατί;) (βλέπε Θεώρημα 3.2.16). Οι ρίζες του $d(x)$ είναι οι $\alpha^0 = 1, \alpha, \alpha^2, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}$. Έστω $m_0(x) = x-$

1 το ελάχιστο πολυώνυμο του 1, $m_1(x)$ το ελάχιστο πολυώνυμο του α και $m_5(x)$ το ελάχιστο πολυώνυμο του α^5, τότε $d(x) = m_0(x)\cdot m_1(x)\cdot m_5(x)$.

Αν ο κώδικας $\mathcal{BCH}^{\perp}$ ήταν ένας BCH κώδικας, τότε, σύμφωνα με τον ορισμό ενός BCH κώδικα (Ορισμός 5.1.1), θα υπήρχαν ακέραιοι b και δ με $b \geq 0$ και $15 \geq \delta \geq 2$ έτσι ώστε κάθε ένα από τα πολυώνυμα $m_0(x)$, $m_1(x)$ και $m_5(x)$ να έχει ως ρίζα τουλάχιστον ένα από τα στοιχεία α^b, α^{b+1}, ..., $\alpha^{b+\delta-2}$ και επιπλέον όλα τα στοιχεία αυτά να είναι ρίζες του $d(x)$. Αυτό όμως είναι αδύνατον καθότι, αν, για παράδειγμα, το α^5, το οποίο είναι ρίζα του $m_5(x)$, ήταν της μορφής $\alpha^5 = \alpha^{b+i}$, $i = 0, \ldots, \delta-2$, τότε αναγκαστικά τουλάχιστον ένα από τα α^3 και α^6 θα ήταν ρίζα του $d(x)$, άτοπο.

Όμοια αποκλείονται και οι υπόλοιπες περιπτώσεις.

Παραδείγματα 5.3.4. 1. Έστω $\mathcal{GRS}$ ένας πρωταρχικός γενικευμένος κώδικας Reed-Solomon επί ενός πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Υποθέτουμε ότι $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ είναι οι εντοπισμοί και $u_1, u_2, u_3, \ldots, u_n$ είναι οι συντελεστές στηλών του. Τότε οι συντελεστές στηλών του δυϊκού κώδικα είναι οι $v_r = \alpha_r/u_r$, $r = 1, 2, \ldots, n$. Πράγματι, ο κώδικας έχει υποτεθεί πρωταρχικός ($n = q-1$). Αντικαθιστούμε στην σχέση $\sum_{r=1}^{n} u_r v_r \alpha_r^{i+j}$ τα v_r με τα α_r/u_r και έχουμε:

$$\sum_{r=1}^{q-1} u_r \alpha_r / u_r \alpha_r^{i+j} = \sum_{r=1}^{q-1} \alpha_r \alpha_r^{i+j}.$$

Έστω α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{F}$. Τα μη μηδενικά στοιχεία του σώματος $\mathbb{F}$ (με μια αναρίθμηση, αν είναι αναγκαία) είναι της μορφής $\alpha_r = \alpha^r$ για όλα τα $r = 1, 2, \ldots, q-1$, οπότε συνεχίζοντας την προηγουμένη ισότητα έχουμε:

$$\begin{aligned}\sum_{r=1}^{q-1} \alpha_r \alpha_r^{i+j} &= \sum_{r=1}^{q-1} \alpha^r (\alpha^r)^{i+j} \\ &= \sum_{r=1}^{q-1} (\alpha^r)^{i+j+1} = \sum_{r=1}^{q-1} (\alpha^{i+j+1})^r \\ &= (\alpha^{(i+j+1)q} - \alpha^{i+j+1})/(\alpha^{i+j+1} - 1) = 0\end{aligned}$$

καθότι $\alpha^{q-1} = 1$.

Η τελευταία ισότητα ισχύει για όλα τα $i = 0, 1, 2, \ldots, k-1$ και $j = 0, 1, 2, \ldots, n-k-1$. Αυτό αποδεικνύει τον ισχυρισμό.

2. Ο Δυϊκός κώδικας ενός κανονικοποιημένου, πρωταρχικού γενικευμένου κώδικα Reed-Solomon είναι ένας υπό την στενή έννοια πρωταρχικός κώδικας Reed-Solomon.

   Πράγματι, επειδή ο κώδικας έχει υποτεθεί κανονικοποιημένος έχουμε ότι όλοι οι συντελεστές στηλών είναι ίσοι με 1 ($u_i = 1$). Από το προηγούμενο παράδειγμα έπεται ότι οι συντελεστές στηλών του δυϊκού κώδικα είναι ίσοι με τους εντοπισμούς του κώδικα ($v_i = \alpha_i$). Αυτό σημαίνει ότι ο δυϊκός κώδικας είναι υπό την στενή έννοια γενικευμένος κώδικας Reed-Solomon.

Έστω $\mathcal{GRS}$ ένας $[n, k, n-k+1]$ γενικευμένος κώδικας Reed-Solomon επί ενός πεπερασμένου σώματος $\mathbb{F}$. Από τα προηγούμενα έχουμε ότι ένας γεννήτορας πίνακάς του είναι της μορφής:

$$\mathrm{G} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix} \cdot \begin{pmatrix} v_1 & 0 & 0 & \cdots & 0 \\ 0 & v_2 & 0 & \cdots & 0 \\ 0 & 0 & v_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & v_n \end{pmatrix}.$$

Επομένως έχουμε ότι $\mathcal{GRS} = \{ (c_0, c_1, \ldots, c_{k-1}) \cdot G \mid (c_0, c_1, \ldots, c_{k-1}) \in \mathbb{F}^k \}$. Αν, ως συνήθως, ταυτοποιήσουμε την προς κωδικοποίηση λέξη $(c_0, c_1, \ldots, c_{k-1})$ με το πολυώνυμο $\varphi(x) = c_0 + c_1 x + \cdots + c_{k-1} x^{k-1} \in \mathbb{F}_{k-1}[x]$, τότε εύκολα βλέπουμε ότι $(c_0, c_1, \ldots, c_{k-1}) \cdot \mathrm{G} = (v_1\varphi(\alpha_1), v_2\varphi(\alpha_2), \ldots, v_n\varphi(\alpha_n))$. Δηλαδή $\mathcal{GRS} = \{ (v_1\varphi(\alpha_1), v_2\varphi(\alpha_2), \ldots, v_n\varphi(\alpha_n)) \mid \varphi(x) \in \mathbb{F}_{k-1}[x] \}$.

Η τελευταία έκφραση ενός γενικευμένου κώδικα Reed-Solomon αποτελεί έναν ισοδύναμο ορισμό των γενικευμένων κωδίκων Reed-Solomon και δικαιολογεί την ονομασία των α_i ως *εντοπισμούς* του κώδικα.

Παρατήρηση 5.3.5. Η αποκωδικοποίηση με έναν γενικευμένο κώδικα Reed-Solomon με ελάχιστη απόσταση $d = n-k+1$ μπορεί να διατυπωθεί τώρα

ως εξής: Υποθέτουμε ότι οι τιμές ενός πολυωνύμου $\varphi(x) = c_0 + c_1 x + \cdots + c_{k-1}x^{k-1} \in \mathbb{F}_{k-1}[x]$ στις θέσεις $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ έχουν υπολογισθεί και έχουμε $\varphi(\alpha_i) = b_i$, $i = 1, 2, \ldots, n$. Αν, κατά τους υπολογισμούς, έχουν γίνει λάθη το πολύ σε $[(d-1)/2] = [(n-k)/2]$ θέσεις, τότε μπορούμε να υπολογίσουμε τους συντελεστές $c_0, c_1, \ldots, c_{k-1}$ του πολυωνύμου.

Ως γνωστόν (Παρεμβολή Lagrange. Παράρτημα: Θεώρημα Α΄.2.36) ένα πολυώνυμο βαθμού $n-1$ μπορεί να υπολογισθεί αν γνωρίζουμε τις τιμές του σε n το πλήθος διακεκριμένες θέσεις. Αυτό αποτελεί ειδική περίπτωση όπου $d = 1$ ($n = k$), δηλαδή δεν επιτρέπεται να υπεισέλθουν λάθη κατά τους υπολογισμούς. Εδώ επιτρέπεται να έχουμε λάθη, οπότε θα μπορούσαμε να μιλήσουμε για *Θορυβώδη παρεμβολή Lagrange*.

Παράδειγμα 5.3.6. Έστω $\mathcal{RS}$ ένας $[n, k, n-k+1]$ πρωταρχικός, υπό την στενή έννοια, συμβατικός κώδικας Reed-Solomon επί ενός πεπερασμένου σώματος $\mathbb{F}$. Στην σελίδα 5.3 είχαμε δει ότι αυτός αποτελεί ειδική περίπτωση ενός γενικευμένου κώδικα Reed-Solomon με στοιχεία εντοπισμού $\alpha_i = \alpha^{i-1}$ και συντελεστές στηλών $u_i = \alpha^{i-1}$, $i = 1, 2, \ldots, n$, όπου α είναι ένα πρωταρχικό στοιχείο του σώματος. Τότε, σύμφωνα με το παράδειγμα 5.3.4 οι συντελεστές στηλών του δυϊκού κώδικα είναι οι $v_i = \alpha_i/u_i = 1$, $i = 1, 2, \ldots, n$. Συνεπώς από τα προηγούμενα έχουμε ότι:

$$\mathcal{RS} = \{\, (\varphi(1), \varphi(\alpha), \ldots, \varphi(\alpha^{n-1})) \mid \varphi(x) \in \mathbb{F}_{k-1}[x] \,\}.$$

Παρατήρηση 5.3.7. Στο προηγούμενο παράδειγμα η έκφραση ενός πρωταρχικού, υπό την στενή έννοια, συμβατικού κώδικα Reed-Solomon $[n, k, n-k+1]$ ως $\mathcal{RS} = \{\, (\varphi(1), \varphi(\alpha), \ldots, \varphi(\alpha^{n-1})) \mid \varphi(x) \in \mathbb{F}_{k-1}[x] \,\}$ αποτέλεσε, ιστορικά, τον πρώτο ορισμό των κωδίκων Reed-Solomon με όλες τις γενικεύσεις και παραλλαγές, που παρουσιάσαμε μέχρι τώρα, να έπονται. Επίσης αυτό απετέλεσε και την βάση για τον ορισμό των Goppa κωδίκων, τους οποίους θα μελετήσουμε στα επόμενα. Το κυριώτερο όμως είναι ότι ο ορισμός αυτός αποτελεί την *πύλη* για την είσοδο σε μια ευρύτατη και άκρως ενδιαφέρουσα περιοχή των Μαθηματικών την '*Αλγεβρική Γεωμετρία και Κώδικες*', η οποία αποτελεί πεδίο σύγχρονης έρευνας και μια περαιτέρω αναφορά είναι πέραν του σκοπού αυτού του βιβλίου.

Για μια πρώτη επαφή ο ενδιαφερόμενος αναγνώστης μπορεί να ανατρέξει στα: Walker, J. L. [2000] και Huffman, C. W. and Pless, V. [2003].

5.3.2 Εναλλασόμενοι Κώδικες

Στην παράγραφο 5.2.1 σελίδα 321 είχαμε παρουσιάσει τους BCH κώδικες ως υποκώδικες των συμβατικών κωδίκων Reed-Solomon. Εδώ θα δούμε πως μπορούμε να το γενικεύσουμε στην περίπτωση των γενικευμένων κωδίκων Reed-Solomon.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία, $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ βαθμού s και $\mathcal{GRS}$ ένας γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{K}$ με παραμέτρους $[n, k, d = n - k + 1]$ (ο κώδικας είναι MDS).

Θεωρούμε τον κώδικα $\mathcal{A} = \mathbb{F}^n \cap \mathcal{GRS}$, δηλαδή από τον κώδικα $\mathcal{GRS}$ επιλέγουμε μόνο τις (κωδικο)λέξεις, των οποίων τα γράμματα (οι χαρακτήρες) ανήκουν στο (αρχικό) σώμα $\mathbb{F}$.

Ο κώδικας $\mathcal{A}$ είναι ένας υποκώδικας του κώδικα $\mathcal{GRS}$ και μάλιστα γραμμικός (ως τομή διανυσματικών χώρων επί του ιδίου σώματος $\mathbb{F}$). Μάλιστα δε ως υποκώδικας του $\mathcal{CRS}$ είναι *αραιώτερος*, δηλαδή η ελάχιστη απόστασή του είναι τουλάχιστον ίση με d.

Ορισμός 5.3.8. *Το ζεύγος των κωδίκων $\mathcal{GRS}$ και $\mathcal{A}$ ονομάζονται **Εναλλασόμενοι** κώδικες και καθένας μεμονωμένα εναλλακτικός (ως προς τον άλλο) κώδικας.*

Έστω $\mathrm{H} = (h_{ij})$ ένας πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{GRS}$. Με την βοήθεια του πίνακα αυτού θα κατασκευάσουμε έναν πίνακα ελέγχου ισοτιμίας του εναλλακτικού κώδικα $\mathcal{A}$. Κάθε στοιχείο h_{ij} ανήκει στο σώμα $\mathbb{K}$, το οποίο είναι μια επέκταση του σώματος $\mathbb{F}$ βαθμού s. Θεωρούμε το σώμα $\mathbb{K}$ ως διανυσματικό χώρο επί του $\mathbb{F}$ και επιλέγουμε και σταθεροποιούμε μια διατεταγμένη βάση του $\mathbf{B} = \{e_1, e_2, \dots, e_s\}$. Κάθε h_{ij} το εκφράζουμε ως γραμμικό συνδυασμό των δυανυσμάτων της βάσης που επιλέξαμε και με $[r_i^j]$ συμβολίζουμε το διάνυσμα στήλη των συντελεστών στην έκφραση αυτή. Δηλαδή $h_{ij} = [r_i^j]^t \cdot (e_1, e_2, \dots, e_s)^t$.

Από τον τρόπο ορισμού του κώδικα $\mathcal{A}$ έχουμε ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1, c_2, \ldots, c_n) \cdot \mathrm{H}^t = \mathbf{0}$. Οπότε, σε συνδυασμό με την προηγούμενη σχέση έχουμε ότι το $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $c_1[r_i^1] + c_2[r_i^2] + \cdot c_n[r_i^n] = \mathbf{0}$ για κάθε $i = 1, 2, \ldots, d-1$.

Κατασκευάζουμε τον πίνακα:

$$\mathrm{P} = \begin{pmatrix} [r_1^1] & [r_1^2] & [r_1^3] & \cdots & [r_1^n] \\ [r_2^1] & [r_2^2] & [r_2^3] & \cdots & [r_2^n] \\ [r_3^1] & [r_3^2] & [r_3^3] & \cdots & [r_3^n] \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ [r_{d-1}^1] & [r_{d-1}^2] & [r_{d-1}^3] & \cdots & [r_{d-1}^n] \end{pmatrix},$$

ο οποίος προκύπτει από τον πίνακα H με την αντικατάσταση κάθε h_{ij} με το διάνυσμα στήλη $[r_i^j]$ των συντελεστών του στην έκφρασή του ως γραμμικό συνδυασμό των διανυσμάτων της βάσης $\mathbf{B}$. Προφανώς από τα προηγούμενα έπεται ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1, c_2, \ldots, c_n) \cdot \mathrm{P}^t = \mathbf{0}$.

Στον πίνακα P, αν αναπτύξουμε κάθε στήλη $[r_i^j]$, η οποία περιλαμβάνει s το πλήθος στοιχεία, τότε προκύπτει ένας $(d-1)s \times n$ πίνακας $\overline{H}$, του οποίου τα στοιχεία είναι από το σώμα $\mathbb{F}$ και για τον οποίο ισχύει ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$ ανήκει στον κώδικα αν και μόνο αν $(c_1, c_2, \ldots, c_n) \cdot \overline{H}^t = \mathbf{0}$.

Συνεπώς με την διαδικασία αυτή κατασκευάσαμε έναν πίνακα ελέγχου ισοτιμίας για τον εναλλακτικό κώδικα $\mathcal{A}$ επί του σώματος $\mathbb{F}$.

Συνοψίζοντας, οι παράμετροι του κώδικα $\mathcal{A}$ είναι οι εξής:

Το μήκος του είναι n, ίσον με το μήκος του γενικευμένου κώδικα Reed-Solomon $\mathcal{GRS}$, του οποίου σμίκρυνση αποτελεί ο κώδικας $\mathcal{A}$.

Η ελάχιστη απόστασή του είναι μεγαλύτερη ή ίση από την ελάχιστη απόσταση d του κώδικα $\mathcal{GRS}$.

Η διάστασή του, έστω r, ικανοποιεί την σχέση $n - r \leq (d-1)s$, καθότι η διαφορά $n - r$ δεν υπερβαίνει το πλήθος των γραμμών του πίνακα ελέγχου ισοτιμίας του.

Από την τελευταία σχέση έχουμε $r \geq n - (d-1)s$, δηλαδή προκύπτει ένα κάτω φράγμα για την διάσταση του κώδικα $\mathcal{A}$.

Ανακεφαλαιώνοντας έχουμε:

Αν θέλουμε να κατασκευάσουμε έναν κώδικα, επί ενός πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία, μήκους n και με επιθυμητή ελάχιστη απόσταση τουλάχιστον ίση με d, τότε αρκεί να επιλέξουμε έναν θετικό ακέραιο s, μια επέκταση $\mathbb{K}$ του σώματος $\mathbb{F}$ βαθμού s και να κατασκευάσουμε έναν γενικευμένο κώδικα Reed-Solomon $\mathcal{GRS}$ επί του $\mathbb{K}$ με παραμέτρους $[n,\, n-d+1,\, d]$. Οπότε ο εναλλακτικός κώδικας $\mathcal{A}$ που κατασκευάσαμε προηγουμένως πληροί τις απαιτήσεις μας. Επιπλέον η απαίτηση ο κώδικας να είναι όσον το δυνατόν μεγαλύτερος (να έχει ικανότητα κωδικοποίησης μεγάλου όγκου πληροφοριών) επιβάλει το κάτω φράγμα στη σχέση $r \geq n-(d-1)s$ να είναι όσον το δυνατόν μεγαλύτερο, δηλαδή ο βαθμός επέκτασης s να είναι όσον το δυνατόν μικρότερος. Από την άλλη πλευρά ο περιορισμός, σε έναν γενικευμένο κώδικα Reed-Solomon $\mathcal{GRS}$, το μήκος του κώδικα δεν πρέπει να υπερβαίνει το μέγεθος του σώματος $\mathbb{K}$ ($n \leq q^s$) επιβάλλει $s \geq [log_q n]$.

Παρατηρήσεις 5.3.9.

1. Η όλη διαδικασία 'μετάβασης' από έναν κώδικα σε έναν άλλο και αντίστροφα, την οποία παρουσιάσαμε προηγουμένως διακαιολογεί την ονομασία εναλλασόμενοι/εναλλακτικοί κώδικες.

2. Όπως θα έχετε ήδη παρατηρήσει, η διαδικασία κατασκευής του εναλλακτικού κώδικα $\mathcal{A} = \mathbb{F}^n \cap \mathcal{GRS}$, ως προς τον γενικευμένο κώδικα Reed-Solomon $\mathcal{GRS}$, αποτελεί μια εφαρμογή όσων έχουν παρουσιασθεί στην Παράγραφο 2.3.2.

Παράδειγμα 5.3.10. Έστω $\mathbb{F} = \mathbb{Z}_2$, $n = 7$, $d = 3$ και $s = 3$. Λαμβάνουμε την επέκταση $\mathbb{K} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ και το πρωταρχικό στοιχείο $\alpha = x + \langle x^3 + x + 1\rangle$.

Επί του σώματος $\mathbb{K}$ κατασκευάζουμε τον πρωταρχικό, κανονικοποιημένο γενικευμένο κώδικα Reed-Solomon $\mathcal{GRS}$ με παραμέτρους $[n = 7, n-d+1 = 5, d = 3]$, ο οποίος έχει ως πίνακα ελέγχου ισοτιμίας τον πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}.$$

Επιλέγουμε και σταθεροποιούμε την διατεταγμένη βάση $\mathbf{B} = \{1, \alpha, \alpha^2\}$ το σώματος $\mathbb{K}$ επί του $\mathbb{F} = \mathbb{Z}_2$. Κάθε στοιχείο του πίνακα το εκφράζουμε ως

γραμμικό συνδυασμό των διανυσμάτων της βάσης που επιλέξαμε και με $[r_i^j]$ συμβολίζουμε το διάνυσμα στήλη των συντελεστών του στοιχείου στη θέση $(i,\, j)$ στην έκφραση αυτή. Για παράδειγμα:

$$1 = [r_1^1]^t \cdot (1,\, \alpha,\, \alpha^2)^t = (1,0,0) \cdot (1,\, \alpha,\, \alpha^2)^t,$$
$$\alpha^6 = [r_2^4]^t \cdot (1,\, \alpha,\, \alpha^2)^t = (1,0,1) \cdot (1,\, \alpha,\, \alpha^2)^t.$$

Τελικά ο $(2 \cdot 3) \times 7)$ πίνακας:

$$\overline{\mathrm{H}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ - & - & - & - & - & - & \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

ο οποίος κατασκευάστηκε με την διαδικασία που περιγράψαμε, είναι ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{A}$. Προφανώς μπορούμε να διαγράψουμε την δεύτερη και τρίτη γραμμή του πίνακα $\overline{\mathrm{H}}$ και να προκύψει ο πίνακας:

$$\widehat{\mathrm{H}} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

ο οποίος είναι ένας άλλος πίνακας ελέγχου ισοτιμίας του κώδικα $\mathcal{A}$. Εύκολα βλέπουμε τώρα ότι οι παράμετροι του κώδικα $\mathcal{A}$ είναι $[7,\, 3,\, 4]$, δηλαδή η ελάχιστη απόσταση του κώδικα $\mathcal{A}$ είναι γνήσια μεγαλύτερη από την ελάχιστη απόσταση του κώδικα $\mathcal{GRS}$.

Οι κώδικες $\mathcal{GRS}$ και $\mathcal{A}$ αποτελούν ένα ζεύγος εναλλασομένων κωδίκων.

Συγκρίνετε το παράδειγμα αυτό με το παράδειγμα 5.1.10.

5.3.3 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;* αυτής της παραγράφου.

2. Έστω $\mathcal{GRS}$ ένας γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{F}$ με παραμέτρους $[n,\, k,\, d = n-k+1]$, με εντοπισμούς τα στοιχεία α_i, $i = 1, 2, \ldots, n$ και συντελεστές στηλών τα στοιχεία u_i, $i = 1, 2, \ldots, n$.

   (α′) Δείξτε ότι ο κώδικας $\mathcal{GRS}$ είναι ίσος με έναν άλλο γενικευμένο κώδικα Reed-Solomon επί του σώματος $\mathbb{F}$, με εντοπισμούς τα στοιχεία α_i^{-1}, $i = 1, 2, \ldots, n$ και συντελεστές στηλών τα (κατάλληλα επιλεγμένα) στοιχεία v_i, $i = 1, 2, \ldots, n$, τα οποία εσείς θα υπολογίσετε.

   (β′) Έστω $\mu, \nu, \eta \in \mathbb{F}$ με $\mu, \eta \neq 0$. Ορίζουμε έναν άλλο γενικευμένο κώδικα Reed-Solomon $\mathcal{GRS}'$ επί του σώματος $\mathbb{F}$, με εντοπισμούς τα στοιχεία α'_i, $i = 1, 2, \ldots, n$ και συντελεστές στηλών τα στοιχεία u'_i, $i = 1, 2, \ldots, n$, όπου $\alpha'_i = \mu\alpha_i + \nu$ και $u'_i = \eta u_i$.
   Δείξτε ότι οι δύο κώδικες $\mathcal{GRS}$ και $\mathcal{GRS}'$ είναι ίσοι.

   (γ′) Έστω $\mu, \nu, \sigma, \tau \in \mathbb{F}$ με $\mu\tau \neq \sigma\nu$. Δείξτε ότι ο κώδικας $\mathcal{GRS}$ είναι ίσος με τον γενικευμένο κώδικα Reed-Solomon επί του σώματος $\mathbb{F}$, του οποίου οι εντοπισμοί είναι τα στοιχεία $\alpha'_i = \frac{\mu\alpha_i+\nu}{\sigma\alpha_i+\tau}$, $i = 1, 2, \ldots, n$ και οι συντελεστές στηλών είναι κατάλληλα επιλεγμένοι.

3. Έστω $\mathcal{GRS}$ ένας γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{F}$ με παραμέτρους $[n,\, k,\, d = n-k+1]$ $(1 < k < n)$. Δείξτε ότι υπάρχει ένας άλλος γενικευμένος κώδικας Reed-Solomon $\overline{\mathcal{GRS}}$ με παραμέτρους $[n,\, k+1,\, d-1 = n-(k+1)+1]$, του οποίου (γνήσιος) υποκώδικας είναι ο κώδικας $\mathcal{GRS}$.

4. Έστω $\mathcal{GRS}$ ένας γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{F}$ με παραμέτρους $[n,\, k,\, d = n-k+1]$, εντοπισμούς τα στοιχεία α_i, $i = 1, 2, \ldots, n$ και συντελεστές στηλών τα στοιχεία u_i, $i = 1, 2, \ldots, n$. Δείξτε ότι για ένα πολυώνυμο $f(x) = r_0 + r_1 x + \cdots + r_{n-k}x^{n-k} \in \mathbb{F}[x]$ βαθμού $n-k$ μπορούμε να επιλέξουμε τους συντελεστές έτσι ώστε $f(\alpha_i) \neq 0$ για όλα τα $i = 1, 2, \ldots, n$.

   Επιλέγουμε και σταθεροποιούμε ένα τέτοιο πολυώνυμο.

   (α′) Έστω
   $$\partial_i(x) = -\frac{f(x) - f(\alpha_i}{f(\alpha_i)(x-\alpha_i)}\,,\ i = 1, 2, \ldots, n.$$

Δείξτε ότι:

$$\partial_i(x) = -\frac{1}{f(\alpha_i)} \sum_{s=0}^{n-k-1} x^s \sum_{j=s+1}^{n-k} r_j \alpha_i^{j-s-1}$$

για όλα τα $i = 1, 2, \ldots, n$.

(β′) Δείξτε ότι $(x-\alpha_i)\partial_i(x) \equiv 1 \, mod\,(f(x))$, για όλα τα $i = 1, 2, \ldots, n$.

(γ′) Δείξτε ότι το στοιχείο $(c_1, c_2, \ldots, c_n) \in \mathbb{F}^n$ είναι μια (κωδικο)λέξη του κώδικα $\mathcal{GRS}$ αν και μόνο αν $\sum_{i=1}^{n} c_i u_i f(\alpha_i)\partial_i(x) = 0$.

Υπόδειξη: Θεωρήστε ως πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{GRS}$ τον πίνακα:

$$(-1)\begin{pmatrix} r_{n-k} & 0 & 0 & \cdots & 0 \\ r_{n-k-1} & r_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & 0 \\ r_2 & r_3 & \cdots & r_{n-k} & 0 \\ r_1 & r_2 & \cdots & r_{n-k-1} & r_{n-k} \end{pmatrix} \cdot \mathrm{H},$$

όπου H είναι ο πίνακας ελέγχου ισοτιμίας με τον οποίο ορίσθηκε ο κώδικας $\mathcal{GRS}$ και συσχετίστε την i-στήλη του με τους συντελεστές του $\partial_i(x)$.

5. Έστω $\mathcal{C}$ ένας γραμμικός κώδικας επί ενός πεπερασμένου σώματος $\mathbb{F}$ με παραμέτρους $[n, k, d]$, όπου $d \geq 3$. Αποδείξτε ότι υπάρχει ένας γενικευμένος κώδικας Reed-Solomon $\mathcal{GRS}$ επί μιας επέκτασης $\mathbb{K}$ του $\mathbb{F}$ βαθμού $n-k$ και με παραμέτρους $[n, n-1, 2]$ έτσι ώστε οι δύο κώδικες να είναι εναλλασόμενοι (δηλαδή $\mathcal{C} = \mathcal{GRS} \cap \mathbb{F}^n$).

6. Έστω $\mathcal{GRS}$ ένας κανονικοποιημένος γενικευμένος Reed-Solomon κώδικας με παραμέτρους $[n, k, 3]$ και εντοπισμούς $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Μια (κωδικο)λέξη **c** μεταδίδεται μέσω ενός διαύλου επικοινωνίας και λαμβάνεται μια λέξη **y** στην οποία έχει παρεισφύσει ένα λάθος στην θέση j. Κατά την αποκωδικοποίηση υπολογίζουμε το σύνδρομο της **y**, το οποίο, ως προς τον κανονικό πίνακα ελέγχου ισοτιμίας, είναι το $s_0\, s_1$.

Δείξτε ότι $\alpha_j = s_1/s_0$ και ότι η τιμή του λάθους ισούται με s_0.

5.4 Κώδικες Goppa

Μια μεγάλη οικογένεια κωδίκων, οι οποίοι χρησιμοποιούνται σε ένα ευρύ φάσμα εφαρμογών, είναι οι κώδικες Goppa, οι οποίοι επινοήθηκαν από τον V. D. Goppa το 1970. Οι κώδικες αυτοί αποτελούν γενίκευση των υπό στενή έννοια BCH κωδίκων και είναι εναλλακτικοί ως προς έναν γενικευμένο κώδικα Reed-Solomon.

Θα ξεκινήσουμε την παρουσίαση, όπως έχουν ορισθεί αρχικά, χωρίς την αναφορά σε εναλλασόμενους κώδικες και μετά θα δούμε τους κώδικες αυτούς ως εναλλακτικούς ως προς έναν γενικευμένο κώδικα Reed-Solomon.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathbb{K}$ μια επέκτασή του βαθμού m. Έστω $g(x) \in \mathbb{K}[x]$ και $\mathcal{R}_{g(x)}[x] =: \mathbb{K}[x]/\langle g(x) \rangle$ ο δακτύλιος πηλίκων (ορισμένες φορές, αν δεν υπάρχει σύγχυση ως προς το πολυώνυμο $g(x)$, θα συμβολίζουμε απλά με $\mathcal{R}[x]$ και το στοιχείο $\varphi(x) + \langle g(x) \rangle$ θα το συμβολίζουμε με $\overline{\varphi(x)}$). Ο δακτύλιος $\mathcal{R}_{g(x)}[x]$ δεν είναι σώμα, στην περίπτωση όπου το πολυώνυμο $g(x)$ δεν είναι ανάγωγο επί του $\mathbb{K}$. Παρ' όλα ταύτα, αν $g(a) \neq 0$ για $a \in \mathbb{K}$, τότε το στοιχείο $\overline{x-a}$ είναι αντιστρέψιμο στον δακτύλιο $\mathcal{R}_{g(x)}[x]$ (γιατί;). Μάλιστα δε, από την ταυτότητα διαίρεσης πολυωνύμων, έχουμε:

$$(\overline{x-a})^{-1} = -\overline{\frac{(g(x)-g(a))}{x-a}}(g(a))^{-1}. \quad \text{(γιατί;)}$$

Ορισμός 5.4.1. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία, $\mathbb{K}$ μια επέκτασή του βαθμού m και $L = \{a_1, a_2, \ldots, a_n\} \subseteq \mathbb{K}$. Έστω $g(x) \in \mathbb{K}[x]$ με $2 \leq deg(g(x)) = \nu < n$ και με την ιδιότητα $g(a_i) \neq 0$ για κάθε $i = 1, 2, \ldots, n$. Το σύνολο:*

$$\mathcal{G}(L, g(x)) = \left\{ \mathbf{c} = c_1\, c_2 \cdots c_n \mid c_i \in \mathbb{F} \text{ και } \sum_{i=1}^{n} \overline{\frac{c_i}{x-a_i}} = 0 \in \mathcal{R}_{g(x)}[x] \right\}$$

θα ονομάζεται ***κώδικας Goppa*** *.*

Ένας κώδικας Goppa χαρακτηρίζεται από το σύνολο L (σύνολο *εντοπισμών* του κώδικα) και το πολυώνυμο $g(x)$, το οποίο θα ονομάζεται (*χαρακτηριστικό* ή πολυώνυμο *γεννήτορας* του κώδικα).

Πριν δώσουμε παραδείγματα κωδίκων Goppa θα λεπτολογήσουμε περισσότερο για το στοιχείο $(\overline{x-a})^{-1} \in \mathcal{R}_{g(x)}[x]$ και θα καταλήξουμε σε έναν ισοδύναμο ορισμό του κώδικα.

Έστω:

$$g(x) = r_\nu x^\nu + r_{\nu-1}x^{\nu-1} + \cdots + r_1 x + r_0 \in \mathbb{K}[x] \quad (r_\nu \neq 0).$$

Τότε από την σχέση:

$$(\overline{x-a})^{-1} = \overline{-\frac{(g(x)-g(a))}{x-a}(g(a))^{-1}}$$

κάνοντας πρώτα τις πράξεις στον δακτύλιο $\mathbb{K}[x]$ και μετά μεταβαίνοντας στον δακτύλιο πηλίκων $\mathcal{R}_{g(x)}[x] =: \mathbb{K}[x]/\langle g(x)\rangle$ έχουμε ότι:

$$\begin{aligned}(x-a)^{-1} = \; & g(a)^{-1}r_\nu x^{\nu-1} + g(a)^{-1}(r_{\nu-1}+ar_\nu)x^{\nu-2}+\\ & +g(a)^{-1}(r_{\nu-2}+ar_{\nu-1}+a^2r_\nu)x^{\nu-3}+\\ & \vdots\\ & +g(a)^{-1}(r_1+\cdots+a^{\nu-1}r_\nu).\end{aligned} \tag{$*$}$$

Από τον ορισμό ενός κώδικα Goppa έχουμε ότι το στοιχείο $\mathbf{c} = c_1\,c_2\cdots c_n$, $c_i \in \mathbb{F}$, ανήκει στον κώδικα αν:

$$\sum_{i=1}^{n} \overline{\frac{c_i}{x-a_i}} = 0 \in \mathcal{R}_{g(x)}[x],$$

οπότε από την σχέση $(*)$ έχουμε ότι το στοιχείο $\mathbf{c} = c_1\,c_2\cdots c_n$, $c_i \in \mathbb{F}$, ανήκει στον κώδικα αν:

$$\begin{aligned}\sum_{i=1}^{n} c_i[\,& g(a_i)^{-1}r_\nu x^{\nu-1} + g(a_i)^{-1}(r_{\nu-1}+a_ir_\nu)x^{\nu-2}+\\ & + g(a_i)^{-1}(r_{\nu-2}+a_ir_{\nu-1}+a_i^2r_\nu)x^{\nu-3}+\\ & \vdots\\ & + g(a_i)^{-1}(r_1+\cdots+a_i^{\nu-1}r_\nu)\,] = 0 \in \mathcal{R}_{g(x)}[x]\,.\end{aligned}$$

Στη σχέση αυτή κάνουμε πράξεις και την εκφράζουμε ως πολυώνυμο βαθμού

$\nu-1$ (κατά τις κατιούσες δυνάμεις του x) και έχουμε:

$$\left(\sum_{i=1}^{n} c_i\, g(a_i)^{-1} r_\nu\right) x^{\nu-1} + \left(\sum_{i=1}^{n} c_i g(a_i)^{-1}(r_{\nu-1} + a_i r_\nu)\right) x^{\nu-2} + \\ + \left(\sum_{i=1}^{n} c_i\, g(a_i)^{-1}(r_{\nu-2} + a_i r_{\nu-1} + a_i^2 r_\nu)\right) x^{\nu-3} + \cdots + \\ + \left(\sum_{i=1}^{n} c_i\, g(a_i)^{-1}(r_1 + \cdots + a_i^{\nu-1} r_\nu)\right) = 0 \in \mathcal{R}_{g(x)}[x].$$

Επομένως έχουμε ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$, $c_i \in \mathbb{F}$, ανήκει στον κώδικα αν οι συντελεστές των x^j, $j = 0, 1, \ldots, \nu-1$ είναι όλοι ίσοι με μηδέν. Δηλαδή:

$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1} r_\nu = 0$$
$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1}(r_{\nu-1} + a_i r_\nu) = 0$$
$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1}(r_{\nu-2} + a_i r_{\nu-1} + a_i^2 r_\nu) = 0$$
$$\ldots \ldots \ldots$$
$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1}(r_1 + \cdots + a_i^{\nu-1} r_\nu) = 0.$$

Από την πρώτη σχέση, επειδή $r_\nu \neq 0$, έχουμε:

$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1} = 0$$

Από την δεύτερη σχέση έχουμε:

$$(\sum_{i=1}^{n} c_i\, g(a_i)^{-1}) r_{\nu-1} + (\sum_{i=1}^{n} c_i\, g(a_i)^{-1} a_i) r_\nu = 0$$

και επειδή έχουμε $\sum_{i=1}^{n} c_i\, g(a_i)^{-1} = 0$ και $r_\nu \neq 0$ έπεται ότι:

$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1} a_i = 0.$$

Από την τρίτη σχέση, λαμβάνοντας υπ' όψη τα προηγούμενα έχουμε ότι:

$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1} a_i^2 = 0.$$

Οπότε συνεχίζουμε βήμα-βήμα και καταλήγουμε στην τελευταία σχέση, όπου έχουμε:

$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1} a_i^{\nu-1} = 0.$$

Ανακεφαλαιώνοντας, έχουμε τελικά ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$, $c_i \in \mathbb{F}$, ανήκει στον κώδικα αν:

$$\sum_{i=1}^{n} c_i\, g(a_i)^{-1} a_i^{j} = 0 \quad \text{για όλα τα } j = 0,\, 1,\, \ldots,\, \nu-1.$$

Την τελευταία σχέση θα την εκφράσουμε ως γινόμενο πινάκων.

Θεωρούμε τον πίνακα:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{\nu-1} & \alpha_2^{\nu-1} & \alpha_3^{\nu-1} & \cdots & \alpha_n^{\nu-1} \end{pmatrix} \cdot$$

$$\cdot \begin{pmatrix} g(a_1)^{-1} & 0 & 0 & \cdots & 0 \\ 0 & g(a_2)^{-1} & 0 & \cdots & 0 \\ 0 & 0 & g(a_3)^{-1} \cdots & 0 & \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & g(a_n)^{-1} \end{pmatrix}.$$

Οπότε άμεσα προκύπτει ότι το στοιχείο $\mathbf{c} = c_1\, c_2 \cdots c_n$, $c_i \in \mathbb{F}$, ανήκει στον κώδικα αν $(c_1\, c_2 \cdots c_n) \cdot \mathrm{H}^t = \mathbf{0}$.

Έχοντας τώρα υπ' όψη όλα όσα έχουμε παρουσιάσει για τους γενικευμένους κώδικες Reed-Solomon και για τους εναλλασόμενους κώδικες έχουμε αποδείξει το ακόλουθο θεώρημα.

Θεώρημα 5.4.2. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία, $\mathbb{K}$ μια επέκτασή του βαθμού m και $L = \{\, a_1, a_2, \ldots, a_n \,\}$ ένα υποσύνολο στοιχείων του σώματος $\mathbb{K}$. Έστω $g(x) \in \mathbb{K}[x]$ με $2 \leq deg(g(x)) = \nu < n$ και με την ιδιότητα $g(a_i) \neq 0$ για κάθε $i = 1, 2, \ldots, n$. Αν $\mathcal{GRS}$ είναι ο γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{K}$ με πίνακα ελέγχου*

ισοτιμίας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_1^{\nu-1} & a_2^{\nu-1} & a_3^{\nu-1} & \cdots & a_n^{\nu-1} \end{pmatrix} \cdot \begin{pmatrix} g(a_1)^{-1} & 0 & 0 & \cdots & 0 \\ 0 & g(a_2)^{-1} & 0 & \cdots & 0 \\ 0 & 0 & g(a_3)^{-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & g(a_n)^{-1} \end{pmatrix},$$

τότε ο εναλλακτικός κώδικας $\mathcal{A} = \mathbb{F}^n \cap \mathcal{GRS}$ *είναι ο κώδικας Goppa* $\mathcal{G}(L, g(x))$*, ο οποίος έχει παραμέτρους* $[n, k, d]$*, που ικανοποιούν τις σχέσεις* $d \geq \nu + 1$ *και* $n - m\nu \leq k \leq n - \nu$*.*

Απόδειξη. Η απόδειξη έχει προηγηθεί αρκεί, ως προς τις παραμέτρους, να λάβουμε υπ' όψη όσα έχουν ειπωθεί για τις παραμέτρους ενός εναλλακτικού κώδικα. ό.έ.δ.

Παρατηρήσεις 5.4.3. 1. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία, $\mathbb{K}$ μια επέκτασή του βαθμού m και α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Έστω $a_i = \alpha^{i-1}$ για όλα τα $i = 1, 2, \ldots, n$, όπου $n = |\mathbb{K}| - 1$. Θέτουμε $L = \{a_1, a_2, \ldots, a_n\}$. Δηλαδή το σύνολο L περιέχει όλα τα μη μηδενικά στοιχεία του σώματος $\mathbb{K}$. Έστω $g(x) = x^\nu$, όπου $\nu = |\mathbb{K}| - 2 < n$, τότε έχουμε $g(a_i) = a_i^{-1}$ για κάθε $i = 1, 2, \ldots, n$ (γιατί;). Ο πίνακας του σχήματος 5.1 είναι ο πίνακας ελέγχου ενός πρωταρχικού συμβατικού, υπό την στενή έννοια, κώδικα Reed-Solomon, έστω $\mathcal{GRS}$, επί του σώματος $\mathbb{K}$.

Ο εναλλακτικός κώδικας $\mathcal{A} = \mathbb{F}^n \cap \mathcal{GRS}$ είναι αφ' ενός ένας κώδικας Goppa $\mathcal{G}(L, g(x))$, όπου $g(x) = x^\nu$, αφ' ετέρου δε ένας πρωταρχικός, υπό την στενή έννοια, BCH κώδικας (βλέπε σελίδα 321 και την παράγραφο για εναλλασόμενους κώδικες).

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_1^{\nu-1} & a_2^{\nu-1} & a_3^{\nu-1} & \cdots & a_n^{\nu-1} \end{pmatrix} \cdot$$

$$\cdot \begin{pmatrix} g(a_1)^{-1} & 0 & 0 & \cdots & 0 \\ 0 & g(a_2)^{-1} & 0 & \cdots & 0 \\ 0 & 0 & g(a_3)^{-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & g(a_n)^{-1} \end{pmatrix} =$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ a_1^3 & a_2^3 & a_3^3 & \cdots & a_n^3 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_1^{\nu} & a_2^{\nu} & a_3^{\nu} & \cdots & a_n^{\nu} \end{pmatrix}$$

Σχήμα 5.1: ο πίνακας ελέγχου ενός πρωταρχικού συμβατικού κώδικα Reed-Solomon επί του σώματος $\mathbb{K}$.

Επομένως αποδείξαμε ότι οι κώδικες Goppa περιλαμβάνουν ως υποκατηγορία τους υπό στενή έννοια BCH κώδικες.

2. Μπορούμε να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας ενός κώδικα Goppa, ως εναλλακτικού κώδικα ενός γενικευμένου κώδικα Reed-Solomon (βλέπε την σχετική παρουσίαση στην παράγραφο για εναλλασσόμενους κώδικες).

3. Το χαρακτηριστικό πολυώνυμο $g(x)$ ενός κώδικα Goppa δεν είναι κατ' ανάγκην ανάγωγο. Στην ειδική περίπτωση, όπου το $g(x)$ είναι ανάγωγο, ο κώδικας θά ονομάζεται ανάγωγος κώδικας Goppa.

Παραδείγματα 5.4.4. 1. Έστω $\mathbb{F} = \mathbb{Z}_2$ και $\mathbb{K}$ η επέκταση του $\mathbb{F}$ βαθμού 3. Δηλαδή αν α είναι ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$, τότε

$\mathbb{K} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^6\}$. Έστω $\alpha_i = \alpha^{i-1}$ για όλα τα $i = 1, 2, \ldots, 7$. Θέτουμε $L = \{0, a_1, a_2, \ldots, a_7\}$. Δηλαδή το σύνολο L περιέχει όλα τα στοιχεία του σώματος $\mathbb{K}$. Έστω $g(x) = x^2 + x + 1 \in \mathbb{K}[x]$. Το πολυώνυμο αυτό δεν μηδενίζεται από κανένα στοιχείο του σώματος $\mathbb{K}$. Έστω $\mathcal{GRS}$ ο γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{K}$ με πίνακα ελέγχου ισοτιμίας H =

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & a_1 & a_2 & \cdots & a_7 \end{pmatrix} \cdot \begin{pmatrix} g(0)^{-1} & 0 & 0 & \cdots & 0 \\ 0 & g(a_1)^{-1} & 0 & \cdots & 0 \\ 0 & 0 & g(a_2)^{-1} & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & g(a_7)^{-1} \end{pmatrix}.$$

Ο εναλλακτικός κώδικας $\mathcal{A} = \mathbb{F}^n \cap \mathcal{GRS}$ είναι ο κώδικας Goppa $\mathcal{G}(L, g(x))$.

Για να υπολογίσουμε τον πίνακα H, θα πρέπει να εκφράσουμε τις τιμές του πολυωνύμου $g(x)$ στα στοιχεία του σώματος $\mathbb{K}$ ως δυνάμεις του πρωταρχικού στοιχείου α.

Θεωρούμε το ανάγωγο πολυώνυμο $x^3+x+1 \in \mathbb{F}[x]$. Ως γνωστόν το σώμα $\mathbb{K}$ είναι (ισόμορφο με) το σώμα $\mathbb{F}[x]/\langle x^3 + x + 1\rangle$, οπότε, λαμβάνοντας ως πρωταρχικό στοιχείο α το στοιχείο $x + \langle x^3 + x + 1\rangle$, έχουμε ότι το α πληροί την σχέση $\alpha^3 = \alpha + 1$. Έχοντας υπ' όψη τη σχέση αυτή λαμβάνουμε:

$$\begin{aligned} g(a_2) = g(\alpha) &= \alpha^2 + \alpha + 1 = \alpha^2 + \alpha^3 = \alpha^2(\alpha + 1) = \alpha^5, \\ g(a_3) = g(\alpha^2) &= \alpha^4 + \alpha^2 + 1 = \alpha^4 + \alpha^5 + \alpha = \alpha(\alpha^3 + \alpha^4 + 1) \\ &= \alpha(\alpha + \alpha^4) = \alpha^2(1 + \alpha^3) = \alpha^3, \\ g(a_4) = g(\alpha^3) &= \alpha^6 + \alpha^3 + 1 = \alpha^6 + \alpha = \alpha(\alpha^5 + 1) = \alpha(\alpha^2 + \alpha) \\ &= \alpha^2(\alpha + 1) = \alpha^5. \end{aligned}$$

Όμοια συνεχίζοντας έχουμε:

$$g(a_5) = g(\alpha^4) = \cdots = \alpha^6, \qquad g(a_6) = g(\alpha^5) = \cdots = \alpha^6,$$
$$g(a_7) = g(\alpha^6) = \cdots = \alpha^3.$$

Συνεπώς ο πίνακας H είναι ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & \alpha^2 & \alpha^4 & \alpha^2 & \alpha & \alpha & \alpha^4 \\ 0 & 1 & \alpha^3 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}$$

(να κάνετε τον έλεγχο των πράξεων).

Όπως έχουμε επισημάνει ο πίνακας H δεν είναι πίνακας ελέγχου ισοτιμίας του κώδικα Goppa $\mathcal{G}(L,\, g(x))$. Αν θέλουμε να υπολογίσουμε έναν πίνακα ελέγχου ισοτιμίας για τον κώδικα $\mathcal{G}(L,\, g(x))$, θα εφαρμόσουμε την μέθοδο που παρουσιάσαμε στην παράγραφο **Εναλλασόμενοι Κώδικες**. Συγκεκριμμένα, επιλέγοντας την διατεταγμένη βάση $\{\, 1,\, \alpha,\, \alpha^2 \,\}$ του σώματος $\mathbb{K}$ ως διανυσματικού χώρου επί του $\mathbb{F}$, εκφράζουμε τα στοιχεία του πίνακα ως γραμμικούς συνδυασμούς των στοιχείων αυτής της βάσης και λαμβάνοντας τους αντίστοιχους συντελεστές κατασκευάζουμε τον πίνακα:

$$\overline{\mathrm{H}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

που είναι ένας πίνακας ελέγχου ισοτιμίας του κώδικα Goppa $\mathcal{G}(L, g(x))$. Οι παράμετροι του κώδικα αυτού είναι $[8,\, 2,\, d]$.

Μπορείτε να υπολογίσετε την ελάχιστη απόσταση d;

Μπορείτε να υπολογίσετε τα στοιχεία του;

Διαπιστώστε ότι ο κώδικας αυτός δεν είναι κυκλικός.

2. Στην πρώτη από τις προηγούμενες παρατηρήσεις είχαμε δεί, θεωρώντας τους κώδικες Goppa ως εναλλακτικούς κώδικες γενικευμένων κωδίκων Reed-Solomon, ότι οι υπό στενή έννοια BCH κώδικες αποτελούν υποκατηγορία των κωδίκων Goppa. Στο παράδειγμα αυτό θα δούμε τους BCH κώδικες ως υποκατηγορία των κωδίκων Goppa, αλλά χρησιμοποιώντας τη μέθοδο, η οποία οδήγησε στον αρχικό ορισμό των κωδίκων Goppa.

Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία, n ένας φυσικός αριθμός με την ιδιότητα να διαιρεί τον $q^s - 1$ για κάποιον s θετικό ακέραιο και ο s να είναι ελάχιστος με αυτή την ιδιότητα. Έστω $\mathbb{K}$ μια επέκταση του σώματος $\mathbb{F}$ βαθμού s και α μια πρωταρχική n-οστη ρίζα της μονάδας στο σώμα $\mathbb{K}$. Σύμφωνα με τον ορισμό (σελίδα 306) ο, υπό την στενή έννοια, BCH κώδικας προσχεδιασμένης απόστασης $\delta \geq 2$ είναι ο:

$$\begin{aligned}\mathcal{BCH}(n,\,\delta,\,\alpha) = \{\, f(x) \in \mathbb{F}_{n-1}[x] \mid \alpha^i \text{ είναι ρίζα του } f(x) \\ \text{για όλα τα } 1 \leq i \leq \delta - 1 \,\} \\ = \{\, \mathbf{r} = r_0\, r_1 \cdots r_{n-1} \mid \text{το πολυώνυμο} \\ r_0 + r_1 x + \cdots + r_{n-1} x^{n-1} \in \mathbb{F}_{n-1}[x] \\ \text{έχει ως ρίζες τα } \alpha^i \text{ για όλα τα } 1 \leq i \leq \delta - 1 \,\}.\end{aligned}$$

Ας ξεκινήσουμε από την σχέση:

$$\begin{aligned}(x^n - 1) \sum_{i=0}^{n-1} \frac{r_i}{x - \alpha^{-i}} &= \sum_{i=0}^{n-1} r_i \sum_{j=0}^{n-1} x^j (\alpha^{-i})^{n-1-j} \\ &= \sum_{j=0}^{n-1} x^j \sum_{i=0}^{n-1} r_i (\alpha^{j+1})^i.\end{aligned}$$

Από την ιδιότητα των στοιχείων του κώδικα $\mathcal{BCH}(n,\,\delta,\,\alpha)$ έχουμε:

$$\sum_{i=0}^{n-1} r_i (\alpha^{j+1})^i = 0 \quad \text{για όλα τα } 0 \leq j \leq \delta - 2.$$

Επομένως το δεξιό μέρος της παραπάνω σχέσης είναι ένα πολυώνυμο με βαθμό ελαχίστου όρου τουλάχιστον ίσον με $\delta - 1$. Συνεπώς τελικά έχουμε:

$$(x^n - 1) \sum_{i=0}^{n-1} \frac{r_i}{x - \alpha^{-i}} \;=\; x^{\delta-1}\sigma(x), \quad \text{όπου } \sigma(x) \in \mathbb{K}[x].$$

Η τελευταία σχέση γράφεται:

$$\sum_{i=0}^{n-1} \frac{r_i}{x - \alpha^{-i}} \;=\; \frac{x^{\delta-1}\sigma(x)}{x^n - 1}.$$

Αυτό σημαίνει ότι το στοιχείο $\mathbf{r} = r_0\, r_1 \cdots r_{n-1} \in \mathcal{BCH}(n, \delta, \alpha)$ αν και μόνο αν: $\sum_{i=0}^{n-1} \frac{r_i}{x - \alpha^{-i}} = 0 \in \mathcal{R}_{x^{\delta-1}}[x]\}$.

Η τελευταία όμως σχέση αποτελεί τον (κλασικό) ορισμό ενός $\mathcal{G}(L, g(x))$ κώδικα Goppa, όπου $L = \{\alpha^i, i = 0, 1, 2, \ldots, n-1\}$ και $g(x) = x^{\delta-1}$.

Άρα αποδείξαμε ότι ένας, υπό την στενή έννοια, BCH κώδικας είναι ένας κώδικας Goppa.

Θα πρέπει να επισημάνουμε ότι στο παράδειγμα αυτό ταυτοποιούμε (ως συνήθως) τον δακτύλιο $\mathbb{F}_{n-1}[x]$ με τον δακτύλιο $\mathbb{F}[x]/\langle x^n - 1\rangle$, για τον λόγο αυτό 'αγνοούμε' τον παρανομαστή $x^n - 1$ στο κλάσμα:

$$\frac{x^{\delta-1}\sigma(x)}{x^n - 1}.$$

Στο Θεώρημα 5.4.2 είχαμε δεί ότι η ελάχιστη απόσταση d ενός κώδικα Goppa $\mathcal{G}(L, g(x))$ πληροί τη σχέση $d \geq deg(g(x)) + 1$. Δηλαδή ο αριθμός λαθών που διορθώνει ο κώδικας φράσεται (από κάτω) από μια συνάρτηση του βαθμού του πολυωνύμου $g(x)$. Στην περίπτωση των δυαδικών κωδίκων Goppa θα δούμε ότι αυτό το κάτω φράγμα μπορεί να βελτιωθεί.

Θεώρημα 5.4.5. *Έστω $\mathbb{K}$ μια επέκταση του $\mathbb{F} = \mathbb{Z}_2$ και $\mathcal{G}(L, g(x))$ ένας δυαδικός κώδικας Goppa. Αν $\overline{g}(x) \in \mathbb{K}[x]$ είναι το μικροτέρου βαθμού πολυώνυμο, το οποίο είναι τέλειο τετράγωνο και διαιρείται από το $g(x)$, τότε $\mathcal{G}(L, g(x)) = \mathcal{G}(L, \overline{g}(x))$. Δηλαδή η ελάχιστη απόσταση του κώδικα είναι τουλάχιστον ίση με $deg(\overline{g}(x)) + 1$.*

Απόδειξη. Έστω $L = \{a_1, a_2, \ldots, a_n\}$. Επιλέγουμε ένα στοιχείο $\mathbf{c} = c_1 c_2 \cdots c_n$ του κώδικα βάρους έστω w και υποθέτουμε ότι στις θέσεις $i_1, i_2, \ldots, i_w$ τα αντίστοιχα c_{i_j} είναι ίσα με 1, (ενώ στις υπόλοιπες θέσεις τα αντίστοιχα c_r ισούνται με μηδέν). Θεωρούμε το πολυώνυμο $f(x) = \prod_{j=1}^{w}(x - a_{i_j})$ και λαμβάνουμε την (τυπική) παράγωγό του $f'(x)$. Δεν είναι δύσκολο να δούμε ότι $f'(x) = \sum_{i=1}^{n} \frac{c_i}{x - a_i} \cdot f(x)$.

Τα πολυώνυμα $f(x)$ και $g(x)$ δεν έχουν κοινές ρίζες, επομένως είναι σχετικά πρώτα (γιατί;). Από τον (κλασικό) ορισμό του κώδικα Goppa έχουμε ότι $\sum_{i=1}^{n} \overline{\frac{c_i}{x - a_i}} = 0 \in \mathcal{R}_{g(x)}[x]$. Επομένως το $\mathbf{c} = c_1\, c_2 \cdots c_n \in \mathcal{G}(L, g(x))$ αν και

και μόνο αν το $g(x)$ διαιρεί το άθροισμα $\sum_{i=1}^{n} \frac{c_i}{x-a_i}$, αν και μόνο αν το $g(x)$ διαιρεί την παράγωγο $f'(x)$.

Γενικά ισχύει ότι η παράγωγος ενός πολυωνυμού με συντελεστές από ένα σώμα χαρακτηριστικής 2 είναι τέλειο τετράγωνο, δηλαδή $f'(x) = h(x^2) = (h(x))^2$ (γιατί;). Επομένως, αν $\overline{g}(x) \in \mathbb{K}[x]$ είναι το μικροτέρου βαθμού πολυώνυμο, το οποίο είναι τέλειο τετράγωνο και διαιρείται από το $g(x)$, τότε ισχύει ότι το πολυώνυμο $g(x)$ διαιρεί την παράγωγο $f'(x)$ αν και μόνο αν το πολυώνυμο $\overline{g}(x)$ διαιρεί την παράγωγο $f'(x)$ (γιατί;). Συνοψίζοντας έχουμε ότι το $\mathbf{c} = c_1\, c_2 \cdots c_n \in \mathcal{G}(L,\, g(x))$ αν και μόνο αν το $\overline{g}(x)$ διαιρεί την παράγωγο $f'(x)$, αν και μόνο αν το $\overline{g}(x)$ διαιρεί το άθροισμα $\sum_{i=1}^{n} \frac{c_i}{x-a_i}$, αν και μόνο αν το $\mathbf{c} = c_1\, c_2 \cdots c_n \in \mathcal{G}(L,\, \bar{g}(x))$. ό.έ.δ.

Πόρισμα 5.4.6. *Έστω $\mathbb{K}$ μια επέκταση του $\mathbb{F} = \mathbb{Z}_2$ και $\mathcal{G}(L,\, g(x))$ ένας δυαδικός κώδικας Goppa. Υποθέτουμε ότι το πολυώνυμο $g(x)$ δεν έχει πολλαπλές ρίζες. Τότε $\mathcal{G}(L,\, g(x)) = \mathcal{G}(L,\, (g(x))^2)$. Δηλαδή ο κώδικας $\mathcal{G}(L,\, g(x))$ διορθώνει τουλάχιστον τόσα λάθη όσος είναι ο βαθμός του πολυωνύμου $g(x)$.*

Απόδειξη. Επειδή το πολυώνυμο δεν έχει πολλαπλές ρίζες είναι εύκολο να δούμε ότι το μικροτέρου βαθμού πολυώνυμο, το οποίο είναι τέλειο τετράγωνο και διαιρείται από το $g(x)$ είναι το πολυώνυμο $(g(x))^2$. Οπότε το αποτέλεσμα έπεται από το προηγούμενο θεώρημα. ό.έ.δ.

Παραδείγματα 5.4.7.

1. Στο παράδειγμα 5.4.4$_1$ συναντήσαμε έναν κώδικα Goppa $\mathcal{G}(L,\, g(x))$, όπου $g(x) = x^2 + x + 1 \in \mathbb{K}[x]$ (το $\mathbb{K}$ είναι η επέκταση του $\mathbb{F} = \mathbb{Z}_2$ βαθμού 3) και είχαμε θέσει το ερώτημα ποια είναι η ελάχιστη απόστασή του, η οποία ικανοποιεί την σχέση $d \geq deg(g(x)) + 1 = 2 + 1$ (με το ενδεχόμενο να είναι ίση με 3). Το πολυώνυμο $g(x)$ δεν έχει πολλαπλές ρίζες, άρα, σύμφωνα με το προηγούμενο πόρισμα, έχουμε $\mathcal{G}(L,\, g(x)) = \mathcal{G}(L,\, (g(x))^2)$ και συνεπώς η ελάχιστη απόστασή του ικανοποιεί την σχέση $d \geq deg((g(x))^2) + 1 = 4 + 1$.

2. Έστω $\mathbb{F} = \mathbb{Z}_2$ και $\mathbb{K}$ η επέκταση του $\mathbb{F}$ βαθμού 3. Έστω α ένα πρωταρχικό στοιχείο του σώματος $\mathbb{K}$. Θέτουμε $L = \{\, 0,\, \alpha,\, \alpha^2,\, \alpha^3,\, \alpha^5,\, \alpha^6 \,\}$.

Έστω $g(x) = x^2 + 1 \in \mathbb{K}[x]$. Το πολυώνυμο αυτό δεν μηδενίζεται από κανένα στοιχείο του συνόλου L. Επιπλέον, επειδή η χαρακτηριστική του $\mathbb{K}$ ισούται με 2, έχουμε ότι $g(x) = (x+1)^2$. Σύμφωνα με το προηγούμενο πόρισμα έχουμε ότι $\mathcal{G}(L, g(x)) = \mathcal{G}(L, x+1)$.

Έστω $\mathcal{GRS}$ ο γενικευμένος κώδικας Reed-Solomon επί του σώματος $\mathbb{K}$ με πίνακα ελέγχου ισοτιμίας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} g(0)^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & g(\alpha)^{-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & g(\alpha^2)^{-1} & 0 & 0 & 0 \\ 0 & 0 & 0 & g(\alpha^3)^{-1} & 0 & 0 \\ 0 & 0 & 0 & 0 & g(\alpha^5)^{-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & g(\alpha^6)^{-1} \end{pmatrix} =$$
$$= \cdots = \begin{pmatrix} 1 & \alpha^4 & \alpha & \alpha^6 & \alpha^3 & \alpha^5 \end{pmatrix}.$$

Ο εναλλακτικός κώδικας $\mathcal{A} = \mathbb{F}^n \cap \mathcal{GRS}$ είναι ο κώδικας Goppa $\mathcal{G}(L, x+1)$.

Ο πίνακας H δεν είναι πίνακας ελέγχου ισοτιμίας του κώδικα Goppa $\mathcal{G}(L, x+1)$. Ένας πίνακας ελέγχου ισοτιμίας για τον κώδικα $\mathcal{G}(L, x+1)$ υπολογίζεται (πλέον) κατά τα γνωστά και έχουμε τον πίνακα:

$$\overline{H} = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

που είναι ένας πίνακας ελέγχου ισοτιμίας του κώδικα Goppa $\mathcal{G}(L, x+1)$. Οι παράμετροι του κώδικα αυτού είναι $[6, 3, 3]$.

Μπορείτε να υπολογίσετε τα στοιχεία του; Είναι ο κώδικας αυτός κυκλικός;

5.4.1 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;* αυτής της παραγράφου.

2. Έστω $\mathbb{K}$ μια επέκταση του $\mathbb{Z}_2$ βαθμού 4 και $g(x) = x^2 + 1 \in \mathbb{K}[x]$. Έστω $L \subseteq \mathbb{K}$ να είναι το σύνολο όλων των 15-οστών πρωταρχικών ριζών της μονάδας. Να μελετήσετε τον κώδικα Goppa $\mathcal{G}(L, g(x))$.

3. Έστω $\mathbb{F}$ μια επέκταση του $\mathbb{Z}_2$ βαθμού t και $g(x) \in \mathbb{F}[x]$ βαθμού r χωρίς πολλαπλές ρίζες. Έστω $\mathbb{E}$ το σώμα ριζών του $g(x)$ βαθμού επέκτασης (επί του $\mathbb{Z}_2$) s. Έστω m θετικός ακέραιος με τις ιδιότητες $\mu\kappa\delta(s, m) = 1$ και ο t να διαιρεί τον m. Λαμβάνουμε ως $L = \mathbb{K}$, όπου $\mathbb{K}$ είναι μια επέκταση του $\mathbb{Z}_2$ βαθμού m. Να μελετήσετε τον κώδικα Goppa $\mathcal{G}(L, g(x))$.

4. Έστω $\mathbb{K}$ μια επέκταση του $\mathbb{Z}_2$ βαθμού m, όπου το 3 δεν διαιρεί τον m και $g(x) = x^3 + x + 1 \in \mathbb{K}[x]$. Έστω $L = \mathbb{K}$. Να μελετήσετε τον κώδικα Goppa $\mathcal{G}(L, g(x))$.

5. Έστω $\mathcal{C}$ ο δυαδικός κυκλικός κώδικας μήκους 15 με πολυώνυμο γεννήτορα $\gamma(x) = x^2 + x + 1$ και ω μια 15^η πρωταρχική ρίζα της μονάδας. Δείξτε ότι:

   i) Ο κώδικας $\mathcal{C}$ είναι ένας BCH κώδικας με προσχεδιασμένη απόσταση $\delta = 2$.

   ii) Ο κώδικας $\mathcal{C}$ δεν είναι ένας κώδικας Goppa.

   (Κατά συνέπεια **δεν** είναι υπο την στενή έννοια BCH κώδικας).

6. Να υπολογίσετε την ελάχιστη απόσταση ενός δυαδικού κώδικα Goppa $\mathcal{G}(L, g(x))$, όπου $g(x) = x^2 + 1$, $L = \{0, z, z^2\}$ και $z \neq 1$ είναι ένα στοιχείο ενός σώματος με τέσσερα στοιχεία.

7. Να υπολογίσετε έναν πίνακα ελέγχου ισοτιμίας ενός δυαδικού κώδικα Goppa $\mathcal{G}(L, g(x))$, όπου $g(x) = x^2 + x + \alpha^3$ και L είναι το σώμα με 16 το πλήθος στοιχεία, του οποίου πρωταρχικό στοιχείο είναι το α.

Βιβλιογραφία

Berlekamp, E. R. *"Algebraic Coding Theory"*. Laguna Hills, CA: Aegean Park Press, 1984.

Hall, J.I. *Notes on Coding Theory*. (σε ηλεκτρονική μορφή). www.math.msu.edu/~jhall.

Herstein, I. N. *"Abstract Algebra"*. New York: Macmillan, 1990.

Huffman, C. W. and Pless, V. . *"Fundamentals of Error-Correcting Codes"*. Cambridge University Press, 2003.

McEliece, R. J. *"Finite Fields for Computer Scientists and Engineers"*. Boston: Kluwer Academic Publishers, 1987.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*. Wiley, New York, 1998.

Roman, S. *"Coding and Information Theory"*. Springer-Verlag, 1992.

Ron M. Roth. *"Introduction to Coding Theory"*. Cambridge University Press, 2006.

van Lint, J.H. *"Introduction to Coding Theory"*. Springer-Verlag, 1999.

Vermani, L. *"Elements of Algebraic Coding Theory"*. Chapman and Hall, London, 1996.

Walker, J. L. *"Codes and Curves"*, volume 7 of *Student Mathematical Library*. AMS, 2000.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

ΚΕΦΑΛΑΙΟ 6

Κώδικες και συνδυαστικές κατασκευές

Η Συνδυαστική είναι ένας ευρύς, εντυπωσιακός και ενεργός κλάδος των Μαθηματικών με πολλές, τόσο θεωρητικές, όσο και πρακτικές εφαρμογές. Στο κεφάλαιο αυτό απλώς θα αναφέρουμε ορισμένες έννοιες από τη Συνδυαστική, οι οποίες έχουν άμεση σχέση με τη Θεωρία Κωδίκων. Για τον ενδιαφερόμενο αναγνώστη παραπέμπουμε στα vanLint, J.H. and Wilson, R.M [2001] και Anderson, I. [2000].

6.1 Σχεδιασμοί και Κώδικες

Η διευθέτηση των στοιχείων ενός συνόλου σε υποσύνολα, σύμφωνα με ορισμένες *απαιτήσεις* αποτελεί ένα ενδιαφέρον πρόβλημα της Συνδυαστικής με πλείστες όσες εφαρμογές. Ανάλογα με τις απαιτήσεις η πολυπλοκότητα του προβλήματος ποικίλει.

Ας γίνουμε πιο σαφείς ως προς το περιεχόμενο της λέξης *απαιτήσεις* στην ειδική περίπτωση των *Στρατηγικών Σχηματισμών*.

Ορισμοί 6.1.1. *1. Έστω S ένα σύνολο με v το πλήθος στοιχεία. Ένας* ***Στρατηγικός Σχηματισμός*** *(επί του συνόλου S) είναι μια οικογένεια*

αποτελούμενη από b το πλήθος υποσύνολα (τμήματα),[1] *κάθε ένα από τα οποία περιέχει k ($k < v$) το πλήθος στοιχεία, έτσι ώστε κάθε στοιχείο του συνόλου S να ανήκει σε ακριβώς r το πλήθος από αυτά τα υποσύνολα.*

2. *Ένας στρατηγικός σχηματισμός με την επιπλέον απαίτηση κάθε (μη διατεταγμένο) ζεύγος στοιχείων του συνόλου S να εμφανίζεται σε ακριβώς λ το πλήθος υποσύνολα θα ονομάζεται* ***Ισορροπημένος μη Πλήρης***, ***κατά τμήματα***, ***Σχεδιασμός*** *ή απλά σχεδιασμός.*[2]

Παραστατικά θα μπορούσαμε να πούμε ότι ένας σχεδιασμός είναι μια συλλογή από b το πλήθος *επιτροπές*, τα μέλη των οποίων επιλέγονται από ένα σύνολο S με v το πλήθος άτομα. Κάθε επιτροπή έχει k το πλήθος μέλη. Κάθε άτομο μετέχει σε r το πλήθος επιτροπές και κάθε ζεύγος ατόμων μετέχει σε λ το πλήθος επιτροπές.

Όπως βλέπουμε από τους προηγούμενους ορισμούς ένας σχεδιασμός επί ενός συνόλου S δεν εξαρτάται από τη φύση των στοιχείων του συνόλου, αλλά από το πλήθος v των στοιχείων του και από τις υπόλοιπες παραμέτρους b, r, k, λ. Για τον λόγο αυτό, στο εξής ένας σχεδιασμός θα συμβολίζεται ως (v, b, r, k, λ)-σχεδιασμός.

Παράδειγμα 6.1.2. Έστω $S = \{1, 2, 3, 4, 5, 6, 7\}$. Θεωρούμε τα υποσύνολα $B_1 = \{1, 2, 3\}$, $B_2 = \{3, 4, 5\}$, $B_3 = \{1, 5, 6\}$, $B_4 = \{1, 4, 7\}$, $B_5 = \{3, 6, 7\}$, $B_6 = \{2, 5, 7\}$, $B_7 = \{2, 4, 6\}$. Κάθε στοιχείο του συνόλου S εμφανίζεται σε τρία από τα υποσύνολα αυτά και κάθε ζεύγος στοιχείων εμφανίζεται σε ακριβώς ένα από τα υποσύνολα. Δηλαδή έχουμε έναν $(7, 7, 3, 3, 1)$-σχεδιασμό.

Στην περίπτωση όπου $b = v$, ο σχεδιασμός καλείται **συμμετρικός**. Εδώ θα θέλαμε να επισημάνουμε ότι στον ορισμό η λέξη *ισορροπημένος* αναφέρεται στο γεγονός ότι κάθε ζεύγος στοιχείων του συνόλου εμφανίζεται στον ίδιο αριθμό υποσυνόλων, ενώ η λέξη *μη πλήρης* δηλώνει ότι κάθε υποσύνολο περιέχει λιγότερα από v το πλήθος στοιχεία. Στην ακραία περίπτωση όπου

[1] Τα υποσύνολα αυτά στην ξενόγλωσση βιβλιογραφία ονομάζονται **blocks**.

[2] Στην ξενόγλωσση βιβλιογραφία έχουμε την ονομασία Balanced Incomplete Block Design.

$v = k$, τότε έχουμε την περίπτωση ενός πλήρους (v, b, b, v, b)-σχεδιασμού, όπου όλα τα σύνολα (τμήματα) της οικογένειας που σχηματίζουν τον σχεδιασμό συμπίπτουν με το σύνολο S.

Πρόταση 6.1.3. *Μεταξύ των πέντε παραμέτρων v, b, r, k, λ ενός σχεδιασμού ισχύουν οι σχέσεις.*

i) $vr = bk$.

ii) $r(k-1) = \lambda(v-1)$.

Απόδειξη. i) Κάθε ένα από τα b το πλήθος υποσύνολα του σχεδιασμού περιέχει k το πλήθος στοιχεία, δηλαδή στην *ανάπτυξη* του σχεδιασμού εμφανίζονται τελικά bk το πλήθος στοιχεία. Αλλά κάθε ένα από τα v το πλήθος διακεκριμένα στοιχεία του συνόλου S εμφανίζεται ακριβώς σε r το πλήθος υποσύνολα. Επομένως, έχουμε $vr = bk$.

ii) Έστω a ένα στοιχείο του συνόλου S. Το στοιχείο αυτό εμφανίζεται σε r το πλήθος υποσύνολα που το καθένα από αυτά περιέχει k το πλήθος στοιχεία, δηλαδή με το στοιχείο a σχηματίζονται $r(k-1)$ το πλήθος ζεύγη. Όμως το στοιχείο a μπορεί να σχηματίσει, με τα υπόλοιπα στοιχεία του συνόλου S, $v-1$ το πλήθος ζεύγη, τα οποία εμφανίζονται σε λ το πλήθος υποσύνολα. Άρα $r(k-1) = \lambda(v-1)$. ό.έ.δ.

Από την προηγούμενη πρόταση έπεται ότι σε έναν σχεδιασμό, αν δωθούν τρείς, οποιεσδήποτε, από τις πέντε παραμέτρους, τότε εύκολα μπορούν να υπολογισθούν οι άλλες δύο. Για τον λόγο αυτόν, ορισμένες φορές, ένας (v, b, r, k, λ)-σχεδιασμός αναφέρεται ως (v, k, λ)-σχεδιασμός.

Οι αναγκαίες συνθήκες, που αναφέρονται στην προηγούμενη πρόταση για τις παραμέτρους ενός σχεδιασμού, δεν είναι ικανές για την ύπαρξη ενός σχεδιασμού με τις παραμέτρους αυτές. Για παράδειγμα, είναι ανοικτό το πρόβλημα αν υπάρχει $(22, 33, 12, 8, 4)$-σχεδιασμός.

Έστω ένας (v, b, r, k, λ)-σχεδιασμός επί του συνόλου $S = \{1, 2, \dots, v\}$ και $B_1, B_2, \dots, B_b$ τα υποσύνολα του S που απαρτίζουν τον σχεδιασμό. Στον σχεδιασμό αυτόν προσάπτουμε έναν $v \times b$ πίνακα $\mathrm{G} = (\gamma_{ij})$ με $\gamma_{ij} = \begin{cases} 1 & \text{αν } i \in B_j \\ 0 & \text{αν } i \notin B_j \end{cases}$. Δηλαδή κάθε γραμμή αντιστοιχεί σε ένα στοιχείο του συνό-

λου S και κάθε στήλη σε ένα από τα υποσύνολα που απαρτίζουν τον σχεδιασμό. Ο πίνακας G ονομάζεται **προσαπτόμενος** πίνακας του σχεδιασμού.

Παρατήρηση 6.1.4. Πρέπει να σημειωθεί ότι, σε μέρος της σχετικής βιβλιογραφίας, ως προσαπτόμενος πίνακας ενός σχεδιασμού θεωρείται ο ανάστροφος πίνακας του πίνακα G.

Παράδειγμα 6.1.5. Ο προσαπτόμενος πίνακας του σχεδιασμού του προηγουμένου παραδείγματος είναι ο:

$$\mathrm{G} = \begin{array}{c|ccccccc} & B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \\ \hline 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 3 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 5 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 7 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array} .$$

Εδώ πρέπει να παρατηρήρουμε ότι ο προσαπτόμενος πίνακας εξαρτάται τόσο από τη διάταξη των στοιχείων του συνόλου S, όσο και από τη σειρά με την οποία διατάσσουμε τα υποσύνολα B_i. Μια αναδιάταξη των στοιχείων του συνόλου S επιφέρει αναδιάταξη των γραμμών του πίνακα, ενώ διαφορετική απαρίθμηση των συνόλων B_i επιφέρει αναδιάταξη των στηλών του πίνακα, δηλαδή πρόκειται για ισοδυνάμους πίνακες.

Πρόταση 6.1.6. *Για τον προσαπτόμενο πίνακα* G *ενός* (v, b, r, k, λ)*-σχεδιασμού ισχύουν οι παρακάτω ιδιότητες:*

1. $\mathrm{GG}^t = (r-\lambda)\mathrm{I}_v + \lambda \mathrm{J}_{v\,v}$.
2. $\det(\mathrm{GG}^t) = [r + (v-1)\cdot\lambda]\cdot(r-\lambda)^{v-1}$.
3. $\mathrm{GJ}_{b\,b} = r\mathrm{J}_{v\,b}$.
4. $\mathrm{J}_{v\,v}\mathrm{G} = k\mathrm{J}_{v\,b}$.

Όπου με I_n *συμβολίζουμε τον* $n \times n$ *ταυτοτικό πίνακα και με* $\mathrm{J}_{m\,n}$ *τον* $m \times n$ *πίνακα, όπου όλα τα στοιχεία του είναι ίσα με 1.*

Απόδειξη. Για την απόδειξη της πρώτης ιδιότητας αρκεί να παρατηρήσουμε ότι στην i γραμμή το 1 εμφανίζεται στην j στήλη, αν και μόνο αν το i στοιχείο ανήκει στο B_j υποσύνολο. Επομένως, στο γινόμενο $\mathrm{GG}^t = (\sigma_{i\,j})$, επειδή κάθε γραμμή περιέχει r το πλήθος 1, έχουμε $\sigma_{i\,i} = r$ για κάθε $i = 1, 2, \ldots, v$. Στην περίπτωση του πολλαπλασιασμού της i γραμμής του πίνακα G με την j στήλη του πίνακα G^t (δηλαδή της j γραμμής του πίνακα G), για $i \neq j$, έχουμε αποτέλεσμα ίσον με το πλήθος των υποσυνόλων στα οποία και τα δύο στοιχεία i και j εμφανίζονται (γιατί;), το οποίο από τον ορισμό του σχεδιασμού ισούται με λ, δηλαδή $\sigma_{i\,j} = \lambda$ για $i \neq j$. Άρα, ο πίνακας GG^t είναι της μορφής:

$$\mathrm{GG}^t = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{pmatrix}.$$

Από την παραπάνω μορφή του πίνακα GG^t εύκολα προκύπτει ότι:

$$\mathrm{GG}^t = (r - \lambda)\mathrm{I}_v + \lambda \mathrm{J}_{v\,v}.$$

Επίσης, από αυτή τη μορφή του πίνακα εύκολα μπορούμε, με στοιχειώδεις πράξεις επί των στηλών του και των γραμμών του, να υπολογίσουμε την ορίζουσά του και να δούμε ότι πράγματι ισχύει η δεύτερη ιδιότητα.

Η τρίτη και τέταρτη ιδιότητα απλώς δηλώνουν ότι σε κάθε γραμμή του πίνακα G εμφανίζονται r το πλήθος 1 και σε κάθε στήλη k το πλήθος 1. ό.έ.δ.

Ως εφαρμογή της προηγούμενης πρότασης έχουμε το εξής, αναμενόμενο, αλλά όχι τόσο προφανές, αποτέλεσμα.

Πόρισμα 6.1.7. *Σε έναν (v, b, r, k, λ)-σχεδιασμό, επί ενός συνολού S, το πλήθος των υποσυνόλων είναι μεγαλύτερο ή ίσον από το πλήθος των στοιχείων του συνόλου S ($b \geq v$).*

Απόδειξη. Πράγματι, επειδή $r > \lambda$, έχουμε ότι ο πίνακας GG^t είναι αντιστρέψιμος, άρα $b \geq rank(\mathrm{G}) \geq rank(\mathrm{GG}^t) = v$. ό.έ.δ.

Στην περίπτωση ενός συμμετρικού (v, b, r, k, λ)-σχεδιασμού ($b = v$ και $k = r$), από την προηγούμενη πρόταση έπεται ότι $\det(\mathrm{G}\mathrm{G}^t) = [r + (v-1)\cdot\lambda]\cdot(r-\lambda)^{v-1} = [k + (v-1)\cdot\lambda]\cdot(k-\lambda)^{v-1}$, αλλά από την Πρόταση 6.1.3 έχουμε ότι $r(k-1) = \lambda(v-1)$. Οπότε, συνεχίζοντας στην προηγούμενη σχέση, έχουμε τελικά $\det(\mathrm{G}\mathrm{G}^t) = k^2\cdot(k-\lambda)^{v-1}$, απ' όπου έχουμε ότι $\det \mathrm{G} = \pm k\cdot(k-\lambda)^{(v-1)/2}$. Συνεπώς, επειδή η ορίζουσα του πίνακα G είναι ακέραιος αριθμός, έχουμε ότι, στην περίπτωση όπου ο v είναι άρτιος, η διαφορά $k-\lambda$ είναι αναγκαστικά τέλειο τετράγωνο.

Ερώτημα: Τι μπορούμε να πούμε αν ο v είναι περιττός;

Απάντηση: (Χωρίς απόδειξη) Στην περίπτωση αυτή η διοφαντική εξίσωση $x^2 = (k-\lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2$ έχει μη μηδενική ακεραία λύση.

Έστω ένας (v, b, r, k, λ)-σχεδιασμός, επί ενός συνόλου S με προσαπτόμενο πίνακα G. Το **συμπλήρωμα** του πίνακα G είναι ο πίνακας $\overline{\mathrm{G}}$, ο οποίος προέρχεται από τον πίνακα G τοποθετώντας στις θέσεις, όπου εμφανίζεται 1, το μηδέν και στις θέσεις, όπου εμφανίζεται μηδέν, το 1.

Μπορούμε να δείξουμε ότι ο πίνακας $\overline{\mathrm{G}}$ είναι ο προσαπτόμενος πίνακας ενός άλλου σχεδιασμού επί του συνόλου S. Πράγματι, κάθε γραμμή του $\overline{\mathrm{G}}$ έχει $b-r$ το πλήθος 1 και κάθε στήλη έχει $v-k$ το πλήθος 1. Αυτό υποδεικνύει ότι στον νέο σχεδιασμό θα έχουμε $\overline{r} = b-r$ και $\overline{k} = v-k$. Επιπλέον, επειδή δύο διαφορετικές γραμμές του πίνακα G έχουν το 1 σε ακριβώς λ το πλήθος κοινές θέσεις, κάθε μία έχει $r-\lambda$ το πλήθος 1 στις υπόλοιπες $b-\lambda$ θέσεις, όπου όμως αναγκαστικά στις αντίστοιχες θέσεις της άλλης γραμμής θα υπάρχουν μηδενικά, οπότε, συμμετρικά, σε $2(r-\lambda)$ το πλήθος θέσεις οι δύο γραμμές διαφέρουν. Δηλαδή έχουν κοινά σημεία σε $b-2(r-\lambda)$ το πλήθος θέσεις, εκ των οποίων σε λ το πλήθος θέσεις έχουν από κοινού 1 και στις υπόλοιπες $b-2(r-\lambda)-\lambda = b-2r+\lambda$ το πλήθος θέσεις έχουν από κοινού μηδέν. Συνεπώς, στον συμπληρωματικό πίνακα $\overline{\mathrm{G}}$ υπάρχουν $\overline{\lambda} = b-2r+\lambda$ το πλήθος γραμμές, οι οποίες έχουν από κοινού 1. Άρα, ο πίνακας $\overline{\mathrm{G}}$ είναι ο προσαπτόμενος πίνακας του (συμπληρωματικού) $(v, b, b-r, v-k, b-2r+\lambda)$-σχεδιασμού.

Η μελέτη των σχεδιασμών εκτείνεται πέραν των σκοπών του συγκεκριμένου βιβλίου. Εμείς εδώ παραθέτουμε τα ελάχιστα αναγκαία στοιχεία για να

δούμε την σύνδεσή τους με τους κώδικες.

Παράδειγμα 6.1.8. Στο Παράδειγμα 6.1.2 είχαμε δει έναν σχεδιασμό και στο Παράδειγμα 6.1.5 τον προσαπτόμενο πίνακά του. Κατασκευάζουμε έναν δυαδικό κώδικα ως εξής:

Ως (κωδικο)λέξεις λαμβάνουμε τις γραμμές τόσο του πίνακα G στο Παράδειγμα 6.1.5, όσο και τις γραμμές του συμπληρώματός του. Επιπλέον, ως στοιχεία του θεωρούμε και τις λέξεις $\mathbf{0} = 0000000$ και $\mathbf{1} = 1111111$. Δηλαδή έχουμε τον $(7, 16, d)$ κώδικα $\mathcal{C}$ με στοιχεία τα:

$$
\begin{array}{lcccccccc}
\mathbf{0} & = & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mathbf{1} & = & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\mathbf{a_1} & = & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
\mathbf{a_2} & = & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
\mathbf{a_3} & = & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
\mathbf{a_4} & = & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
\mathbf{a_5} & = & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
\mathbf{a_6} & = & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
\mathbf{a_7} & = & 0 & 0 & 0 & 1 & 1 & 1 & 0
\end{array}
\qquad
\begin{array}{lcccccccc}
\mathbf{b_1} & = & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
\mathbf{b_2} & = & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
\mathbf{b_3} & = & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
\mathbf{b_4} & = & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\
\mathbf{b_5} & = & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
\mathbf{b_6} & = & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
\mathbf{b_7} & = & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{array}
$$

Είναι εύκολο να δούμε ότι ο κώδικας αυτός είναι γραμμικός. Θα υπολογίσουμε την ελάχιστη απόσταση του κώδικα. Από τον ορισμό του σχεδιασμού έχουμε ότι σε κάθε γραμμή του πίνακα G το 1 εμφανίζεται σε ακριβώς τρεις θέσεις και κάθε δύο διαφορετικές γραμμές έχουν το 1 σε μόνο μια κοινή θέση, άρα $w(a_i) = 3$ για κάθε i και συνεπώς $d(a_i, a_j) = w(a_i)+w(a_j)-2w(a_i \cap a_j) = 4$ για $i \neq j$ (ιδέ την Πρόταση 1.2.11).

Με το ίδιο σκεπτικό για τον σχεδιασμό που ορίζει ο πίνακας $\overline{\mathrm{G}}$ έχουμε ότι $d(b_i, b_j) = 4$ για $i \neq j$. (Εναλλακτικά, η απόσταση μεταξύ δύο (κωδικο)λέξεων παραμένει αμετάβλητη, αν και στις δύο όλα τα 1 μετατραπούν σε 0 και όλα τα 0 μετατραπούν σε 1.)

Προφανώς $d(a_i, b_i) = 7$ για κάθε i.

Για $i \neq j$ οι (κωδικο)λέξεις a_i, b_j διαφέρουν ακριβώς σε τόσες θέσεις, όσες είναι οι θέσεις στις οποίες οι (κωδικο)λέξεις a_i, a_j συμφωνούν, δηλαδή:

$$d(a_i, b_j) = 7 - d(a_i, a_j) = 7 - 4 = 3.$$

Προφανώς έχουμε $d(\mathbf{0}, \mathbf{c}) \geq 3$ και $d(\mathbf{1}, \mathbf{c}) \geq 3$ για κάθε άλλη (κωδικο)λέξη $\mathbf{c} \in \mathcal{C}$. Επομένως, η ελάχιστη απόσταση του κώδικα $\mathcal{C}$ είναι ίση με 3.

Από την Πρόταση 1.5.12 εύκολα βλέπουμε ότι ο κώδικας αυτός είναι ένας τέλειος κώδικας και συνεπώς $A_2(7, 3) = 16$ (ιδέ τον Πίνακα 1.2 στην σελίδα 63).

Παρατήρηση 6.1.9. Ο κώδικας που κατασκευάσαμε προηγουμένως, με την βοήθεια της έννοιας του σχεδιασμού, είναι ο $\mathcal{H}(3, 2)$ κώδικας Hamming (ιδέ την Παράγραφο 4.1.3).

Για να δούμε την περαιτέρω σχέση μεταξύ των σχεδιασμών και των κωδίκων, θα δώσουμε έναν γενικότερο ορισμό από τον Ορισμό 6.1.1.

Ορισμός 6.1.10. *Έστω S ένα σύνολο με v το πλήθος στοιχεία και t ένας θετικός ακέραιος. Ένας $t-(v, b, r, k, \lambda)$-σχεδιασμός (επί του συνόλου S) είναι μια οικογένεια αποτελούμενη από b το πλήθος υποσύνολα (τμήματα), κάθε ένα από τα οποία περιέχει k ($k < v$) το πλήθος στοιχεία, κάθε ένα από τα στοιχεία του συνόλου S ανήκει σε ακριβώς r το πλήθος υποσύνολα (τμήματα) και, επιπλέον, κάθε υποσύνολο του συνόλου S με t το πλήθος στοιχεία περιέχεται σε ακριβώς λ το πλήθος από τα υποσύνολα (τμήματα). Προφανώς, για να υπάρχει μια τέτοια δυνατότητα, υποτίθεται ότι $0 < t < k < v$.*

Αμέσως βλέπουμε ότι ένας (v, b, r, k, λ)-σχεδιασμός, σύμφωνα με τον αμέσως προηγούμενο ορισμό, είναι ένας $2-(v, b, r, k, \lambda)$-σχεδιασμός.

Όπως και προηγουμένως, ένας $t-(v, b, r, k, \lambda)$-σχεδιασμός αναφέρεται και ως $t-(v, k, \lambda)$-σχεδιασμός.

Στην ειδική περίπτωση, όπου $\lambda = 1$, δηλαδή κάθε υποσύνολο του συνόλου S με t το πλήθος στοιχεία περιέχεται σε ακριβώς ένα υποσύνολο (τμήμα), ο $t-(v, b, r, k, 1)$-σχεδιασμός ονομάζεται σχεδιασμός **Steiner** και συμβολίζεται με $S(t, k, v)$.

Παρατήρηση 6.1.11. Ένας $2-(v, v, r, k, 1)$-σχεδιασμός είναι το **προβολικό επίπεδο** τάξης $n = k - 1$.[3] Από την Πρόταση 6.1.3 έπεται άμεσα ότι ένα

[3] Η μελέτη Πεπερασμένων Γεωμετριών είναι πέραν του σκοπού μας. Εδώ απλώς αναφέρουμε τη σχέση τους με τους σχεδιασμούς.

προβολικό επίπεδο τάξης n είναι ένας $S(2, n+1, n^2+n+1)$ σχεδιασμός Steiner.

Το Παράδειγμα 6.1.2 αποτελεί το *κλασσικό* παράδειγμα προβολικού επιπέδου τάξης 2 αποτελούμενο από επτά σημεία και επτά γραμμές.

Πρόταση 6.1.12. *Μεταξύ των πέντε παραμέτρων v, b, r, k και λ ενός t-σχεδιασμού ισχύουν οι παρακάτω σχέσεις.*

i) $vr = bk$.

ii) $r\binom{k-1}{t-1} = \lambda\binom{v-1}{t-1}$.

iii) $b\binom{k}{t} = \lambda\binom{v}{t}$.

Απόδειξη. Η Πρόταση αυτή αποτελεί γενίκευση της Πρότασης 6.1.3 και η ιδέα της απόδειξης είναι η ίδια, με τις τεχνικές λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Θα μπορούσαμε να δούμε την προηγούμενη πρόταση και ως πόρισμα του επομένου Θεωρήματος.

Θεώρημα 6.1.13. *Έστω ένας $t-(v, k, \lambda)$-σχεδιασμός (επί του συνόλου S). Το σύνολο S επιδέχεται έναν $s-(v, k, \lambda_s)$-σχεδιασμό για κάθε $s \leq t$.*

Απόδειξη. Έστω $s \leq t$ και A ένα υποσύνολο του συνόλου S με s το πλήθος στοιχεία. Υποθέτουμε ότι το σύνολο A περιέχεται, ως υποσύνολο, σε λ_s το πλήθος υποσύνολα (τμήματα) του δοθέντος $t-(v, k, \lambda)$-σχεδιασμού. Θα δείξουμε ότι το λ_s δεν εξαρτάται από το σύνολο A (παρά μόνο από το s, το πλήθος των στοιχείων του).

Ας υπολογίσουμε, με δύο τρόπους, το πλήθος των ζευγών (D, B), όπου B είναι ένα υποσύνολο (τμήμα) και D ένα υποσύνολο με t το πλήθος στοιχεία με την ιδιότητα $A \subset D \subset B$.

Υπάρχουν $\binom{v-s}{t-s}$ το πλήθος επιλογές για το υποσύνολο D (γιατί;) και κάθε τέτοιο υποσύνολο, από τον ορισμό του σχεδιασμού περιέχεται σε ακριβώς λ το πλήθος υποσύνολα (τμήματα), δηλαδή υπάρχουν $\lambda\binom{v-s}{t-s}$ ο πλήθος ζεύγη με την παραπάνω ιδιότητα.

Διαφορετικά, για κάθε ένα από τα λ_s το πλήθος υποσύνολα (τμήματα) B που περιέχουν το υποσύνολο A υπάρχουν $\binom{k-s}{t-s}$ το πλήθος δυνατοί τρόποι να

επιλέξουμε ένα υποσύνολο D με την ιδιότητα $A \subset D \subset B$, δηλαδή υπάρχουν $\lambda_s\binom{k-s}{t-s}$ ο πλήθος ζεύγη με την παραπάνω ιδιότητα.

Από τα ανωτέρω έχουμε αφενός μεν $\lambda\binom{v-s}{t-s} = \lambda_s\binom{k-s}{t-s}$, αφετέρου δε το πλήθος λ_s είναι ανεξάρτητο από την επιλογή του συνόλου A.

Συνεπώς, το σύνολο S επιδέχεται έναν $s-(v,\,k,\,\lambda_s)$-σχεδιασμό, όπου το λ_s υπολογίζεται από την προηγουμένη σχέση. ό.έ.δ.

Παρατηρήσεις 6.1.14.

1. Στο προηγούμενο θεώρημα θα πρέπει να παρατηρήρουμε ότι, για $s \leq t$, από τις πέντε παραμέτρους του $t-(v,b,r,k,\lambda)$-σχεδιασμού στον νέο $s-(v,b,r,k,\lambda_s)$-σχεδιασμό μόνο η παράμετρος λ_s είναι διαφορετική.

2. Αναγκαία συνθήκη για την ύπαρξη ενός $t-(v,\,k,\,\lambda)$-σχεδιασμού είναι οι αριθμοί $\lambda\binom{v-s}{t-s}/\binom{k-s}{t-s}$ να είναι ακέραιοι για όλα τα $0 \leq s \leq t$.

   Η ανωτέρω αναγκαία συνθήκη δεν είναι πάντοτε ικανή για την ύπαρξη ενός $t-(v,\,k,\,\lambda)$-σχεδιασμού. Παρόλα ταύτα στην ειδική περίπτωση των $S(2,\,3,\,v)$, $S(2,\,4,\,v)$, $S(2,\,5,\,v)$ και $S(3,\,4,\,v)$ σχεδιασμών Steiner έχει αποδειχθεί ότι είναι και ικανή. (Προσπαθήστε να το αποδείξετε, τουλάχιστον στην περίπτωση $S(2,\,3,\,v)$).

3. Συνδυάζοντας τις σχέσεις $b\binom{k}{t} = \lambda\binom{v}{t}$ και $\lambda\binom{v-s}{t-s} = \lambda_s\binom{k-s}{t-s}$, *επαναποδεικνύουμε* την γνωστή συνδυαστική σχέση:

$$\binom{v}{t}\binom{k}{s}\binom{k-s}{t-s} = \binom{v}{s}\binom{k}{t}\binom{v-s}{t-s}.$$

Όπως στην περίπτωση ενός $2-(v,\,k,\,\lambda)$-σχεδιασμού έτσι και στην περίπτωση ενός $t-(v,\,k,\,\lambda)$-σχεδιασμού, $t \geq 2$, μπορούμε να ορίσουμε την έννοια του προσαπτόμενου πίνακα (ιδέ σελίδα 355), μάλιστα δε ισχύει η αντίστοιχη με την Πρόταση 6.1.6.

Πρόταση 6.1.15. *Για τον προσαπτόμενο πίνακα* G *ενός* $t-(v,\,b,\,r,\,k,\,\lambda)$*-σχεδιασμού ισχύουν οι παρακάτω ιδιότητες:*

1. $\mathrm{G}\mathrm{G}^t = (r-\lambda_2)\mathrm{I}_v + \lambda_2 \mathrm{J}_{v\,v}$.

2. $\det(\mathrm{G}\mathrm{G}^t) = [r+(v-1)\cdot\lambda_2]\cdot(r-\lambda_2)^{v-1}$.

3. $\mathrm{GJ}_{b\,b} = r\mathrm{J}_{v\,b}$.

4. $\mathrm{J}_{v\,v}\mathrm{G} = k\mathrm{J}_{v\,b}$.

Όπου με I_n *συμβολίζουμε τον* $n \times n$ *ταυτοτικό πίνακα και με* $\mathrm{J}_{m\,n}$ *τον* $m \times n$ *πίνακα, όπου όλα τα στοιχεία του είναι ίσα με 1.*

Απόδειξη. Η απόδειξη είναι παρόμοια με την απόδειξη της Πρότασης 6.1.6. Αρκεί να παρατηρήσουμε ότι για τον υπολογισμό του γινομένου GG^t πρέπει να λάβουμε υπόψη την σχέση $\lambda\binom{v-s}{t-s} = \lambda_s\binom{k-s}{t-s}$ του Θεωρήματος 6.1.13 για $s = 2$. ό.έ.δ.

Παράδειγμα 6.1.16. Έστω $S(t,\, k,\, v)$ ένας σχεδιασμός Steiner με προσαπτόμενο πίνακα G. Οι γραμμές του αναστόφου πίνακα G^t αντιστοιχούν στα υποσύνολα (τμήματα) του σχεδιασμού. Το σύνολο αυτών των γραμμών αποτελεί τις (κωδικο)λέξεις ενός κώδικα $\mathcal{C}$ με παραμέτρους $(\, n = v,\, M = b = \binom{v}{t}/\binom{k}{t},\, d \geq 2(k-t+1)\,)$.

Επαληθεύστε ότι η ελάχιστη απόσταση του κώδικα ικανοποιεί πράγματι την παραπάνω ανισότητα. Παρατηρήστε, επίσης, ότι όλες οι (κωδικο)λέξεις έχουν το ίδιο βάρος k, δηλαδή πρόκειται για κώδικα *σταθερού* βάρους. Ο κώδικας αυτός δεν είναι γραμμικός.

Υπενθυμίζουμε ότι, αν έχουμε ένα διάνυσμα $\mathbf{a} = a_1 a_2 \cdots a_n$, το σύνολο των θέσεων $\{\, i_1,\, i_2,\, \ldots,\, i_k \,\}$, όπου $a_{i_j} \neq 0,\ j = 1,\, 2,\, \ldots,\, k$ ονομάζεται υπόβαθρο του $\mathbf{a}$.

Επίσης, αν έχουμε δύο διανύσματα $\mathbf{a} = a_1 a_2 \cdots a_n$ και $\mathbf{b} = b_1 b_2 \cdots b_n$, το $\mathbf{a}$ καλύπτει το $\mathbf{b}$, αν το υπόβαθρο του $\mathbf{b}$ είναι υποσύνολο του υπόβαθρου του $\mathbf{a}$.

Ορισμός 6.1.17. *Έστω* $\mathcal{C}$ *ένας δυαδικός κώδικας μήκους* n *και* S_w *το σύνολο των (κωδικο)λέξεων βάρους* w*. Αν τα υπόβαθρα των (κωδικο)λέξεων που ανήκουν στο σύνολο* S_w *αποτελούν τα υποσύνολα (τμήματα) ενός* $t-(n,\, w,\, \lambda)$ *σχεδιασμού (επί του συνόλου* $\{\, 1,\, 2,\, \ldots,\, n \,\}$*), θα λέμε ότι το σύνολο* S_w *σχηματίζει έναν* $t-(n,\, w,\, \lambda)$ *σχεδιασμό. Δηλαδή για κάθε υποσύνολο* T *του* $\{\, 1,\, 2,\, \ldots,\, n \,\}$ *με* t *το πλήθος στοιχεία υπάρχουν ακριβώς* λ

το πλήθος (κωδικο)λέξεις στον κώδικα $\mathcal{C}$ βάρους w οι οποίες έχουν 1 στις θέσεις που υπαγορεύονται από τα στοιχεία του συνόλου T.

Θεώρημα 6.1.18. *Έστω $\mathcal{C}$ ένας δυαδικός (n, M, d) τέλειος κώδικας. Το σύνολο S_d των (κωδικο)λέξεων ελαχίστου βάρους d σχηματίζει έναν σχεδιασμό Steiner $S(t+1, d, n)$, με $t = \frac{d-1}{2}$.*

Απόδειξη. Ο κώδικας $\mathcal{C}$ έχει υποτεθεί τέλειος, επομένως οι σφαίρες κάλυψης ακτίνας $t = \frac{d-1}{2}$ είναι ξένες μεταξύ τους και καλύπτουν ολόκληρο τον χώρο $\mathbb{Z}_2^n$. Συνεπώς, μια (κωδικο)λέξη $\mathbf{x}$ βάρους $t+1$ περιέχεται σε ακριβώς μια σφαίρα κάλυψης με κέντρο έστω $\mathbf{c}$. Αυτό σημαίνει ότι $d(\mathbf{c}, \mathbf{x}) \leq t$, απ' όπου έχουμε ότι $w(\mathbf{c}) \leq d(\mathbf{c}, \mathbf{x}) + w(\mathbf{x}) \leq t + (t+1) = d$, δηλαδή $\mathbf{c} \in S_d$. Συνοψίζοντας, από τα προηγούμενα, έχουμε $w(\mathbf{x}) = t+1$, $w(\mathbf{c}) = d = 2t+1$, $d(\mathbf{c}, \mathbf{x}) \leq t$.

Από την Πρόταση 1.2.11 τώρα έχουμε $2w(\mathbf{x} \cap \mathbf{c}) = w(\mathbf{x}) + w(\mathbf{c}) - d(\mathbf{c}, \mathbf{x}) \geq 2t+2$, δηλαδή $w(\mathbf{x} \cap \mathbf{c}) \geq t+1 = w(\mathbf{x})$, αυτό σημαίνει ότι το $\mathbf{c}$ καλύπτει το $\mathbf{x}$.

Το τελευταίο αποδεικνύει τον ισχυρισμό του Θεωρήματος. (γιατί;) ό.έ.δ.

Πόρισμα 6.1.19. *Έστω $\mathcal{C}$ ένας δυαδικός (n, M, d) τέλειος κώδικας. Αν $d = 2t+1$, τότε οι αριθμοί $\lambda_s = \binom{n-s}{t+1-s} / \binom{2t+1-s}{t+1-s}$ είναι ακέραιοι για όλα τα $1 \leq s \leq t$.*

Απόδειξη. Απλός συνδυασμός των δύο προηγουμένων Θεωρημάτων (6.1.13 και 6.1.18. ό.έ.δ.

Πόρισμα 6.1.20. *Έστω $\mathcal{C}$ ένας δυαδικός (n, M, d) τέλειος κώδικας με $d = 2t+1$. Το πλήθος των (κωδικο)λέξεων ελαχίστου βάρους d είναι ίσον με $A_d = \binom{n}{t+1} / \binom{d}{t+1}$.*

Παράδειγμα 6.1.21. Στον δυαδικό κώδικα Hamming $\mathcal{H}(r, 2)$ το σύνολο S_d των (κωδικο)λέξεων ελαχίστου βάρους d σχηματίζει έναν $S(2, 3, 2^r - 1)$ σχεδιασμό Steiner και το πλήθος των (κωδικο)λέξεων βάρους 3 ισούται με $A_3 = \binom{2^r-1}{2} / \binom{3}{2} = \frac{(2^r-1)(2^{r-1}-1)}{3}$.

Θα τελειώσουμε με μια *επαναπόδειξη* ότι δεν υπάρχουν τέλειοι κώδικες με παραμέτρους $(n, M, d) = (90, 2^{78}, 3)$.

Στην Παράγραφο 4.3 (ιδέ το Θεώρημα 4.3.1, όπως επίσης και την Πρόταση 4.3.2) είχαμε δει ότι (αν υπάρχει) ένας κώδικας με παραμέτρους $(n,\, M,\, d) = (90,\, 2^{78},\, 3)$ πληροί το φράγμα ομαδοποίησης σφαιρών. Παρόλα ταύτα η αναγκαία αυτή συνθήκη δεν είναι ικανή για την ύπαρξη ενός τέτοιου κώδικα.

Είναι εύκολο να δούμε ότι, αν υπήρχε ένας κώδικας με παραμέτρους $(n, M, d) = (90,\, 2^{78},\, 3)$, από το Πόρισμα 6.1.19 θα έπρεπε ο αριθμός $\lambda_2 = \binom{88}{1}/\binom{3}{1} = 88/3$ να είναι ακέραιος.

Εδώ θα πρέπει να τονίσουμε ότι η απόδειξη της Πρότασης 4.3.2 στην πραγματικότητα είναι η *ίδια* με την απόδειξη του Θεωρήματος 6.1.18, μόνο που εκεί, αν και χρησιμοποιούμε την έννοια του σχεδιασμού, δεν την *ομολογούμε*.

6.1.1 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.

2. Δείξτε ότι οι (κωδικο)λέξεις ελαχίστου βάρους στον κώδικα Goley $\mathcal{G}_{23}$ σχηματίζουν έναν σχεδιασμό Steiner $S(4,\, 7,\, 23)$. Υπολογίστε το πλήθος των (κωδικο)λέξεων βάρους 7.

   Συγκρίνετε το αποτέλεσμα αυτό με την Άσκηση $4.2.5_2$.

   Υπόδειξη: Επικαλεσθήτε το Θεώρημα 6.1.18.

3. Έστω $\mathcal{C}$ ένας δυαδικός $(n,\, M,\, d)$ τέλειος κώδικας και $\widehat{\mathcal{C}}$ ο κώδικας που προκύπτει αν επισυνάψουμε ένα ψηφίο ελέγχου ισοτιμίας. Δείξτε ότι το σύνολο των (κωδικο)λέξεων βάρους $d+1$ σχηματίζει έναν $S(t+2,\, d+1,\, n+1)$ σχεδιασμό Steiner, με $t = \frac{d-1}{2}$.

   Συγκρίνατε με το Θεώρημα 6.1.18.

4. Έστω $S(t,\, k,\, v)$ ένας σχεδιασμός Steiner επί του συνόλου S. Επιλέγουμε ένα στοιχείο $s \in S$. Από τον σχεδιασμό $S(t,\, k,\, v)$ επιλέγουμε μόνο εκείνα τα υποσύνολα (τμήματα), τα οποία περιέχουν το στοιχείο s. Κατόπιν, διαγράφουμε από τα τμήματα αυτά το στοιχείο s. Οπότε προκύπτει μια (υπο)οικογένεια, της οποίας τα τμήματα έχουν $k-1$ το πλήθος

στοιχεία. Δείξτε ότι η οικογένεια που αποτελείται από τα τμήματα αυτά σχηματίζει έναν $S(t-1,\, k-1,\, v-1)$ σχεδιασμό Steiner.

5. Έστω $B_1 = \{1, 3, 4, 5, 9\}$, $B_2 = \{1, 4, 6, 7, 8\}$, $B_3 = \{4, 7, 9, 10, 11\}$, $B_4 = \{1, 2, 3, 7, 10\}$, $B_5 = \{2, 4, 5, 6, 10\}$, $B_6 = \{2, 5, 7, 8, 9\}$, $B_7 = \{1, 5, 8, 10, 11\}$, $B_8 = \{2, 3, 4, 8, 11\}$, $B_9 = \{3, 5, 6, 7, 11\}$, $B_{10} = \{3, 6, 8, 9, 10\}$, $B_{11} = \{1, 2, 6, 9, 11\}$ τα τμήματα ένος $2-(11,\, 5,\, 2)$ σχεδιασμού. Όπως στο Παράδειγμα 6.1.8, να κατασκευάσετε έναν δυαδικό κώδικα με παραμέτρους $(11,\, 24,\, 5)$. Δείξτε ότι ο κώδικας αυτός είναι βέλτιστος (επιτυγχάνεται το φράγμα Plotkin).

   Δείξτε ότι στην περίπτωση αυτή το φράγμα Hamming δεν είναι ένα καλό φράγμα.

6.2 Πίνακες και κώδικες Hadamard

Ως γνωστόν, η ανισότητα Hadamard είναι η εξής: Για κάθε τετραγωνικό $n \times n$ πίνακα $\mathrm{H} = (h_{ij})$ με στοιχεία πραγματικούς αριθμούς που ικανοποιούν τη σχέση $|\, h_{ij} \,| \leq 1$ για όλα τα $1 \leq i,\, j \leq n$ ισχύει $|\, \det(\mathrm{H}) \,| \leq n^{n/2}$. Επιπλέον, στην παραπάνω σχέση ισχύει ισότητα, αν και μόνο αν $\mathrm{HH}^t = n\mathrm{I}_n$, όπου I_n είναι ο ταυτοτικός πίνακας τάξης n.

Ορισμός 6.2.1. *Ένας τετραγωνικός $n \times n$ πίνακας* H, *του οποίου όλα τα στοιχεία ισούνται με 1 ή -1 και ικανοποιεί τη σχέση* $\mathrm{HH}^t = n\mathrm{I}_n$ *ονομάζεται* ***πίνακας Hadamard*** *τάξης n.*

Παραδείγματα 6.2.2. 1. Οι πίνακες:

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{και} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

είναι πίνακες Hadamard τάξης 2 και 4 αντίστοιχα.

2. Ας υποθέσουμε ότι έχουμε έναν 3×3 πίνακα Hadamard. Ο πίνακας αυτός θα είναι της μορφής:

$$\mathrm{H} = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

Από την απαίτηση του ορισμού έχουμε ότι όλα τα a_i, b_i, c_i ισούνται με 1 ή -1. Επίσης $\mathrm{HH}^t = 3\mathrm{I}_3$. Αυτό σημαίνει ότι, αν πολλαπλασιάσουμε την πρώτη γραμμή του πίνακα με την δεύτερη, θα έχουμε $a_1b_1 + a_2b_2 + a_3b_3 = 0$, ισότητα που δεν μπορεί να ισχύει (γιατί;).

Άρα, δεν υπάρχουν 3×3 πίνακες Hadamard.

Παρατηρήσεις 6.2.3. Έστω H ένας πίνακας Hadamard τάξης n.

1. Από τη σχέση $\mathrm{HH}^t = n\mathrm{I}_n$ έπεται ότι $(\det(\mathrm{H}))^2 = n^n$, δηλαδή ένας πίνακας Hadamard είναι αντιστρέψιμος. Μάλιστα δε έχουμε ότι:

$$\mathrm{H}^{-1}(\mathrm{HH}^t) = \mathrm{H}^{-1}(n\mathrm{I}_n) = n\mathrm{H}^{-1}.$$

Δηλαδή $\mathrm{H}^t = n\mathrm{H}^{-1}$. Συνεπώς $\mathrm{H}^{-1} = \frac{1}{n}\mathrm{H}^t$ και επομένως $\mathrm{H}^t\mathrm{H} = n\mathrm{I}_n$. Άρα, ο ανάστροφος ενός πίνακα Hadamard είναι και αυτός πίνακας Hadamard.

2. Από τον ορισμό ($\mathrm{HH}^t = n\mathrm{I}_n$) έχουμε ότι δύο (διαφορετικές) γραμμές του πίνακα H είναι μεταξύ τους κάθετες (το εσωτερικό τους γινόμενο, ως διανύσματα, είναι ίσον με μηδέν). Επειδή η ορθογωνιότητα διατηρείται αν αντί του ενός διανύσματος πάρουμε το αντίθετό του, έπεται ότι, αν πολλαπλασιάσουμε μια γραμμή του πίνακα H με το -1, ο πίνακας που προκύπτει είναι και αυτός πίνακας Hadamard (γιατί;). Όμοια, αν πολλαπλασιάσουμε μια στήλη του πίνακα H με το -1, ο πίνακας που προκύπτει είναι και αυτός πίνακας Hadamard.

3. Πολλαπλασιάζοντας τώρα με το -1 όλες τις στήλες του πίνακα H, που το πρώτο τους στοιχείο είναι ίσον με -1 και όλες τις γραμμές του,

που το πρώτο τους στοιχείο είναι ίσον με -1, προκύπτει ένας πίνακας Hadamard, του οποίου όλα τα στοιχεία της πρώτης γραμμής και της πρώτης στήλης είναι ίσα με 1. Ένας τέτοιος πίνακας ονομάζεται **κανονικοποιημένος** πίνακας Hadamard.

Επομένως, δοθέντος ενός πίνακα Hadamard, πάντα υπάρχει ένας κανονικοποιημένος πίνακας Hadamard.

4. Αν μεταθέσουμε δύο γραμμές ή δύο στήλες του πίνακα H, τότε προφανώς προκύπτει ένας πίνακας Hadamard.

Δύο πίνακες Hadamard τάξης n ονομάζονται ισοδύναμοι, αν ο ένας προκύπτει από τον άλλο εφαρμόζοντας μεταθέσεις στις γραμμές ή στήλες του ή πολλαπλασιάζοντας γραμμές ή στήλες του με -1.

Προφανώς η παραπάνω σχέση είναι σχέση ισοδυναμίας μεταξύ όλων των πινάκων Hadamard της ιδίας τάξης.

Όπως είδαμε στο Παράδειγμα 6.2.2 δεν υπάρχουν πίνακες Hadamard τάξης 3. Το επιχείρημα που εφαρμόσαμε εκεί μπορεί να γενικευθεί.

Θεώρημα 6.2.4. *Έστω* $\mathrm{H} = (h_{ij})$ *ένας πίνακας Hadamard τάξης* $n > 2$. *Τότε* $n = 4m$.

Απόδειξη. Δεδομένου ότι υπάρχει ένας πίνακας Hadamard τάξης n, υπάρχει ένας κανονικοποιημένος πίνακας Hadamard τάξης n. Επομένως, χωρίς βλάβη, μπορούμε να υποθέσουμε ότι τα στοιχεία της πρώτης γραμμής είναι όλα ίσον με 1 και ότι το άθροισμα των στοιχείων κάθε άλλης γραμμής είναι ίσον με μηδέν.

Δεδομένου ότι η δεύτερη και τρίτη γραμμή είναι μεταξύ τους κάθετες, αναπτύσσοντας το άθροισμα $\sum_{j=1}^{n}(1+h_{2j})(1+h_{3j})$ έχουμε ότι:

$$\sum_{j=1}^{n}(1+h_{2j})(1+h_{3j}) = n+\sum_{j=1}^{n}h_{2j}+\sum_{j=1}^{n}h_{3j}+\sum_{j=1}^{n}h_{2j}h_{3j} = n.$$

Αλλά κάθε όρος $(1+h_{2j})(1+h_{3j})$ του αθροίσματος ισούται είτε με μηδέν είτε με 4. Συνεπώς το n είναι πολλαπλάσιο του 4. ό.έ.δ.

Από τα προηγούμενα έπεται ότι αναγκαία συνθήκη για την ύπαρξη ενός πίνακα Hadamard τάξης n είναι $n = 1$ ή $n = 2$ ή $n = 4m$. Παρόλα ταύτα παραμένει ανοικτό το ερώτημα κατά πόσον η συνθήκη αυτή είναι και ικανή. Δηλαδή, υπάρχει πίνακας Hadamard τάξης n για κάθε $n = 4k,\ k \geq 1$;

Έχουν αναπτυχθεί διάφορες τεχνικές κατασκευής πινάκων Hadamard. Εμείς εδώ απλώς αναφέρουμε τον προφανή τρόπο κατασκευής ενός πίνακα Hadamard τάξης $2n$ από έναν πίνακα Hadamard τάξης n.

Πρόταση 6.2.5. *Αν ο πίνακας* H *είναι πίνακας Hadamard τάξης* n*, τότε ο πίνακας:*

$$\begin{pmatrix} \mathrm{H} & \mathrm{H} \\ \mathrm{H} & -\mathrm{H} \end{pmatrix}$$

είναι πίνακας Hadamard τάξης $2n$*.*

Απόδειξη. Με απλές πράξεις επαληθεύεται ότι:

$$\begin{pmatrix} \mathrm{H} & \mathrm{H} \\ \mathrm{H} & -\mathrm{H} \end{pmatrix} \cdot \begin{pmatrix} \mathrm{H} & \mathrm{H} \\ \mathrm{H} & -\mathrm{H} \end{pmatrix}^t = 2n\mathrm{I}_{2n}.$$

ό.έ.δ.

Θα δούμε τώρα τη σχέση μεταξύ πινάκων Hadamard και σχεδιασμών.

Έστω H ένας κανονικοποιημένος πίνακας Hadamard τάξης $4t$ ($t \geq 2$). Από τον πίνακα H κατασκευάζουμε έναν άλλο πίνακα G με την εξής διαδικασία. Στις θέσεις του πίνακα H, όπου εμφανίζεται -1, αντικαθιστούμε το -1 με μηδέν και, κατόπιν, διαγράφουμε την πρώτη γραμμή και πρώτη στήλη, οπότε προκύπτει ένας $(4t-1) \times (4t-1)$ πίνακας G.

Ας δούμε τι ιδιότητες έχει ο πίνακας G. Από τον ορισμό του κανονικοποιημένου πίνακα Hadamard, έχουμε ότι κάθε γραμμή και κάθε στήλη του πίνακα G έχει $2t$ το πλήθος μηδενικά και $2t-1$ το πλήθος 1. Επιπλέον, παρατηρούμε ότι, επειδή στον κανονικοποιημένο πίνακα H σε κάθε δύο διαφορετικές γραμμές (εκτός της πρώτης) υπάρχουν t το πλήθος κοινές θέσεις, όπου εμφανίζεται το 1 (γιατί;), έχουμε ότι στον πίνακα G σε κάθε δύο διαφορετικές γραμμές υπάρχουν $t-1$ το πλήθος κοινές θέσεις, όπου εμφανίζεται το 1.

Επομένως, με απλή επαλήθευση, βλέπουμε ότι ισχύει $\mathrm{GG}^t = t\mathrm{I} + (t-1)\mathrm{J}$, όπου I είναι ο ταυτοτικός $(4t-1)\times(4t-1)$ πίνακας και J ένας $(4t-1)\times(4t-1)$ πίνακας, του οποίου όλα τα στοιχεία είναι ίσα με 1.

Θεωρούμε τώρα τις $4t-1$ το πλήθος συντεταγμένες μιας γραμμής ως στοιχεία ενός συνόλου S και για κάθε γραμμή θεωρούμε το υποσύνολο (τμήμα) του συνόλου S που αποτελείται από τις συντεταγμένες εκείνες στις οποίες εμφανίζεται το 1. Κάθε τέτοιο υποσύνολο (τμήμα) περιέχει $2t-1$ το πλήθος στοιχεία και κάθε δύο συντεταγμένες (στοιχεία του συνόλου S) εμφανίζονται σε $t-1$ το πλήθος υποσύνολα (τμήματα). Δηλαδή έχουμε κατασκευάσει έναν $2-(4t-1,\, 4t-1,\, 2t-1,\, 2t-1,\, t-1)$ ισορροπημένο μη πλήρη σχεδιασμό, του οποίου ο προσαπτόμενος πίνακας είναι ο πίνακας G.

Αντίστροφα, έστω ένας $2-(4t-1,\, 4t-1,\, 2t-1,\, 2t-1,\, t-1)$ σχεδιασμός ($t \geq 2$), του οποίου ο προσαπτόμενος πίνακας είναι ο πίνακας G. Τότε μπορούμε να κατασκευάσουμε έναν κανονικοποιημένο $(4t)\times(4t)$ πίνακα Hadamard αντικαθιστώντας στον πίνακα G τα μηδέν με -1 και επισυνάπτοντας επιπλέον (ως αρχικές) μια γραμμή και μια στήλη των οποίων όλα τα στοιχεία ισούνται με 1[4].

Παράδειγμα 6.2.6. Στο Παράδειγμα 6.1.2 είχαμε το σύνολο:

$$S = \{1,\, 2,\, 3,\, 4,\, 5,\, 6,\, 7\},$$

από το οποίο, λαμβάνοντας τα υποσύνολα:

$$\begin{aligned} B_1 &= \{1,\, 2,\, 3\}, & B_2 &= \{3,\, 4,\, 5\},\\ B_3 &= \{1,\, 5,\, 6\}, & B_4 &= \{1,\, 4,\, 7\},\\ B_5 &= \{3,\, 6,\, 7\}, & B_6 &= \{2,\, 5,\, 7\} \text{ και}\\ B_7 &= \{2,\, 4,\, 6\}, \end{aligned}$$

είχαμε κατασκευάσει τον $2-(7,\, 7,\, 3,\, 3,\, 1)$-σχεδιασμό.

Στο Παράδειγμα 6.1.5 είχαμε δει ότι ο προσαπτόμενος πίνακας του σχεδιασμού αυτού είναι ο πίνακας:

[4]Για τον λόγο, αυτό στην σχετική βιβλιογραφία ένας $2-(4t-1,\, 4t-1,\, 2t-1,\, 2t-1,\, t-1)$ σχεδιασμός ονομάζεται σχεδιασμός Hadamard

$$\mathrm{G} = \begin{array}{c|ccccccc} & B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \\ \hline 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 3 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 5 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 6 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 7 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}.$$

Οπότε ο κανονικοποιημένος πίνακας Hadamard, που προκύπτει από τον παραπάνω πίνακα είναι ο πίνακας:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}.$$

Όταν δοθεί ο προσαπτόμενος πίνακας ενός σχεδιασμού, μπορούμε να κατασκευάσουμε κώδικες (βλέπε Παραδείγματα 6.1.8 και 6.1.16). Επομένως και εδώ, όταν δοθεί ένας κανονικοποιημένος πίνακας Hadamard, κατασκευάζοντας τον αντίστοιχο σχεδιασμό, μπορούμε να κατασκευάσουμε διάφορους κώδικες.

Έστω H ένας κανονικοποιημένος πίνακας Hadamard τάξης $n = 4t$. Όπως προηγουμένως, στις θέσεις του πίνακα H, όπου εμφανίζεται -1, αντικαθιστούμε το -1 με μηδέν οπότε προκύπτει ένας πίνακας M (ο *δυαδικός* πίνακας Hadamard). Κάθε δύο γραμμές του πίνακα M συμφωνούν σε $2t = n/2$ το πλήθος θέσεις και διαφέρουν σε $2t = n/2$ το πλήθος θέσεις. Επομένως, αν κατασκευάσουμε τον κώδικα $\mathcal{A}_n$ του οποίου τα στοιχεία είναι οι γραμμές του πίνακα M και τα συμπληρώματά τους, τότε έχουμε έναν $(n, 2n, n/2)$ κώδικα.

Αν από τα στοιχεία του κώδικα $\mathcal{A}_n$ διαγράψουμε την πρώτη συντεταγμένη, τότε προκύπτει ένας κώδικας $\mathcal{B}_n$, του οποίου το μήκος κάθε (κω-

δικο)λέξης είναι ίσον με $n-1$ και με ελάχιστη απόσταση τουλάχιστον ίση με $d = \frac{n}{2} - 1$ (γιατί;), άρα έχουμε έναν $(n-1,\, 2n,\, d)$ κώδικα.

Αν από τις γραμμές του πίνακα M διαγράψουμε την πρώτη συντεταγμένη, τότε λαμβάνουμε έναν $(n-1,\, n,\, n/2)$ κώδικα $\mathcal{C}_n$.

Παρατηρήσεις 6.2.7. 1. Ο κώδικας $\mathcal{B}_n$ αποτελεί μια σύμπτυξη του κώδικα $\mathcal{A}_n$ και ο κώδικας $\mathcal{C}_n$ αποτελεί μια σμίκρυνση του $\mathcal{B}_n$, δηλαδή μια συμπύκνωση του κώδικα $\mathcal{A}_n$ (ιδέ σελίδα 47).

2. Ο προσαπτόμενος στον σχεδιασμό $2-(4t-1,\, 4t-1,\, 2t-1,\, 2t-1,\, t-1)$ πίνακας G προέρχεται, από τον πίνακα M, με διαγραφή της πρώτης στήλης και πρώτης γραμμής του.

3. Οι κώδικες που κατασκευάσαμε παραπάνω δεν είναι κατ' ανάγκη γραμμικοί.

Οι τρείς κώδικες που κατασκευάσαμε ονομάζονται **κώδικες Hadamard**.

Θεώρημα 6.2.8. *Οι τρεις κώδικες Hadamard $\mathcal{A}_n$, $\mathcal{B}_n$, $\mathcal{C}_n$ ικανοποιούν το φράγμα Plotkin.*

Απόδειξη. Η απόδειξη είναι άμεση από το Θεώρημα 1.5.25. ό.έ.δ.

Παράδειγμα 6.2.9. Έστω ο κανονικοποιημένος πίνακας Hadamard:

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Σύμφωνα με τα προηγούμενα έχουμε τους εξής Hadamard κώδικες:

$$\begin{aligned} \mathcal{A}_4 &= \{\, 1111,\, 1010,\, 1100,\, 1001,\, 0000,\, 0101,\, 0011,\, 0110 \,\}, \\ \mathcal{B}_4 &= \{\, 111,\, 010,\, 100,\, 001,\, 000,\, 101,\, 011,\, 110 \,\}, \\ \mathcal{C}_4 &= \{\, 111,\, 010,\, 100,\, 001 \,\}. \end{aligned}$$

Έστω ο πίνακας Hadamard:

$$\mathrm{H}_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Από την Πρόταση 6.2.5 έπεται ότι για κάθε $m \geq 2$ μπορούμε αναδρομικά να κατασκευάσουμε τους πίνακες Hadamard:

$$\mathrm{H}_{2^m} = \begin{pmatrix} \mathrm{H}_{2^{m-1}} & \mathrm{H}_{2^{m-1}} \\ \mathrm{H}_{2^{m-1}} & -\mathrm{H}_{2^{m-1}} \end{pmatrix}.$$

Πρόταση 6.2.10. *Ο κώδικας $\mathcal{A}_{2^m}$ που προκύπτει από τον πίνακα H_{2^m} σύμφωνα με την κατασκευή που περιγράψαμε προηγουμένως, [δηλαδή ως (κωδικο)λέξεις λαμβάνουμε τις γραμμές του πίνακα H_{2^m} και τα συμπληρώματά τους και όπου εμφανίζεται -1, αντικαθιστούμε το -1 με μηδέν], είναι ο κώδικας Reed-Muller $\mathcal{RM}_1(m)$.*

Απόδειξη. Στην Παράγραφο 4.4 (ιδέ σελίδα 257 και εντεύθεν) είχαμε ορίσει αναδρομικά, για κάθε $m \geq 1$, τους κώδικες Reed-Muller $\mathcal{RM}_1(m)$ χρησιμοποιώντας την $(\mathbf{u},\, \mathbf{u}+\mathbf{v})$-κατασκευή. Συγκεκριμμένα, είχαμε δει ότι για $m \geq 2$ ισχύει:

$$\mathcal{RM}_1(m) = \{(\mathbf{u},\, \mathbf{u}) \mid \mathbf{u} \in \mathcal{RM}_1(m-1)\} \cup \{(\mathbf{u},\, \mathbf{u}+\mathbf{1}) \mid \mathbf{u} \in \mathcal{RM}_1(m-1)\}. \quad (*)$$

Για $m = 1, 2$ εύκολα βλέπουμε ότι πράγματι $\mathcal{A}_2 = \mathcal{RM}_1(1)$ και $\mathcal{A}_{2^2} = \mathcal{RM}_1(2)$. Θα χρησιμοποιήσουμε επαγωγή για $m \geq 3$.

Από τον τρόπο κατασκευής του πίνακα H_{2^m} από τον πίνακα $\mathrm{H}_{2^{m-1}}$ έχουμε ότι οι (κωδικο)λέξεις που λαμβάνουμε από τις γραμμές του πίνακα H_{2^m} και τα συμπληρώματά τους, αντικαθιστώντας όπου εμφανίζεται -1 με μηδέν, είναι ακριβώς της μορφής $(\mathbf{u},\, \mathbf{u})$ και $(\mathbf{u},\, \mathbf{u}+\mathbf{1})$, όπου το $\mathbf{u}$ διατρέχει τις γραμμές του πίνακα $H_{2^{m-1}}$ και τα συμπληρώματά τους αντικαθιστώντας το -1 (όπου εμφανίζεται) με μηδέν. Από την υπόθεση της επαγωγής και τη σχέση $(*)$ έπεται το αποτέλεσμα. ό.έ.δ.

6.2.1 Ασκήσεις

1. Στο Θεώρημα 6.2.8 εξετάστε αν ισχύει ισότητα στο φράγμα Plotkin για τους τρεις κώδικες Hadamard $\mathcal{A}_n$, $\mathcal{B}_n$ και $\mathcal{C}_n$.

2. Έστω H_1 και H_2 δύο κανονικοποιημένοι πίνακες Hadamard τάξης n. Για κάθε έναν από αυτούς κατασκευάζουμε τους κώδικες Hadamard (ιδέ σελίδα 371). Να συγκρίνετε αυτούς τους κώδικες.

3. Να κατασκευάσετε έναν κανονικοποιημένο πίνακα Hadamard H και με την διαδικασία που περιγράφεται στη σελίδα 369 να επανακατασκευάσετε τον σχεδιασμό που αναφέρεται στο Παράδειγμα 6.1.2. Κατόπιν, να κατασκευάσετε τον κώδικα που αναφέρεται στο Παράδειγμα 6.1.8.

   Να συγκρίνετε τον κώδικα που μόλις κατασκευάσατε με τους κώδικες Hadamard που κατασκευάσαμε στην σελίδα 371.

6.3 Λατινικά Τετράγωνα και Κώδικες

Τα Λατινικά Τετράγωνα έχουν επινοηθεί και μελετηθεί εδώ και αιώνες ως μια ενδιαφέρουσα συνδυαστική κατασκευή με πολλές πρακτικές και θεωρητικές εφαρμογές. Η μελέτη τους εξακολουθεί να είναι ενεργή ακόμη και σήμερα με πολλά ανοικτά προβλήματα.

Εμείς εδώ θα περιορισθούμε απλώς σε ορισμούς και σε μερικές ιδιότητες, αναγκαίες για να αναδειχθεί η σχέση μεταξύ Λατινικών Τετραγώνων και Κωδίκων.

Ορισμός 6.3.1. *Ένα* ***Λατινικό Τετράγωνο*** *τάξης (ή μεγέθους)* n *είναι ένας* $n \times n$ *πίνακας, τα στοιχεία του οποίου λαμβάνονται από ένα σύνολο με* n *το πλήθος διακεκριμένα στοιχεία (συνήθως συμβολιζομένων με* $1, 2, \ldots, n-1, n$*), διευθετημένα έτσι, ώστε σε κάθε γραμμή και κάθε στήλη κάθε στοιχείο να εμφανίζεται ακριβώς μια φορά.*

Παράδειγμα 6.3.2. Ένα Λατινικό Τετράγωνο τάξης 4 είναι το ακόλουθο:

1	3	2	4
4	2	3	1
2	4	1	3
3	1	4	2

Επισημαίνουμε ότι, προφανώς, μεταθέτοντας τις γραμμές ή στήλες ενός Λατινικού Τετραγώνου προκύπτει ένα άλλο Λατινικό Τετράγωνο *ισοδύναμο* με το αρχικό. Αυτό σημαίνει ότι πάντα μπορούμε να μεταθέσουμε τις γραμμές και τις στήλες ενός Λατινικού τετραγώνου, ώστε να πετύχουμε ένα ισοδύναμο Λατινικό Τετράγωνο με την ιδιότητα τα στοιχεία της πρώτης γραμμής και της πρώτης στήλης να εμφανίζονται με την διάταξη $1\,2\,\cdots\,n$. Ένα τέτοιο Λατινικό Τετράγωνο θα ονομάζεται *ανηγμένο*.

Για παράδειγμα ένα ανηγμένο Λατινικό Τετράγωνο τάξης 4 είναι το ακόλουθο:

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Θεώρημα 6.3.3. *Για κάθε $n \geq 1$ υπάρχει ένα Λατινικό Τετράγωνο τάξης n.*

Απόδειξη. Λαμβάνοντας ως πρώτη γραμμή την $1\,2\,\cdots\,n$ και κάνοντας κάθε φορά μια κυκλική μετάθεση των στοιχείων της έχουμε κατά σειρά τις επόμενες γραμμές ενός Λατινικού Τετραγώνου.

1	2	3	$\cdots$	$n-2$	$n-1$	n
2	3	4	$\cdots$	$n-1$	n	1
3	4	5	$\cdots$	n	1	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\vdots$
n	1	2	$\cdots$	$n-3$	$n-2$	$n-1$

.

Ένας άλλος τρόπος για την απόδειξη της ύπαρξης Λατινικών Τετραγώνων οποιασδήποτε τάξης είναι να παρατηρήσουμε ότι ο πολλαπλασιαστικός πίνακας μιας πεπερασμένης ομάδας αποτελεί ένα Λατινικό Τετράγωνο (γιατί;). ό.έ.δ.

Παρατήρηση 6.3.4. Αν και ο πολλαπλασιαστικός πίνακας οποιασδήποτε πεπερασμένης ομάδας αποτελεί ένα Λατινικό Τετράγωνο, υπάρχουν Λατινικά Τετράγωνα, για τα οποία δεν υπάρχει πεπερασμένη ομάδα της οποίας ο πολλαπλασιαστικός πίνακας να αποτελεί το δοθέν Λατινικό Τετράγωνο. Μπορείτε να δώσετε ένα παράδειγμα;

Το κυριώτερο, ίσως, πρόβλημα στα Λατινικά Τετράγωνα είναι ο υπολογισμός του πλήθους των Λατινικών Τετραγώνων τάξης n για κάθε φυσικό αριθμό n. Με L_n θα συμβολίζουμε το πλήθος των Λατινικών Τετραγώνων τάξης n και με l_n το πλήθος των ανηγμένων Λατινικών Τετραγώνων τάξης n.

Για μικρές τιμές του n ο υπολογισμός των L_n και l_n είναι δυνατός (μάλιστα με την βοήθεια υπολογιστών έχουν υπολογισθεί τα L_n και l_n και για σχετικά μεγαλύτερες τιμές του n). Γενικά όμως, προς το παρόν (και όπως εικάζεται και στο μέλλον), δεν είναι δυνατόν να υπάρξει μια σχέση (συναρτήσει του n), η οποία να υπολογίζει το l_n. Παρόλα ταύτα μπορούμε να δούμε πώς σχετίζονται τα L_n και l_n.

Θεώρημα 6.3.5. *Για κάθε $n \geq 2$ ισχύει $L_n = n!\,(n-1)!\,l_n$.*

Απόδειξη. Δοθέντος ενός Λατινικού Τετραγώνου τάξης n, είναι προφανές ότι, μεταθέτοντας τις n το πλήθος στήλες του, μπορούμε να κατασκευάσουμε $n!$ το πλήθος Λατινικά Τετράγωνα, διαφορετικά μεταξύ τους. Ομοίως μεταθέτοντας τις $n-1$ το πλήθος γραμμές του (εκτός της πρώτης) κατασκευάζουμε $(n-1)!$ το πλήθος Λατινικά Τετράγωνα, διαφορετικά μεταξύ τους. Προφανώς όλα τα Λατινικά Τετράγωνα, τα οποία κατασκευάζονται με μεταθέσεις γραμμών του αρχικού Λατινικού Τετραγώνου, είναι διαφορετικά από αυτά που κατασκευάζονται με μεταθέσεις των στηλών του αρχικού Λατινικού Τετραγώνου.

Συνεπώς, αν ξεκινήσουμε με ένα ανηγμένο Λατινικό Τετράγωνο, τελικά μπορούμε να κατασκευάσουμε $n!\,(n-1)!$ το πλήθος Λατινικά Τετράγωνα, εκ των οποίων μόνο ένα είναι ανηγμένο. Δεδομένου ότι υπάρχουν l_n το πλήθος ανηγμένα Λατινικά Τετράγωνα τάξης n, μπορούμε τελικά να κατασκευάσουμε $n!\,(n-1)!l_n$ το πλήθος διακεκριμένα Λατινικά Τετράγωνα τάξης n.

Για να ολοκληρωθεί η απόδειξη πρέπει να επισημάνουμε ότι ξεκινώντας από ένα τυχαίο Λατινικό Τετράγωνο τάξης n και εφαρμόζοντας μεταθέσεις στις γραμμές και στις στήλες του επιτυγχάνουμε ακριβώς ένα ανηγμένο Λατινικό Τετράγωνο. ό.έ.δ.

Ερώτημα: Γιατί στην απόδειξη του προηγουμένου θεωρήματος επιτρέπεται να κάνουμε μεταθέσεις σε όλες τις στήλες ενός Λατινικού Τετραγώνου,

ενώ στις μεταθέσεις γραμμών πρέπει να εξαιρεθεί η πρώτη γραμμή;

Δοθέντων δύο Λατινικών Τετραγώνων του ιδίου μεγέθους n μπορούμε να εναποθέσουμε το ένα επί του άλλου, ώστε να προκύψει ένα τετράγωνο με n^2 το πλήθος διατεταγμένα ζεύγη όπως στο παράδειγμα:

1	2	3
2	3	1
3	1	2

a	b	c
c	a	b
b	b	a

$\rightsquigarrow$

$(1,\, a)$	$(2,\, b)$	$(3,\, c)$
$(2,\, c)$	$(3,\, a)$	$(1,\, b)$
$(3,\, b)$	$(1,\, b)$	$(2,\, a)$

.

Στο παράδειγμα αυτό παρατηρούμε ότι τα εννέα διατετεγμένα ζεύγη που σχηματίσθηκαν είναι διαφορετικά μεταξύ τους.

Ορισμός 6.3.6. *Δύο Λατινικά Τετράγωνα τάξης n θα ονομάζονται* ***ορθογώνια*** *, αν εναποθέτοντας το ένα επί του άλλου, τα n^2 το πλήθος διατεταγμένα ζεύγη που σχηματίζονται είναι διαφορετικά μεταξύ τους.*

Μία συλλογή $\{T_1, T_2, \ldots, T_m\}$ από Λατινικά Τετράγωνα, της ιδίας τάξης, θα λέγεται ότι αποτελείται από ***Αμοιβαίως*** *Ορθογώνια Λατινικά Τετράγωνα, αν για $i \neq j$ τα $Ti, T_j,$ είναι ορθογώνια.*[5]

Προφανώς, η ορθογωνιότητα ενός ζεύγους ορθογωνίων Λατινικών Τετραγώνων διατηρείται αν αναριθμήσουμε τα στοιχεία ενός εκ των δύο (άρα και των δύο) τετραγώνων (γιατί;) .

Έστω $N(n)$ το μέγιστο πλήθος Λατινικών Τετραγώνων τάξης n, που δύναται να υπάρξει, ώστε να είναι αμοιβαίως ορθογώνια.

Ένα κεντρικό πρόβλημα στα Λατινικά Τετράγωνα είναι ο υπολογισμός του $N(n)$ για τις διάφορες τιμές του n. Προφανώς δεν υπάρχουν δύο Λατινικά Τετράγωνα τάξης 2, τα οποία να είναι ορθογώνια (άρα $N(2) = 1$).

Θεώρημα 6.3.7. *$N(n) \leq n - 1$ για κάθε $n \geq 2$.*

Απόδειξη. Όπως έχουμε παρατηρήσει η ορθογωνιότητα δύο Λατινικών Τετραγώνων διατηρείται αν αναριθμήσουμε τα στοιχεία τους. Επομένως, μπορούμε να υποθέσουμε ότι σε όλα από τα $N(n)$ το πλήθος Λατινικά Τετράγωνα, τάξης n, η πρώτη γραμμή είναι της μορφής $1\,2\,\cdots\,n$.

[5] Μια τέτοια συλλογή στην ξενόγλωσση βιβλιογραφία συμβολίζεται ως MOLS (ή POLS), εκ του *mutually orthogonal latin squares*. (Η εκ του *pairwise orthogonal latin squares*.)

Ας δούμε τις δυνατές τιμές που μπορούν να εμφανισθούν στη θέση $(2,1)$ (δηλαδή στην δεύτερη γραμμή και πρώτη στήλη) σε καθένα από τα $N(n)$ τετράγωνα. Στη θέση αυτή δεν μπορεί να εμφανισθεί το ένα, διότι δεν θα είχαμε Λατινικό Τετράγωνο. Επίσης, δεν μπορεί σε δύο από τα $N(n)$ τετράγωνα να έχουμε το ίδιο στοιχείο στην ίδια θέση, διότι δεν θα διετηρείτο η ορθογωνιότητα (σε μία εναποθέτηση τετραγώνων όλα τα ζεύγη με ίσες συντεταγμένες θα εμφανίζονται στην πρώτη γραμμή). Επομένως, για την θέση $(2,1)$ μπορούμε να έχουμε το πολύ $n-1$ επιλογές. Άρα $N(n) \leq n-1$. ό.έ.δ.

Στην περίπτωση, όπου υπάρχει n έτσι ώστε $N(n) = n-1$, τότε έχουμε ένα **πλήρες** σύνολο MOLS.

Πριν μελετήσουμε περαιτέρω τα MOLS θα δούμε τη σχέση τους με την ύπαρξη κωδίκων.

Θεώρημα 6.3.8. *Για κάθε φυσικό αριθμό $n \geq 2$ και κάθε αλφάβητο $\mathbb{A}$ με q το πλήθος στοιχεία υπάρχει ένας κώδικας επί του $\mathbb{A}$ με παραμέτρους $(n, q^2, n-1)$, αν και μόνο αν υπάρχουν $n-2$ το πλήθος MOLS τάξης q.*

Απόδειξη. Έστω το αλφάβητο $\mathbb{A} = \{a_1, a_2, \ldots, a_q\}$. Υποθέτουμε ότι υπάρχουν $n-2$ το πλήθος MOLS τάξης q και $\{A^{(k)} \mid 1 \leq k \leq n-2\}$ είναι ένα σύνολο από αυτά με στοιχεία από το αλφάβητο $\mathbb{A}$. Με $a^{(k)}_{i,j}$ θα συμβολίζουμε το στοιχείο που βρίσκεται στην i-γραμμή και j-στήλη του τετραγώνου $A^{(k)}$.

Σχηματίζουμε τον κώδικα $\mathcal{C} = \{(a_i, a_j, a^{(1)}_{ij}, a^{(2)}_{ij}, \cdots, a^{(n-2)}_{ij}),\ 1 \leq i, j \leq q\}$. Ο κώδικας $\mathcal{C}$ έχει παραμέτρους $(n, q^2, n-1)$.

Προφανώς οι χαρακτήρες στις δύο πρώτες θέσεις κάθε (κωδικο)λέξης καθορίζουν το μέγεθος του που είναι ίσον με q^2.

Ως προς την ελάχιστη απόσταση του κώδικα, αν

$$\mathbf{c}_{ij} = (a_i, a_j, a^{(1)}_{ij}, a^{(2)}_{ij}, \cdots, a^{(n-2)}_{ij}) \quad \text{και} \quad \mathbf{c}_{rs} = (a_r, a_s, a^{(1)}_{rs}, a^{(2)}_{rs}, \cdots, a^{(n-2)}_{rs})$$

είναι δύο (κωδικο)λέξεις, τότε αυτές έχουν το πολύ έναν κοινό χαρακτήρα στις $n-2$ τελευταίες θέσεις, διότι αν συμφωνούσαν σε τουλάχιστον δύο θέσεις τότε τα αντίστοιχα Λατινικά Τετράγωνα δεν θα ήταν ορθογώνια. Επίσης, αν οι δύο κωδικολέξεις έχουν κοινό χαρακτήρα στην πρώτη θέση, δεν είναι

δυνατόν να έχουν κοινό χαρακτήρα σε καμία από τις $n-2$ τελευταίες θέσεις, διότι αυτό θα σήμαινε ότι ο ίδιος χαρακτήρας θα επαναλαμβανόταν σε μία γραμμή του αντίστοιχου Λατινικού Τετραγώνου, άτοπο. Όμοια, αν οι δύο (κωδικο)λέξεις έχουν κοινό χαρακτήρα στην δεύτερη θέση, δεν είναι δυνατόν να έχουν κοινό χαρακτήρα σε καμία από τις $n-2$ τελευταίες θέσεις, διότι τότε ο ίδιος χαρακτήρας θα επαναλαμβανόταν σε μία στήλη του αντίστοιχου Λατινικού Τετραγώνου, άτοπο. Συνεπώς, ο κώδικας $\mathcal{C}$ έχει ελάχιστη απόσταση ίση με $n-1$.

Αντίστροφα, υποθέτουμε ότι έχουμε έναν κώδικα που έχει παραμέτρους $(n,\, q^2,\, n-1)$ και στοιχεία από το αλφάβητο $\mathbb{A} = \{\, a_1, a_2, \ldots, a_q \}$. Μπορούμε να συμβολίσουμε τις (κωδικο)λέξεις του όπως προηγουμένως. Κατασκευάζουμε $n-2$ το πλήθος $q \times q$ τετράγωνα από τις $n-2$ τελευταίες θέσεις κάθε (κωδικο)λέξης ως εξής: $A^{(k)} = [a^{(k)}_{i\,j}]$, $k = 1, 2, \ldots, n-2$. Επειδή η ελάχιστη απόσταση του κώδικα είναι ίση με $n-1$ είναι προφανές (γιατί;) ότι πράγματι αυτά τα τεράγωνα είναι Λατινικά και μάλιστα ανά δύο ορθογώνια. ό.έ.δ.

Ερώτημα: Στην απόδειξη του προηγουμένου θεωρήματος δεν εξετάσαμε το ενδεχόμενο οι δύο κωδικολέξεις να έχουν κοινούς χαρακτήρες και στις δύο πρώτες θέσεις (γιατί;) .

Στο προηγούμενο Θεώρημα η ύπαρξη κωδίκων με παραμέτρους $(n,\, q^2,\, n-1)$ ανάγεται στην ύπαρξη $n-2$ το πλήθος MOLS τάξης q. Έχουμε δει στο Θεώρημα 6.3.7 ότι $N(q) \leq q-1$ για κάθε $q \geq 2$. Θα δούμε ότι, αν ο φυσικός αριθμός q είναι δύναμη ενός πρώτου, τότε ισχύει $N(q) = q-1$. Δηλαδή υπάρχει ένα πλήρες σύνολο MOLS.

Θεώρημα 6.3.9. *Αν $q = p^k$, όπου p είναι πρώτος τότε $N(q) = q-1$.*

Απόδειξη. Θεωρούμε το πεπερασμένο σώμα: $\mathbb{F} = \{r_0 = 0, r_1, r_2, \ldots, r_{q-1}\}$ με $q = p^k$ το πλήθος στοιχεία. Κατασκευάζουμε τα $q \times q$ τετράγωνα $T_1, T_2, \ldots,$ T_{q-1} ως εξής: Αριθμούμε τις γραμμές τους και στήλες τους με τους αριθμούς $0, 1, 2, \ldots, q-1$ και σε κάθε θέση $(i,\, j)$ του T_k τετραγώνου τοποθετούμε το στοιχείο $a^k_{i\,j} = r_i + r_k r_j$ του σώματος $\mathbb{F}$.

Είναι εύκολο να δούμε, χρησιμοποιώντας τον νόμο της διαγραφής ως προς την πρόσθεση και τον πολλαπλασιασμό του σώματος, ότι τα T_k είναι Λατινικά

Τετράγωνα και μάλιστα αμοιβαίως ορθογώνια. ό.έ.δ.

Έχοντας υπόψη τον Ορισμό 1.5.13 (ιδέ Παράγραφο 1.5.2) έχουμε το ακόλουθο.

Πόρισμα 6.3.10. *Για έναν φυσικό αριθμό q, ο οποίος είναι δύναμη ενός πρώτου και για κάθε $n \leq q+1$, υπάρχει βέλτιστος MDS γραμμικός κώδικας με παραμέτρους $[n, 2, n-1]$. Δηλαδή έχουμε $A_q(n, n-1) = q^2$.*

Απόδειξη. Η απόδειξη είναι άμεση από τα δύο προηγούμενα θεωρήματα και το γεγονός ότι στην περίπτωση αυτή ικανοποιείται το φράγμα Singleton (ιδέ Θεώρημα 1.5.21). ό.έ.δ.

Το προηγούμενο πόρισμα αναφέρεται σε κώδικες επί ενός αλφάβητου, του οποίου το πλήθος των στοιχείων του είναι δύναμη ενός πρώτου. Στη συνέχεια θα μελετήσουμε την περίπτωση κωδίκων επί αλφάβητων με πλήθος στοιχείων όχι κατ' ανάγκη δύναμη πρώτου αριθμού, αλλά με μικρό μήκος ($n = 3, 4$).

Πρόταση 6.3.11. *$A_q(3, 2) = q^2$ για κάθε $q \geq 2$.*

Απόδειξη. Σύμφωνα με το Θεώρημα 6.3.8, υπάρχει κώδικας με παραμέτρους $(3, q^2, 2)$, αν και μόνο αν υπάρχει Λατινικό Τετράγωνο τάξης q (εδώ $n-2 = 1$). Αλλά πάντα υπάρχουν Λατινικά Τετράγωνα οποιασδήποτε τάξης (Θεώρημα 6.3.3). Εδώ ικανοποιείται το φράγμα Singleton και συνεπώς $A_q(3, 2) = q^2$. ό.έ.δ.

Λήμμα 6.3.12. *Υποθέτουμε ότι έχουμε δύο Λατινικά τετράγωνα T_1 και T_2 με τάξεις n_1 και n_2 αντίστοιχα, τότε μπορούμε να κατασκευάσουμε ένα Λατινικό Τετράγωνο T τάξης $n_1 n_2$.*

Απόδειξη. Έστω $T_1 = (a_{i\,j})$ και $T_2 = (b_{r\,s})$. Κατασκευάζουμε έναν $n_1 n_2 \times n_1 n_2$ L πίνακα ως εξής: Αντικαθιστούμε κάθε στοιχείο $a_{i\,j}$ του T_1 με έναν πίνακα $n_2 \times n_2$, του οποίου τα στοιχεία είναι διατεταγμένα ζεύγη της μορφής $(a_{i\,j}, b_{r\,s})$, $r, s = 1, 2, \ldots, n_2$. Από τον τρόπο κατασκευής είναι προφανές ότι ο πίνακας που προκύπτει είναι πράγματι ένα Λατινικό Τετράγωνο τάξης $n_1 n_2$. ό.έ.δ.

Παράδειγμα 6.3.13. Έστω:

$$T_1 = \begin{array}{|c|c|}\hline 1 & 2 \\ \hline 2 & 1 \\ \hline \end{array} \quad \text{και} \quad T_2 = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}.$$

Σύμφωνα με τα παραπάνω το Λατινικό Τετράγωνο που κατασκευάζουμε είναι το:

$$T = \begin{array}{|c|c|c||c|c|c|}\hline 11 & 12 & 13 & 21 & 22 & 23 \\ \hline 12 & 13 & 11 & 22 & 23 & 21 \\ \hline 13 & 11 & 12 & 23 & 21 & 22 \\ \hline\hline 21 & 22 & 23 & 11 & 12 & 13 \\ \hline 22 & 23 & 21 & 12 & 13 & 11 \\ \hline 23 & 21 & 22 & 13 & 11 & 12 \\ \hline \end{array},$$

όπου, για λόγους συντομίας, στα διατεταγμένα ζεύγη έχουν παραληφθεί οι παρενθέσεις και τα κόμματα.

Μάλιστα, για καθαρά τυπικούς λόγους, θα μπορούσαμε να αντιστοιχίσουμε στα διατεταγμένα ζεύγη 11, 12, 13, 21, 22, 23, κατά σειρά τους αριθμούς 1, 2, 3, 4, 5, 6, οπότε το παραπάνω Λατινικό Τετράγωνο λαμβάνει την μορφή:

$$T = \begin{array}{|c|c|c|c|c|c|}\hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 2 & 3 & 1 & 5 & 6 & 4 \\ \hline 3 & 1 & 2 & 6 & 4 & 5 \\ \hline 4 & 5 & 6 & 1 & 2 & 3 \\ \hline 5 & 6 & 4 & 2 & 3 & 1 \\ \hline 6 & 4 & 5 & 3 & 1 & 2 \\ \hline \end{array}.$$

Παρατήρηση 6.3.14. Στο προηγούμενο λήμμα το πρώτο Λατινικό Τετράγωνο T_1 αποτελεί τον 'οδηγό', όπου σε κάθε θέση του (i, j) 'τοποθετείται' το T_2 και προκύπτει το Λατινικό Τετράγωνο T τάξης $n_1 n_2$.

Αν αλλάξουμε τους 'ρόλους' των δύο τετραγώνων και ως 'οδηγό' πάρουμε το T_2, όπου σε κάθε θέση του (i, j) 'τοποθετείται' το T_1 προκύπτει ένα άλλο Λατινικό Τετράγωνο, έστω $\overline{T}$, της ιδίας τάξης $n_2 n_1$. Οπότε γεννάται το ερώτημα τι σχέση έχουν τα δύο Λατινικά Τετράγωνα;

Να επαναλάβετε το προηγούμενο παράδειγμα αλλάζοντας τους ρόλους των δύο τετραγώνων.

Λήμμα 6.3.15. *Υποθέτουμε ότι υπάρχουν, ένα ζεύγος N_1, M_1 MOLS με τάξη m και ένα ζεύγος N_2, M_2 MOLS με τάξη n. Τότε υπάρχει ένα ζεύγος N, M MOLS με τάξη ίση με mn.*

Απόδειξη. Από το προηγούμενο λήμμα με τα Λατινικά Τετράγωνα N_1 και N_2 κατασκευάζουμε ένα Λατινικό Τετράγωνο L τάξης mn. Όμοια με τα Λατινικά Τετράγωνα M_1 και M_2 κατασκευάζουμε ένα Λατινικό Τετράγωνο M τάξης mn. Από τον τρόπο κατασκευής των N και M έπεται άμεσα ότι τα τετράγωνα αυτά είναι αμοιβαίως ορθογώνια. ό.έ.δ.

Προφανώς, αν έχουμε Λατινικά Τετράγωνα με τάξεις $n_1, n_2, \ldots, n_k$, μπορούμε να εφαρμόσουμε κατ' επανάληψη την παραπάνω μέθοδο και να κατασκευάσουμε ένα Λατινικό Τετράγωνο με τάξη ίση με $n_1 \cdot n_2 \cdots n_k$.

Θεώρημα 6.3.16. *Για κάθε $n \not\equiv 2 mod 4$ υπάρχει (τουλάχιστον) ένα ζεύγος ορθογωνίων Λατινικών Τετραγώνων τάξης n.*

Απόδειξη. Από την υπόθεση ο n είναι είτε περιττός είτε πολλαπλάσιο του 4. Οπότε, αν $n = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}$ είναι η ανάλυση του n σε πρώτους παράγοντες, έχουμε ότι $p_i^{\lambda_i} \geq 3$ για κάθε i. Επομένως, από το Θεώρημα 6.3.9 υπάρχει (τουλάχιστον) ένα ζεύγος MOLS με τάξη ίση με $p_i^{\lambda_i}$ για κάθε i. Συνεπώς, επαναληπτική εφαρμογή του προηγουμένου λήμματος μας δίνει ένα ζεύγος MOLS με τάξη ίση με n. ό.έ.δ.

Η Περίπτωση $n \equiv 2 \mathrm{mod} 4$ είναι ιδιάζουσα (ιδέ Σχόλια). Εδώ παραθέτουμε ένα Θεώρημα χωρίς απόδειξη.

Θεώρημα 6.3.17. *Για όλα τα n, εκτός από $n = 2$ ή $n = 6$, υπάρχει (τουλάχιστον) ένα ζεύγος MOLS τάξης n.*

Πόρισμα 6.3.18. *Για κάθε q διαφορετικό από το 2 και το 6 ισχύει ότι $A_q(4, 3) = q^2$.*

Απόδειξη. Η απόδειξη είναι άμεση από το προηγούμενο θεώρημα, το Θεώρημα 6.3.8 και το γεγονός ότι στην περίπτωση αυτή ικανοποιείται το φράγμα Singleton (ιδέ Θεώρημα 1.5.21). ό.έ.δ.

Σχόλια 6.3.19. 1. Στο Θεώρημα 6.3.9 αποδεικνύεται ότι το μέγιστο πλήθος $N(n)$ των αμοιβαίως ορθογωνίων Λατινικών Τετραγώνων τάξης n, στην περίπτωση όπου ο n είναι δύναμη ενός πρώτου, ισούται με $n-1$. Υπάρχει η εικασία ότι ισχύει και το αντίστροφο.

The prime Power Conjecture: Για $n \geq 2$ ισχύει $N(n) = n-1$, αν και μόνο αν ο n είναι δύναμη ενός πρώτου αριθμού.

2. Στο Θεώρημα 6.3.16 αποδεικνύεται ότι για κάθε $n \not\equiv 2 \bmod 4$ υπάρχει (τουλάχιστον) ένα ζεύγος αμοιβαίως ορθογωνίων Λατινικών Τετραγώνων τάξης n.

   Στην περίπτωση όπου $n \equiv 2 \bmod 4$ είχε διατυπωθεί από τον Euler η εικασία ότι $N(n) = 1$.

   Προφανώς έχουμε ότι $N(2) = 1$. Για $n = 6$ η εικασία απεδείχθει ότι ισχύει (δηλαδή $N(6) = 1$) για πρώτη φορά το 1900 από τον Tarry. Αξιοσημείωτο για την εποχή γεγονός, δεδομένου ότι τότε δεν υπήρχαν ηλεκρονικοί υπολογιστές και το πλήθος L_6 των Λατινικών Τετραγώνων τάξης 6 ισούται με $L_6 \approx 8 \cdot 10^8$. Μια σύντομη και κομψή απόδειξη ότι $N(6) = 1$ έχει δοθεί το 1984 από τον D. R. Stinson.

   Πολύ αργότερα, το 1959, εδόθη ένα αντιπαράδειγμα από τους R. C. Bose και S. S. Shrikhande, όπου αποδεικνύεται ότι $N(22) \geq 2$. Όπως επίσης, το 1960, ο E. T. Parker έδωσε ένα αντιπαράδειγμα, όπου αποδεικνύεται ότι $N(10) \geq 2$. Αυτά τα δύο αντιπαραδείγματα αποδεικνύουν ότι η εικασία του Euler δεν ισχύει. Αμέσως μετά, το 1960, οι R. C. Bose, S. S. Shrikhande και E. T. Parker απέδειξαν το Θεώρημα 6.3.17, που προαναφέραμε.

3. Η μελέτη της σχέσης Λατινικών Τετραγώνων και Κωδίκων φυσικά δεν εξαντλείται στα προηγούμενα. Εδώ απλώς, όπως επισημαίνεται και στην αρχή της παραγράφου, γίνεται μια νύξη, της οποίας σκοπός είναι

να αποτελέσει ερέθισμα για περαιτέρω μελέτη από τον ενδιαφερόμενο αναγνώστη.

6.3.1 Ασκήσεις

1. Να απαντήσετε σε όλα τα *γιατί;*, τα οποία συναντήσατε κατά την μελέτη της παραγράφου αυτής.
2. Να κατασκευάσετε ένα Λατινικό Τετράγωνο, το οποίο δεν έχει ορθογώνιο *ταίρι*.
3. Δείξτε ότι για κάθε περιττό πρώτο p υπάρχει κώδικας επί του $\mathbb{Z}_2$ με παραμέτρους $(4,\, p^2,\, 3)$.
4. Θεωρήστε τον δυϊκό $\mathcal{H}(2,\, 5)^{\perp}$ κώδικα Hamming για να κατασκευάσετε ένα σύνολο από τέσσερα MOLS με τάξη ίση με 5.
5. Να δείξετε ότι $A_{20}(5,\, 4) = 400$.

Βιβλιογραφία

Anderson, I. *"A first course in Combinatorial Mathematics"*. Oxford University Prees, 2000.

Berlekamp, E. R. *"Algebraic Coding Theory"*. Laguna Hills, CA: Aegean Park Press, 1984.

Hamming, R. *"Coding and Information Theory"*. Prentice-Hall, Englewood Cliffs 2^{nd} Edition, 1986.

Hill, R. *"A First Course in Coding Theory"*. Oxford University Press, Oxford, 1986.

Huffman, C. W. and Pless, V. . *"Fundamentals of Error-Correcting Codes"*. Cambridge University Press, 2003.

MacWilliams, F.J. and Sloane, N.J.A. *"The Theory of Error-correcting Codes"*. North-Holland, Amsterdam, 1977.

Mullen, G. L. and Mummert C. *"Finite Fields and Applications"*, volume 41 of *Student Mathematical Library*. AMS, 2007.

Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*. Wiley, New York, 1998.

van Lint, J.H. *"Introduction to Coding Theory"*. Springer-Verlag, 1999.

vanLint, J.H. and Wilson, R.M. *"A course in Combinatorics"*. Cambridge University Prees , 2001.

ΠΑΡΑΡΤΗΜΑ Α΄

Στοιχεία από την Άλγεβρα

Στο Παράρτημα αυτό, το οποίο παρατίθεται για να συμβάλει στην αυτοδυναμία του βιβλίου, ο αναγνώστης θα μπορεί να προστρέχει για αρωγή σε έννοιες και αποτελέσματα που θα συναντά κατά τη μελέτη του πρώτου μέρους. Σε **καμιά** περίπτωση δεν πρέπει να θεωρηθεί ως μια (έστω) σύντομη εισαγωγή σε θέματα Άλγεβρας.

Θεωρούμε γνωστές τις έννοιες της σχέσης ισοδυναμίας, του σώματος, του διανυσματικού χώρου, του δακτυλίου των πολυωνύμων με συντελεστές από ένα σώμα, καθώς και τη στοιχειώδη αριθμητική των ακεραίων $\mod n$.[1]

Ο ενδιαφερόμενος αναγνώστης μπορεί **και** πρέπει να ανατρέχει στη σχετική βιβλιογραφία (Ελληνόγλωσση και ξενόγλωσση) για περαιτέρω μελέτη σε Αλγεβρικά θέματα, γεγονός που θα τον βοηθήσει να κατανοήσει σε αρκετό βάθος έννοιες του πρώτου μέρους.

[1] Εδώ απλώς θα υπενθυμίσουμε, σε ορισμένες περιπτώσεις, τους βασικούς ορισμούς και θα παραθέσουμε μερικές ιδιότητες.

Α΄.1 Δακτύλιοι

Α΄.1.1 Ορισμοί και ιδιότητες

Ως γνωστόν, ένας δακτύλιος $(\mathrm{R},\, +,\, \cdot)$ είναι ένα μη κενό σύνολο R εφοδιασμένο με δύο πράξεις. Την πρόσθεση και τον πολλαπλασιασμό που πληρούν τις εξής ιδιότητες:

1. Ως προς την πρόσθεση είναι αβελιανή ομάδα, δηλαδή:

   (α΄) $a + (b + c) = (a + b) + c$, για όλα τα $a,\, b,\, c \in \mathrm{R}$.
   (Η πρόσθεση είναι προσεταιριστική.)

   (β΄) Υπάρχει $0 \in \mathrm{R}$, έτσι ώστε $0 + a = a + 0$ για κάθε $a \in \mathrm{R}$.
   (Υπαρξη ουδετέρου ως προς την πρόσθεση.)

   (γ΄) Για κάθε $a \in \mathrm{R}$ υπάρχει $-a \in \mathrm{R}$, έτσι ώστε $a+(-a) = (-a)+a = 0$.
   (Υπαρξη αντιθέτου ως προς την πρόσθεση.)

   (δ΄) $a + b = b + a$ για όλα τα $a,\, b \in \mathrm{R}$.

2. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ για όλα τα $a,\, b,\, c \in \mathrm{R}$.
   (Ο πολλαπλασιασμός είναι προσεταιριστικός.)

3. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ και $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ για όλα τα $a,\, b,\, c \in \mathrm{R}$.
   (Ο πολλαπλασιασμός είναι επιμεριστικός ως προς την πρόσθεση.)

Γνωστά παραδείγματα δακτυλίων είναι:

1. Ο δακτύλιος των ακεραίων $(\mathbb{Z},\, +,\, \cdot)$ με τις γνωστές πράξεις, πρόσθεση και πολλαπλασιασμό, των ακεραίων αριθμών.

2. Ο δακτύλιος $\mathbb{R}[x]$ των πολυωνύμων με συντελεστές πραγματικούς αριθμούς και πράξεις την πρόσθεση και πολλαπλασιασμό πολυωνύμων.

3. Ο δακτύλιος $M_n(\mathbb{R})$ των τετραγωνικών $n \times n$ πινάκων με στοιχεία πραγματικούς αριθμούς και πράξεις την πρόσθεση και πολλαπλασιασμό πινάκων.

Γενικά για κάθε δακτύλιο $(\mathrm{R}, +, \cdot)$ ορίζονται οι αντίστοιχοι δακτύλιοι $\mathrm{R}[x]$ και $M_n(\mathrm{R})$ με τις αντίστοιχες πράξεις.

Ένα άλλο παράδειγμα δακτυλίου, το οποίο θα μας απασχολήσει ιδιαιτέρως, είναι ο δακτύλιος $(\mathbb{Z}_m, +, \cdot)$ των ακεραίων $\mod m$ για έναν θετικό ακέραιο m.

Υπενθυμίζουμε πώς ορίζεται ο δακτύλιος $(\mathbb{Z}_m, +, \cdot)$. Έστω m ένας θετικός ακέραιος. Στο σύνολο των ακεραίων αριθμών ορίζουμε μια σχέση $\sim$ ως εξής:

$$a \sim b, \text{ αν και μόνο αν ο } m \text{ διαιρεί τη διαφορά } a - b.$$

Δεν είναι δύσκολο να δούμε ότι η σχέση $\sim$ είναι μια σχέση ισοδυναμίας, η οποία διαμερίζει το σύνολο των ακεραίων σε κλάσεις ισοδυναμίας. Η κλάση ισοδυναμίας ενός ακεραίου αριθμού a είναι το σύνολο:

$$\begin{aligned}
[a] &= \{\, r \in \mathbb{Z}, \mid r \sim a \,\} \\
&= \{\, r \in \mathbb{Z} \mid \text{το } m \text{ διαιρεί τη διαφορά } a - r \,\} \\
&= \{\, a + ms \mid s \in \mathbb{Z} \,\}.
\end{aligned}$$

Υπάρχουν τόσες κλάσεις ισοδυναμίας όσα και τα δυνατά υπόλοιπα της διαίρεσης ενός ακεραίου με τον m (γιατί;). Δηλαδή έχουμε τις κλάσεις $[0]$, $[1], \ldots,$ $[m-1]$, οι οποίες θα ονομάζονται **κλάσεις υπολοίπων** $\mod m$. Δύο ακέραιοι αριθμοί a, b, οι οποίοι βρίσκονται στην ίδια κλάση ισοδυναμίας, θα λέγονται ισότιμοι ως προς μέτρο m και συμβολίζουμε $a \equiv b(\mod m)$.

Το σύνολο $\mathbb{Z}_m = \{\, [0], [1], \ldots, [m-1] \,\}$ όλων των κλάσεων υπολοίπων $\mod m$ είναι οι ακέραιοι $\mod m$. Στο $\mathbb{Z}_m$ ορίζουμε δύο πράξεις. Μια πρόσθεση και έναν πολλαπλασιασμό ως εξής:

$$[a] + [b] = [a + b] \text{ και } [a] \cdot [b] = [a \cdot b].$$

Προσοχή! Τα σύμβολα $+$ και $\cdot$ χρησιμοποιούνται διττά, μια φορά συμβολίζουν πράξεις στο σύνολο $\mathbb{Z}_m$ και μια φορά στο σύνολο των ακεραίων $\mathbb{Z}$. Αυτό δεν (πρέπει να) δημιουργεί σύγχυση.

Άσκηση. Αποδείξτε ότι οι δύο πράξεις που ορίσαμε είναι "καλά ορισμένες", δηλαδή αν $[a_1] = [a_2]$, $[b_1] = [b_2]$, τότε $[a_1] + [b_1] = [a_2] + [b_2]$ και

$[a_1] \cdot [b_1] = [a_2] \cdot [b_2]$. Με διαφορετικά λόγια, οι πράξεις δεν εξαρτώνται από την επιλογή των αντιπροσώπων.

Άσκηση. Αποδείξτε ότι το σύνολο $(\mathbb{Z}_m, +, \cdot)$ με τις πράξεις που ορίσαμε προηγουμένως είναι δακτύλιος.

Παρατηρήσεις Α΄.1.1. 1. Ο τρόπος που ορίσαμε τις πράξεις στο σύνολο $\mathbb{Z}_m$ "υπαγορεύει" έναν εύκολο τρόπο να εκτελούμε τις πράξεις. Έστω ότι έχουμε να προσθέσουμε/πολλαπλασιάσουμε το $[a]$ με το $[b]$, τότε προσθέτουμε/πολλαπλασιάζουμε το a με το b στους ακεραίους, το αποτέλεσμα που βρίσκουμε το διαιρούμε με τον m και το υπόλοιπο $\mod m$ που προκύπτει είναι το αποτέλεσμα της πρόσθεσης/πολλαπλασιασμού του $[a]$ με το $[b]$.

Για παράδειγμα, έστω $[3], [5] \in \mathbb{Z}_6$, τότε $[3] + [5] = [8 = 6 + 2] = [2]$ και $[3] \cdot [5] = [15 = 2 \cdot 6 + 3] = [3]$.

2. Πολλές φορές, όταν δεν υπάρχει ενδεχόμενο σύγχυσης, κάθε κλάση υπολοίπων $\mod m$ $[a]$ την ταυτίζουμε με τον αντίστοιχο αντιπρόσωπο a και γράφουμε $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$.

Ένας δακτύλιος $(\mathrm{R}, +, \cdot)$ θα λέγεται **μεταθετικός** αν ισχύει $r \cdot s = s \cdot r$ για όλα τα $r, s \in \mathrm{R}$.

Αν σε ένα δακτύλιο $(\mathrm{R}, +, \cdot)$ υπάρχει ουδέτερο ως προς τον πολλαπλασιασμό, δηλαδή υπάρχει $e \in \mathrm{R}$, τέτοιο ώστε $e \cdot r = r \cdot e = r$ για κάθε $r \in \mathrm{R}$, τότε ο δακτύλιος ονομάζεται δακτύλιος με **μονάδα** και το e τις περισσότερες φορές συμβολίζεται με 1_{R} (ή απλά 1).

Σε όλα τα προηγούμενα παραδείγματα οι δακτύλιοι είναι μεταθετικοί με μονάδα. Εκτός από τον δακτύλιο $M_n(\mathrm{R})$, ο οποίος έχει μονάδα μόνο αν ο δακτύλιος R έχει μονάδα και δεν είναι μεταθετικός για $n > 1$, ακόμα και αν ο δακτύλιος R είναι μεταθετικός.

Σε έναν δακτύλιο R με μονάδα ένα στοιχείο a θα λέμε ότι έχει **αντίστοφο** (ή ότι το a είναι αντιστρέψιμο), αν υπάρχει $a^{-1} \in \mathrm{R}$, έτσι ώστε $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Έστω $U(\mathrm{R})$ το σύνολο των αντιστρεψίμων στοιχείων ενός δακτυλίου R.

Άσκηση. Αποδείξτε ότι το γινόμενο δύο αντιστρεψίμων στοιχείων είναι αντιστρέψιμο στοιχείο και ότι το $U(\mathrm{R})$ με πράξη τον πολλαπλασιασμό είναι ομάδα, η **πολλαπλασιαστική ομάδα** του δακτυλίου R.

Προφανώς $U(\mathbb{Z}) = \{1, -1\}$ και $U(M_n(\mathbb{R})) = \{\mathrm{A} \in M_n(\mathbb{R}) \mid det(\mathrm{A}) \neq 0\}$.

Άσκηση. Αποδείξτε ότι η πολλαπλασιαστική ομάδα του δακτυλίου των πολυωνύμων $\mathbb{R}[x]$ αποτελείται από τα σταθερά μη μηδενικά πολυώνυμα.

Πρόταση Α΄.1.2. *Έστω m θετικός ακέραιος, το στοιχείο $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμο, αν και μόνο αν ο a είναι πρώτος προς τον m. Δηλαδή*

$$U(\mathbb{Z}_m) = \{[a] \in \mathbb{Z}_m \mid \mu\kappa\delta(a, m) = 1\}.$$

Απόδειξη. Υποθέτουμε ότι το $[a] \in \mathbb{Z}_m$ είναι αντιστρέψιμο, δηλαδή υπάρχει $[b] \in \mathbb{Z}_m$ έτσι ώστε $[a] \cdot [b] = [1]$. Αυτό σημαίνει ότι $ab \equiv 1(\mod m)$, δηλαδή ο m διαιρεί τη διαφορά $ab - 1$. Συνεπώς, υπάρχει ακέραιος k, τέτοιος ώστε $ab - 1 = mk$, δηλαδή $ab - mk = 1$ απ' όπου έπεται ότι ο μέγιστος κοινός διαιρέτης των a και m ισούται με 1.

Αντίστροφα, υποθέτουμε ότι ο a είναι πρώτος προς τον m, τότε υπάρχουν ακέραιοι k, n, έτσι ώστε $ak + mn = 1$[2]. Από την τελευταία σχέση έπεται ότι $ak \equiv 1 \mod m$, δηλαδή $[a][k] = [1]$, άρα το $[a]$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_m$. ό.έ.δ.

Το πλήθος των στοιχείων της πολλαπλασιαστικής ομάδας $U(\mathbb{Z}_m)$ συμβολίζεται με $\varphi(m)$. Η συνάρτηση φ είναι η γνωστή συνάρτηση Euler, της οποίας η τιμή $\varphi(n)$ για κάθε θετικό ακέραιο αριθμό n είναι ίση με το πλήθος των ακεραίων μεταξύ του 1 και του n, οι οποίοι είναι πρώτοι προς τον n.

Για ιδιότητες της συνάρτησης του Euler παραπέμπουμε σε κάθε εγχειρίδιο της Θεωρίας Αριθμών.

Ένα ερώτημα που προκύπτει είναι κατά πόσον η ομάδα $U(\mathbb{Z}_m)$ είναι κυκλική. Προσπαθήστε να αποδείξετε την ακόλουθη άσκηση.

[2]Εδώ χρησιμοποιούμε (χωρίς απόδειξη) το εξής βασικό θεώρημα της Θεωρίας Αριθμών: Έστω α, β ακέραιοι αριθμοί όχι και οι δύο ίσοι με μηδέν, τότε υπάρχουν ακέραιοι κ, λ, έτσι ώστε $\mu\kappa\delta(\alpha, \beta) = \alpha\kappa + \beta\lambda$. Βλέπε για παράδειγμα στο Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη [2013], παρ. 1.2.

Άσκηση. Δείξτε ότι η πολλαπλασιαστική όμαδα $U(\mathbb{Z}_m)$ είναι κυκλική, αν και μόνο αν $m = 2,\, 4,\, p^k,\, 2p^k$, όπου p είναι ένας περιττός πρώτος.

Ένα μη κενό υποσύνολο S ενός δακτυλίου R θα λέγεται **υποδακτύλιος**, αν είναι δακτύλιος ως προς την πρόσθεση και τον πολλαπλασιασμό του δακτυλίου R. Δηλαδή το S είναι υποομάδα ως προς την πρόσθεση και $a \cdot b \in \mathrm{S}$ για κάθε $a,\, b \in \mathrm{S}$.

Επισημαίνουμε ότι το μηδέν (το ουδέτερο της πρόσθεσης) ενός δακτυλίου ανήκει σε **κάθε** υποδακτύλιο (γιατί;). Για την μονάδα (το ουδέτερο του πολλαπλασιασμού) δεν ισχύει κάτι ανάλογο.

1. Ο δακτύλιος των ακεραίων έχει μονάδα. Έστω m ένας θετικός ακέραιος μεγαλύτερος του 1, το σύνολο $m\mathbb{Z} = \{\, m \cdot r \mid r \in \mathbb{Z} \,\}$ είναι υποδακτύλιος του $\mathbb{Z}$, αλλά δεν έχει μονάδα ως προς τον πολλαπλασιασμό.

2. Το σύνολο:
$$\mathrm{R} = \left\{ \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix} \mid r \in \mathbb{Z} \right\}$$
αποτελεί υποδακτύλιο του δακτυλίου $M_2(\mathbb{Z})$ των τετραγωνικών 2×2 πινάκων με στοιχεία ακεραίους αριθμούς. Ο R έχει ως μονάδα τον πίνακα:
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$
ενώ ο $M_2(\mathbb{Z})$ έχει ως μονάδα τον πίνακα:
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Σε έναν δακτύλιο R ένα μη μηδενικό στοιχείο a θα λέγεται **διαιρέτης του μηδενός**, αν υπάρχουν μη μηδενικά $b,\, c \in \mathrm{R}$ έτσι ώστε $ab = ca = 0$.

Άσκηση. Δείξτε ότι σε έναν δακτύλιο με μονάδα ένα αντιστρέψιμο στοιχείο δεν είναι διαιρέτης του μηδενός.

Ένας μεταθετικός δακτύλιος με μονάδα και δύο τουλάχιστον στοιχεία θα λέγεται **ακεραία περιοχή**, αν δεν έχει διαιρέτες του μηδενός.

Ο δακτύλιος των ακεραίων είναι, προφανώς, ακεραία περιοχή.

Άσκηση. Δείξτε ότι ο δακτύλιος $\mathbb{R}[x]$ των πολυωνύμων με πραγματικούς συντελεστές είναι ακεραία περιοχή.

Γενικά, δείξτε ότι, αν R είναι ένας δακτύλιος, ο $\mathrm{R}[x]$ είναι ακεραία περιοχή, αν και μόνο αν ο R είναι ακεραία περιοχή.

Ο δακτύλιος όμως $M_n(\mathrm{R})$ δεν είναι ακεραία περιοχή για $n > 1$. Για παράδειγμα, για τους πίνακες:

$$\mathrm{A} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{και} \quad \mathrm{B} = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$$

έχουμε ότι $\mathrm{B} \cdot \mathrm{A} = \mathbf{0}$.

Πρόταση Α΄.1.3. *Ο δακτύλιος $\mathbb{Z}_m$ είναι ακεραία περιοχή, αν και μόνο αν ο m είναι πρώτος αριθμός.*

Απόδειξη. Δίνουμε μια σκιαγράφηση της απόδειξης με τις λεπτομέρειες να αφήνονται ως άσκηση.

Αρκεί να παρατηρήσουμε ότι αν $m = a \cdot b$ με a, b διάφορα του 1, τότε τα $[a]$, $[b] \in \mathbb{Z}_m$ είναι διαιρέτες του μηδενός.

Αντίστροφα, αν τα $[a]$, $[b] \in \mathbb{Z}_m$ είναι διαιρέτες του μηδενός και ισχύει $[a] \cdot [b] = [0]$, τότε έχουμε ότι ο m διαιρεί το γινόμενο ab, οπότε αν ο m ήταν πρώτος, θα έπρεπε να διαιρεί (τουλάχιστον) έναν από τους a, b. Άρα, ένας από τους $[a]$, $[b]$ θα ήταν ίσος με $[0]$, άτοπο. ό.έ.δ.

Άσκηση. Να υπολογίσετε τους διαιρέτες του μηδενός στον δακτύλιο $\mathbb{Z}_m$.

Έστω R ένας δακτύλιος. Ο μικρότερος θετικός ακέραιος n (αν υπάρχει) με την ιδιότητα $nr = \underbrace{r + r + \cdots + r}_{n-\text{φορές}} = 0$ για ολα τα $r \in \mathrm{R}$ θα λέγεται **χαρακτηριστική** του δακτυλίου . Αν δεν υπάρχει θετικός ακέραιος με την παραπάνω ιδιότητα, τότε θα λέμε ότι η χαρακτηριστική του δακτυλίου ισούται με μηδέν.

Προφανώς η χαρακτηριστική του δακτυλίου $\mathbb{Z}$ των ακεραίων είναι ίση με μηδέν. Ενώ η χαρακτηριστική του δακτυλίου $\mathbb{Z}_m$ είναι ίση με m.

Πρόταση Α΄.1.4. *Η χαρακτηριστική μιας ακεραίας περιοχής D είναι είτε μηδέν είτε πρώτος αριθμός.*

Απόδειξη. Υποθέτουμε ότι η χαρακτηριστική της D δεν είναι μηδέν και είναι ίση με m. Παρατηρούμε ότι ο m είναι ο ελάχιστος θετικός ακέραιος, τέτοιος ώστε $m1 = 0$. Πράγματι, αν υπήρχε $0 < n < m$ με $n1 = 0$, τότε για κάθε $a \in D$ θα είχαμε ότι $na = (n1) \cdot a = 0$. Αυτό είναι άτοπο από τον ορισμό της χαρακτηριστικής.

Αν ο m είναι σύνθετος, τότε θα έχουμε $m = r \cdot s$ με $1 < r,\ s < m$. Οπότε $(r1) \cdot (s1) = (r \cdot s)1 = m1 = 0$ και επειδή η D είναι ακεραία περιοχή έχουμε ότι $r1 = 0$ ή $s1 = 0$, άτοπο από τα προηγούμενα. ό.έ.δ.

Ένας μεταθετικός δακτύλιος $\mathbb{F}$ με μονάδα όπου κάθε μη μηδενικό στοιχείο του έχει αντίστροφο λέγεται **σώμα** . Δηλαδή η πολλαπλασιαστική ομάδα ενός σώματος αποτελείται από όλα τα μη μηδενικά στοιχεία του.

Τα σύνολα $\mathbb{Q}$ των ρητών, $\mathbb{R}$ των πραγματικών και $\mathbb{C}$ των μιγαδικών αριθμών είναι σώματα με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού.

Προφανώς, κάθε σώμα είναι ακεραία περιοχή. Το αντίστροφο, προφανώς, δεν ισχύει, αφού ο δακτύλιος των ακεραίων είναι ακεραία περιοχή, αλλά δεν είναι σώμα.

Αν η ακεραία περιοχή είναι πεπερασμένη, τότε ισχύει και το αντίστροφο. Συγκεκριμμένα έχουμε:

Πρόταση Α΄.1.5. *Κάθε πεπερασμένη ακεραία περιοχή D είναι σώμα.*

Απόδειξη. Για κάθε $0 \neq a \in D$ και κάθε θετικό ακέραιο λ οι δυνάμεις a^λ είναι στοιχεία της D και επειδή η D είναι πεπερασμένη υπάρχουν $\kappa,\ \lambda$ θετικοί ακέραιοι με $\kappa < \lambda$ και $a^\kappa = a^\lambda$. Δηλαδή έχουμε ότι $a^\kappa - a^\lambda = 0$, οπότε έχουμε $a^\kappa(1 - a^{\lambda-\kappa}) = 0$. Επειδή η D είναι ακεραία περιοχή, έχουμε ότι $1 - a^{\lambda-\kappa} = 0$. Από την τελευταία σχέση έχουμε ότι $a^{\lambda-\kappa} = 1$, απ' όπου έπεται ότι το a είναι αντιστρέψιμο στοιχείο. ό.έ.δ.

Ανακεφαλαιώνοντας τα προηγούμενα, μπορούμε να αποδείξουμε:

1. Ένα μη μηδενικό στοιχείο του δακτυλίου $\mathbb{Z}_m$ είναι διαιρέτης του μηδενός, αν και μόνο αν δεν είναι αντιστρέψιμο.

2. Ο δακτύλιος $\mathbb{Z}_m$ είναι ακεραία περιοχή, αν και μόνο αν ο m είναι πρώτος, αν και μόνο αν ο $\mathbb{Z}_m$ είναι σώμα.

Α΄.1.2 Ομομορφισμοί-Ιδεώδη

Έστω R_1 και R_2 δύο δακτύλιοι. Μια απεικόνιση $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ θα λέγεται **ομομορφισμός δακτυλίων**, αν για όλα τα $a, b \in \mathrm{R}_1$ ισχύει:

1. $f(a+b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$

Δηλαδή ένας ομομορφισμός δακτυλίων " διατηρεί" τις πράξεις των δακτυλίων.

Η απεικόνιση $\vartheta : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ με $\vartheta(r) = 0$ για κάθε $r \in \mathrm{R}_1$ είναι προφανώς ένας ομομορφισμός δακτυλίων, ο **τετριμμένος ομομορφισμός**.

Επίσης η απεικόνιση $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(a) = [a]$ για κάθε $a \in \mathbb{Z}$ είναι προφανώς ένας ομομορφισμός δακτυλίων, ο **φυσικός ομομορφισμός**.

Στη συνέχεια, θα μας δοθεί η ευκαιρία να δούμε περισσότερα παραδείγματα ομομορφισμών δακτυλίων.

Έστω $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ ένας ομομορφισμός δακτυλίων. Τότε ισχύει $f(0) = 0$ (γιατί;).

Το σύνολο $f(\mathrm{R}_1) = \{\, f(a) \in \mathrm{R}_2 \mid a \in \mathrm{R}_1 \,\}$ είναι υποδακτύλιος του R_2 (γιατί;), συνήθως συμβολίζεται με $\mathrm{Im}f$ και ονομάζεται **δακτύλιος εικόνα**.

Όταν η απεικόνιση f είναι επί, δηλαδή $\mathrm{Im}f = \mathrm{R}_2$, η f ονομάζεται **επιμορφισμός**.

Το σύνολο $\{\, r \in \mathrm{R}_1 \mid f(r) = 0 \,\}$ ονομάζεται **πυρήνας** του f και συμβολίζεται $\mathrm{Ker}f$.

Ο φυσικός ομομορφισμός $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ με $\varphi(a) = [a]$ είναι προφανώς επί και έχει πυρήνα $\mathrm{Ker}\varphi = \{\, mr \mid r \in \mathbb{Z} \,\}$ (γιατί;)

Προφανώς ο πυρήνας του τετριμμένου ομομορφισμού $\vartheta : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ με $\vartheta(r) = 0$ για κάθε $r \in \mathrm{R}_1$ είναι όλος ο δακτύλιος R_1.

Πρόταση Α΄.1.6. *Ο ομομορφισμός δακτυλίων $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ είναι 1-1, αν και μόνο αν $\mathrm{Ker}f = \{\, 0 \,\}$.*

Απόδειξη. Για $a, b \in \mathrm{R}_1$ ισχύει $f(a) = f(b)$, αν και μόνο αν $f(a) - f(b) = f(a - b) = 0$, αν και μόνο αν $a - b \in \mathrm{Ker}f$. Οπότε η συνέχεια έπεται εύκολα. ό.έ.δ.

Αν ένας ομομορφισμός δακτυλίων είναι 1-1, τότε ονομάζεται **μονομορφισμός**. Αν είναι 1-1 και επί, ονομάζεται **ισομορφισμός**.

Έστω $(\mathrm{R}, +, \cdot)$ ένας δακτύλιος και I ένα μη κενό υποσύνολο του R. Το I θα λέγεται **ιδεώδες** του R (και θα συμβολίζουμε $\mathrm{I} \lhd \mathrm{R}$) αν ισχύουν τα εξής:

i) $a - b \in \mathrm{I}$, για όλα τα $a, b \in \mathrm{I}$.

ii) $r \cdot a,\ a \cdot r \in \mathrm{I}$, για όλα τα $a \in \mathrm{I}$ και $r \in \mathrm{R}$.

Προφανώς, το σύνολο $\{ 0 \}$ που αποτελείται μόνο από το μηδέν είναι ιδεώδες και ονομάζεται το **μηδενικό** ή το τετριμμένο ιδεώδες. Επίσης ολόκληρος ο δακτύλιος R είναι ιδεώδες του εαυτού του. Ένα ιδεώδες I με $\{ 0 \} \neq \mathrm{I} \neq \mathrm{R}$ θα λέγεται **γνήσιο** ιδεώδες.

Όπως βλέπουμε ένα ιδεώδες είναι "κάτι περισσότερο" από υποδακτύλιος.

Για παράδειγμα στον δακτύλιο $\mathbb{Q}[x]$ όλων των πολυωνύμων με ρητούς συντελεστές το σύνολο $\mathbb{Z}[x]$ όλων των πολυωνύμων με ακεραίους συντελεστές είναι υποδακτύλιος, αλλά δεν είναι ιδεώδες (γιατί;). Ενώ το σύνολο K όλων των πολυωνύμων με μηδενικό σταθερό όρο είναι ιδεώδες (γιατί;)

Άσκηση. Στον δακτύλιο των ακεραίων $\mathbb{Z}$ να αποδείξετε ότι για κάθε ιδεώδες I υπάρχει ένας θετικός ακέραιος m έτσι ώστε $\mathrm{I} = m\mathbb{Z} = \{ m \cdot r \mid r \in \mathbb{Z} \}$. Υπόδειξη: Δείξτε ότι (στην περίπτωση που το I είναι μη μηδενικό) ο μικρότερος θετικός ακέραιος $m \in \mathrm{I}$ διαιρεί κάθε άλλο στοιχείο του I.

Έστω $\mathrm{I}_1, \mathrm{I}_2$ ιδεώδη του δακτυλίου R. Τότε μπορούμε εύκολα να αποδείξουμε ότι η τομή $\mathrm{I}_1 \cap \mathrm{I}_2$ είναι ιδεώδες του R.

Άσκηση. Να αποδείξετε ότι αν $\mathrm{I}_1 = \{ m \cdot r \mid r \in \mathbb{Z} \}$ και $\mathrm{I}_2 = \{ n \cdot r \mid r \in \mathbb{Z} \}$ είναι δύο ιδεώδη του δακτυλίου των ακεραίων, τότε $\mathrm{I}_1 \cap \mathrm{I}_2 = \{ k \cdot r \mid r \in \mathbb{Z} \}$, όπου k είναι το ελάχιστο κοινό πολλαπλάσιο των m και n.

Όπως εύκολα μπορούμε να διαπιστώσουμε, η ένωση δύο ιδεωδών δεν είναι κατ' ανάγκην ιδεώδες.

Άσκηση. Να αποδείξετε ότι η ένωση $\mathrm{I}_1 \cup \mathrm{I}_2$ είναι ιδεώδες του R, αν και μόνο αν $\mathrm{I}_1 \subseteq \mathrm{I}_2$ ή $\mathrm{I}_1 \supseteq \mathrm{I}_2$.

Έστω R ένας δακτύλιος και $S \subseteq \mathrm{R}$. Η τομή όλων των ιδεωδών του R που περιέχουν το υποσύνολο S είναι το μικρότερο ιδεώδες του R που περιέχει το υποσύνολο S, ονομάζεται **ιδεώδες παραγόμενο** από το υποσύνολο S και συμβολίζεται με $\langle S \rangle$. Δηλαδή $\langle S \rangle = \bigcap \{ \mathrm{I} \mid \mathrm{I} \lhd \mathrm{R} \textit{ και } S \subseteq \mathrm{I} \}$.

Έστω I_1, I_2 δύο ιδεώδη του δακτυλίου R, Δεν είναι δύσκολο να αποδείξουμε ότι $\langle \mathrm{I}_1 \cup \mathrm{I}_2 \rangle = \{ a+b \mid a \in \mathrm{I}_1,\ b \in \mathrm{I}_2 \}$. Για τον λόγο αυτό, το ιδεώδες $\{ a+b \mid a \in \mathrm{I}_1,\ b \in \mathrm{I}_2 \}$ το συμβολίζουμε με $\mathrm{I}_1 + \mathrm{I}_2$ και το ονομάζουμε **άθροισμα** των ιδεωδών I_1 και I_2.

Πρόταση Α΄.1.7. *Έστω* R *ένας μεταθετικός δακτύλιος με μονάδα και* $\emptyset \neq S \subseteq \mathrm{R}$, *τότε:*

$$\langle S \rangle = \{ a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\, s_i \in S,\, i = 1, 2, \ldots, \nu,\, \nu \geq 1 \}.$$

Απόδειξη. Το σύνολο:

$$\{ a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\, s_i \in S,\, i = 1, 2, \ldots, \nu,\, \nu \geq 1 \}$$

είναι ιδεώδες του R (γιατί;). Επίσης, το υποσύνολο S περιέχεται στο:

$$\{ a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\, s_i \in S,\, i = 1, 2, \ldots, \nu,\, \nu \geq 1 \}.$$

Επομένως, από τον ορισμό του $\langle S \rangle$ έχουμε ότι:

$$\langle S \rangle \subseteq \{ a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\, s_i \in S,\, i = 1, 2, \ldots, \nu,\, \nu \geq 1 \}.$$

Έστω τώρα I ένα ιδεώδες του R με $S \subseteq \mathrm{I}$. Από τον ορισμό του ιδεώδους έπεται ότι:

$$\{ a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\, s_i \in S,\, i = 1, 2, \ldots, \nu,\, \nu \geq 1 \} \subseteq \mathrm{I}.$$

Δηλαδή:

$$\{ a_1 s_1 + a_2 s_2 + \cdots + a_\nu s_\nu \mid a_i \in \mathrm{R},\, s_i \in S,\, i = 1, 2, \ldots, \nu,\, \nu \geq 1 \} \subseteq$$
$$\subseteq \bigcap \{ \mathrm{I} \mid \mathrm{I} \lhd \mathrm{R} \kappa\alpha\iota S \subseteq \mathrm{I} \} = \langle S \rangle$$

και τελειώσαμε.

ό.έ.δ.

Παρατηρήσεις Α΄.1.8. 1. Αν $S = \emptyset$, τότε προφανώς $\langle \emptyset \rangle = \{ 0 \}$, το μηδενικό ιδεώδες.

2. Στη γενική περίπτωση, όπου ο δακτύλιος δεν είναι κατ' ανάγκη μεταθετικός, ούτε έχει κατ' ανάγκη μονάδα, μπορούμε, επίσης, να περιγράψουμε τα στοιχεία ενός ιδεώδους που παράγεται από ένα υποσύνολο του δακτυλίου. Αρκεστήκαμε όμως στη μερική περίπτωση, διότι στα επόμενα θα ασχοληθούμε, χωρίς ιδιαίτερη μνεία, αποκλειστικά με μεταθετικούς δακτυλίους με μονάδα.

Ενδιαφέρον παρουσιάζει η περίπτωση που το υποσύνολο S αποτελείται από ένα στοιχείο. Αν R είναι ένας μεταθετικός δακτύλιος και $a \in \mathrm{R}$, τότε το ιδεώδες το παραγόμενο από το μονοσύνολο $\{\, a \,\}$ θα ονομάζεται **κύριο** και προφανώς ισχύει:

$$\langle \{a\} \rangle = \langle a \rangle = \{r \cdot a \mid r \in \mathrm{R}\}.$$

Προηγουμένως έχουμε δει ότι, αν I είναι ένα ιδεώδες του δακτυλίου των ακεραίων, τότε υπάρχει ένας θετικός ακέραιος m, έτσι ώστε:

$$\mathrm{I} = m\mathbb{Z} = \{m \cdot r \mid r \in \mathbb{Z}\}.$$

Δηλαδή το $\mathrm{I} = \langle\, m \,\rangle$ είναι κύριο. Άρα, κάθε ιδεώδες του δακτυλίου $\mathbb{Z}$ είναι κύριο. Γενικά αν σε ένα δακτύλιο κάθε ιδεώδες του είναι κύριο, τότε ο δακτύλιος θα ονομάζεται **δακτύλιος κυρίων ιδεωδών**. Στα επόμενα θα δούμε και άλλα παραδείγματα δακτυλίων κυρίων ιδεωδών.

Έστω R ένας δακτύλιος με μονάδα και I ένα ιδεώδες του. Υποθέτουμε ότι το $1 \in \mathrm{I}$. Τότε, προφανώς (από τον ορισμό του ιδεώδους) έχουμε ότι $\mathrm{I} = \mathrm{R}$.

Από την απλή αυτή παρατήρηση έπεται άμεσα ότι $\langle\, a \,\rangle = \mathrm{R}$, αν και μόνο αν το στοιχείο $a \in \mathrm{R}$ είναι αντιστρέψιμο (γιατί;).

Άσκηση. Δείξτε ότι σε ένα σώμα τα μόνα ιδεώδη του είναι το μηδενικό ιδεώδες και ολόκληρο το σώμα.

Έστω $f : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ ένας ομομορφισμός δακτυλίων. Υποθέτουμε ότι $a,\, b \in \mathrm{Ker} f$. Δεν είναι δύσκολο να δούμε ότι $a - b \in \mathrm{Ker} f$, όπως επίσης ότι για κάθε $r \in \mathrm{R}_1$ τα $r \cdot a,\ a \cdot r \in \mathrm{Ker} f$. Δηλαδή ισχύει η εξής πρόταση.

Πρόταση Α΄.1.9. *Ο πυρήνας ένος ομομορφισμού δακτυλίων είναι ιδεώδες του πεδίου ορισμού.*

Παράδειγμα Α΄.1.10. Έστω $\mathbb{F}[x]$ ο δακτύλιος των πολυωνύμων με συντελεστές από το σώμα $\mathbb{F}$ και $\varphi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]$ με $\varphi(a_n x^n + \cdot + a_1 x + a_0) = a_0$, δηλαδή η απεικόνιση φ απεικονίζει κάθε πολυώνυμο στον σταθερό του όρο. Δεν είναι δύσκολο να αποδείξουμε ότι η φ είναι ομομορφισμός δακτυλίων. Επίσης, μπορείτε να αποδείξετε ότι ο πυρήνας της φ αποτελείται από όλα τα πολυώνυμα με μηδενικό σταθερό πολυώνυμο. Επομένως, σύμφωνα με τα προηγούμενα, το σύνολο των πολυωνύμων με μηδενικό σταθερό όρο είναι ένα ιδεώδες του $\mathbb{F}[x]$.

Όπως θα δούμε αμέσως ισχύει και το αντίστροφο της προηγούμενης πρότασης, δηλαδή κάθε ιδεώδες είναι ο πυρήνας ενός ομομορφισμού δακτυλίων. Οπότε οι έννοιες πυρήνας ομομορφισμού και ιδεώδες είναι ταυτόσημες.

Έστω I ένα ιδεώδες του δακτυλίου R. Στον δακτύλιο R ορίζουμε μια σχέση $\sim$ ως εξής: $a \sim b$ αν και μόνο αν $a - b \in \mathrm{I}$.

Ως άσκηση μπορείτε να αποδείξετε ότι η σχέση $\sim$ είναι σχέση ισοδυναμίας. Ας υπολογίσουμε τις κλάσεις ισοδυναμίας. Η κλάση ισοδυναμίας του στοιχείου a είναι το σύνολο

$$\begin{aligned} C_a &= \{r \in \mathrm{R} \mid r - a \in \mathrm{I}\} \\ &= \{r \in \mathrm{R} \textit{για τα οποία υπάρχει } h \in \mathrm{I}, \textit{έτσι ώστε } r = a + h\} \\ &= \{a + h \mid h \in \mathrm{I}\}. \end{aligned}$$

Η κλάση $C_a = \{\, a+h \mid h \in \mathrm{I} \,\}$ ονομάζεται **σύμπλοκο** ή **κλάση υπολοίπων** του a ως προς το ιδεώδες I και συμβολίζεται $a + \mathrm{I}$.

Το σύνολο $\{\, a + \mathrm{I} \mid a \in \mathrm{R} \,\}$ όλων των συμπλόκων αποτελεί το σύνολο πηλίκων ως προς τη σχέση ισοδυναμίας $\sim$ και θα συμβολίζεται $\mathrm{R/I}$.

Με τη βοήθεια των πράξεων της πρόσθεσης και του πολλαπλασιασμού στον δακτύλιο R, στο σύνολο $\mathrm{R/I}$ ορίζουμε δύο πράξεις, μια πρόσθεση και έναν πολλαπλασιασμό ως εξής:

$$(a + \mathrm{I}) + (b + \mathrm{I}) = (a + b) + \mathrm{I} \quad \text{και} \quad (a + \mathrm{I}) \cdot (b + \mathrm{I}) = (a \cdot b) + \mathrm{I}.$$

Δεν είναι δύσκολο να αποδείξουμε ότι οι δύο πράξεις είναι καλά ορισμένες (δεν εξαρτώνται από την επιλογή των αντιπροσώπων).

Άσκηση. Να αποδείξετε ότι το σύνολο R/I με αυτές τις πράξεις αποτελεί δακτύλιο. (Το μηδέν, δηλαδή το ουδέτερο ως προς την πρόσθεση, είναι το σύμπλοκο $0+\mathrm{I}=\mathrm{I}$.) Ο δακτύλιος αυτός ονομάζεται **δακτύλιος πηλίκων** ως προς το ιδεώδες I.

Παρατήρηση Α΄.1.11. Ο δακτύλιος των ακεραίων $\mathbb{Z}_m$ των ακεραίων $\mod m$ (βλέπε σελίδα 389) είναι ο δακτύλιος πηλίκων $\mathbb{Z}/\langle m \rangle$.

Έστω $\varphi : \mathrm{R} \longrightarrow \mathrm{R}/\mathrm{I}$ η (φυσική) απεικόνιση με $\varphi(r) = r+\mathrm{I}$. Η φ είναι επιμορφισμός δακτυλίων με $\mathrm{Ker}\varphi = \mathrm{I}$ (γιατί;). Άρα, βλέπουμε ότι για το ιδεώδες I υπάρχει ένας ομομορφισμός δακτυλίων του οποίου ο πυρήνας είναι το I.

Θεώρημα Α΄.1.12. ***1^0 Θεώρημα ισομορφισμών***

Έστω $\varphi : \mathrm{R}_1 \longrightarrow \mathrm{R}_2$ ομομορφισμός δακτυλίων. Τότε υπάρχει ισομορφισμός δακτυλίων:

$$\overline{\varphi} : \mathrm{R}_1/Ker\varphi \longrightarrow \mathrm{Im}\varphi.$$

Απόδειξη. Για κάθε $r+Ker\varphi \in \mathrm{R}_1/Ker\varphi$ ορίζουμε $\overline{\varphi}(r+Ker\varphi) = \varphi(r)$.

Ως άσκηση μπορείτε να αποδείξετε ότι η $\overline{\varphi}$ είναι ομομορφισμός δακτυλίων 1-1 και επί (βλέπε Πρόταση Α΄.1.6 και τον ορισμό του δακτυλίου πηλίκων). ό.έ.δ.

Α΄.1.3 Επεκτάσεις και αυτομορφισμοί σωμάτων

Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{E}$ ένα σώμα που περιέχει το $\mathbb{F}$ ως υπόσωμα. Το $\mathbb{E}$ ονομάζεται **επέκταση** του $\mathbb{F}$ και συμβολίζεται $\mathbb{F} \leq \mathbb{E}$ ή $\mathbb{F} \mid \mathbb{E}$.

Έστω $\mathbb{E}$ μια επέκταση του σώματος $\mathbb{F}$. Το σώμα $\mathbb{E}$ μπορεί να θεωρηθεί ως διανυσματικός χώρος επί του σώματος $\mathbb{F}$, όπου η πρόσθεση είναι η πρόσθεση του σώματος $\mathbb{E}$ και ο αριθμητικός πολλαπλασιασμός είναι ο πολλαπλασιασμός ενός στοιχείου του σώματος $\mathbb{F}$ και ενός στοιχείου του σώματος $\mathbb{E}$.

Η διάσταση του $\mathbb{E}$ ως διανυσματικού χώρου επί του $\mathbb{F}$ ονομάζεται **βαθμός** της επέκτασης και συμβολίζεται με $[\mathbb{E} : \mathbb{F}]$. Αν ο βαθμός επέκτασης είναι πεπερασμένος, τότε η επέκταση $\mathbb{F} \mid \mathbb{E}$ λέγεται πεπερασμένη επέκταση, διαφορετικά λέγεται άπειρη.

Για παράδειγμα, αν $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι τα σώματα των ρητών, των πραγματικών και των μιγαδικών αριθμών αντίστοιχα, τότε $[\mathbb{C} : \mathbb{R}] = 2$ ενώ $[\mathbb{R} : \mathbb{Q}] = \infty$.

Έστω $\mathbb{F} \leq \mathbb{K} \leq \mathbb{E}$. Τότε μπορούμε να αποδείξουμε (προσπαθήστε το!) ότι:

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}].$$

Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής μηδέν και $\mathbb{Q}$ το σώμα των ρητών αριθμών. Ορίζουμε την απεικόνιση $\varphi : \mathbb{Q} \longrightarrow \mathbb{F}$ ως εξής: $\varphi(a/b) = (a \cdot 1) \cdot (b \cdot 1)^{-1}$, όπου $1 \in \mathbb{F}$ είναι το μοναδιαίο του σώματος $\mathbb{F}$.

Μπορείτε να αποδείξετε ότι η απεικόνιση φ είναι ένας ομομορφισμός σωμάτων, μάλιστα δε, είναι 1-1.

Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής p και $\mathbb{Z}_p$ το σώμα των ακεραίων $\bmod\ p$. Ορίζουμε την απεικόνιση $\vartheta : \mathbb{Z}_p \longrightarrow \mathbb{F}$ ως εξής:

$$\vartheta([a]) = \underbrace{1 + 1 + \cdots + 1}_{a\text{–φορές}},$$

όπου 1 είναι το μοναδιαίο του σώματος $\mathbb{F}$.

Μπορείτε να αποδείξετε ότι η απεικόνιση φ είναι ένας ομομορφισμός σωμάτων, μάλιστα δε, είναι 1-1.

Πρόταση Α΄.1.13. *Κάθε σώμα χαρακτηριστικής μηδέν περιέχει ένα υπόσωμα ισόμορφο με το σώμα των ρητών αριθμών.*

Κάθε σώμα χαρακτηριστικής p περιέχει ένα υπόσωμα ισόμορφο με το σώμα $\mathbb{Z}_p$.

Απόδειξη. Αποδείξετε ότι οι απεικονίσεις φ και ϑ που ορίσαμε προηγουμένως είναι πράγματι ομομορφισμοί και 1-1. Οπότε το αποτέλεσμα είναι άμεσο. ό.έ.δ.

Πόρισμα Α΄.1.14. *Το σώμα των ρητών αριθμών είναι (μέσω ισομορφισμού) το μικρότερο υπόσωμα ένος σώματος χαρακτηριστικής μηδέν.*

Το σώμα των ακεραίων $\bmod p$ είναι (μέσω ισομορφισμού) το μικρότερο υπόσωμα ένος σώματος χαρακτηριστικής p.

Απόδειξη. Η τομή υποσωμάτων ενός σώματος είναι σώμα (γιατί;). Επομένως, η τομή όλων των υποσωμάτων ενός σώματος είναι υπόσωμα, το οποίο

στην περίπτωση που η χαρακτηριστική του σώματος είναι μηδέν, περιέχει και περιέχεται στο $\mathbb{Q}$ (γιατί;). Ενώ στην περίπτωση που η χαρακτηριστική του σώματος είναι p, περιέχει και περιέχεται στο $\mathbb{Z}_p$. ό.έ.δ.

Από τα προηγούμενα συνάγουμε τον επόμενο ορισμό.

Ορισμός Α΄.1.15. *Το σώμα των ρητών αριθμών και το σώμα $\mathbb{Z}_p$ ονομάζονται* ***πρώτα*** *σώματα.*

Έστω $\mathbb{F} \leq \mathbb{E}$ μια επέκταση του σώματος $\mathbb{F}$ και $c \in \mathbb{E}$. Ορίζουμε:

$$\mathbb{F}(c) = \bigcap \{\, \mathbb{K} \mid \mathbb{K} \leq \mathbb{E} \text{ με } \mathbb{F} \subseteq \mathbb{K} \text{ και } c \in \mathbb{K} \,\}.$$

Δηλαδή το $\mathbb{F}(c)$ είναι το μικρότερο σώμα του $\mathbb{E}$ που περιέχει το σώμα $\mathbb{F}$ και το στοιχείο c. Το σώμα $\mathbb{F}(c)$ ονομάζεται επέκταση του $\mathbb{F}$ με προσάρτηση του στοιχείου c.

Προφανώς, μπορούμε να προσαρτήσουμε περισσότερα του ενός στοιχεία σε ένα σώμα. Μάλιστα δε ισχύει: Αν $c_1, c_2 \in \mathbb{E}$, τότε $(\mathbb{F}(c_1))(c_2) = (\mathbb{F}(c_2))(c_1)$ (γιατί;). Επομένως, μπορούμε να γράφουμε $\mathbb{F}(c_1, c_2)$.

Για παράδειγμα προσαρτώντας το $\sqrt{2}$ στο $\mathbb{Q}$, έχουμε το σώμα:

$$\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q} \,\}.$$

(Γιατί τα στοιχεία του $\mathbb{Q}(\sqrt{2})$ είναι αυτής της μορφής;)

Έστω $\mathbb{F} \leq \mathbb{E}$ μια επέκταση του σώματος $\mathbb{F}$. Αν υπάρχει $c \in \mathbb{E}$, έτσι ώστε $\mathbb{E} = \mathbb{F}(c)$, τότε η $\mathbb{E}$ ονομάζεται **απλή επέκταση** του $\mathbb{F}$.

Παρατηρήσεις Α΄.1.16.

1. Έστω $\mathbb{F} \leq \mathbb{E}$ μια επέκταση του σώματος $\mathbb{F}$. Το ερώτημα που προκύπτει είναι κατά πόσον η επέκταση αυτή είναι απλή.

2. Στην παράγραφο αυτή θεωρήσαμε ως δεδομένο ότι υπάρχει μια επέκταση $\mathbb{E}$ ενός σώματος $\mathbb{F}$ και αναφέραμε ορισμένες ιδιότητες των επεκτάσεων.

   Το ερώτημα που εγείρεται είναι το εξής: Αν έχουμε ένα σώμα, έστω $\mathbb{F}$, μπορούμε να κατασκευάσουμε (γνήσιες) επεκτάσεις του;

Για το πρώτο ερώτημα, πληροφοριακά αναφέρουμε (χωρίς η απόδειξη να είναι ιδιαίτερα δύσκολη) ότι κάθε πεπερασμένη επέκταση του σώματος $\mathbb{Q}$ των ρητών αριθμών είναι απλή.

Επίσης, θα δούμε (βλέπε σελ. 435) ότι κάθε πεπερασμένη επέκταση ενός πεπερασμένου σώματος είναι απλή.

Για το δεύτερο ερώτημα θα δούμε ότι, με την βοήθεια των πολυωνύμων με συντελεστές από ένα σώμα $\mathbb{F}$, μπορούμε να κατασκευάσουμε γνήσιες επεκτάσεις του (ιδέ σελ. 425).

Παράδειγμα Α΄.1.17. Έστω $\mathbb{Q}(\sqrt{2},\sqrt{3})$ το σώμα που προκύπτει προσαρτώντας στο σώμα των ρητών αριθμών τις τετραγωνικές ρίζες $\sqrt{2}$ και $\sqrt{3}$, θα δείξουμε ότι $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$, δηλαδή η επέκταση $\mathbb{Q}(\sqrt{2},\sqrt{3})$ είναι απλή.

Προφανώς $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. Επίσης, το στοιχείο $(\sqrt{2}+\sqrt{3})^2 = 2+2\sqrt{6}+3$ ανήκει στο σώμα $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, δηλαδή το στοιχείο $\sqrt{6}$ ανήκει στο $\mathbb{Q}(\sqrt{2}+\sqrt{3})$, οπότε $(\sqrt{2}+\sqrt{3})\sqrt{6} = 2\sqrt{3}+3\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Επομένως, $\sqrt{3}, \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ και συνεπώς $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Έστω $\varphi : \mathbb{F}_1 \longrightarrow \mathbb{F}_2$ ένας ομομορφισμός σωμάτων. Τότε προφανώς (γιατί;) ο φ είναι είτε ο τετριμμένος ομομορφισμός είτε ένας μονομορφισμός.

Ένας αυτομορφισμός ενός σώματος $\mathbb{F}$ είναι ένας ομομορφισμός $\varphi : \mathbb{F} \longrightarrow \mathbb{F}$ σωμάτων, ο οποίος είναι 1-1 και επί. Το σύνολο των αυτομορφισμών ενός σώματος $\mathbb{F}$ αποτελεί (γιατί;) ομάδα με πράξη την σύνθεση απεικονίσεων και θα συμβολίζεται με $Aut(\mathbb{F})$.

Πρόταση Α΄.1.18. *Έστω $\mathbb{E}$ ένα σώμα και $\mathbb{F} \leq \mathbb{E}$ το πρώτο σώμα. Για κάθε αυτομορφισμό $\varphi \in Aut(\mathbb{E})$ και για κάθε $c \in \mathbb{F}$ ισχύει $\varphi(c) = c$. Δηλαδή κάθε αυτομορφισμός ενός σώματος αφήνει τα στοιχεία του πρώτου σώματος αναλλοίωτα.*

Απόδειξη. Αν το σώμα $\mathbb{E}$ είναι χαρακτηριστικής μηδέν, τότε το πρώτο του σώμα είναι το σώμα των ρητών αριθμών και επειδή για κάθε αυτομορφισμό $\varphi \in Aut(\mathbb{E})$ έχουμε ότι $\varphi(1) = 1$, έπεται ότι για κάθε κλάσμα $\kappa/\lambda = \lambda^{-1}\cdot\kappa$ θα έχουμε $\varphi(\lambda^{-1}\cdot\kappa) = \varphi(\lambda^{-1})\cdot\varphi(\kappa) = (\varphi(\lambda))^{-1}\cdot\varphi(\kappa) = \lambda^{-1}\cdot\kappa$.

Όμοια αποδεικνύεται και η περίπτωση όπου έχουμε ένα σώμα χαρακτηριστικής p, οπότε το πρώτο του σώμα είναι το σώμα $\mathbb{Z}_p$. ό.έ.δ.

Από την προηγούμενη πρόταση έπεται άμεσα ότι οι ομάδες $Aut(\mathbb{Q})$ και $Aut(\mathbb{Z}_p)$ είναι τετριμμένες, δηλαδή αποτελούνται μόνο από τον ταυτοτικό αυτομορφισμό.

Παράδειγμα Α΄.1.19. Ας υπολογίσουμε την ομάδα αυτομορφισμών του σώματος $\mathbb{Q}(\sqrt{3})$. Έστω $\varphi \in Aut(\mathbb{Q}(\sqrt{3}))$. Ο φ είναι πλήρως καθορισμένος από την εικόνα $\varphi(\sqrt{3})$ (γιατί;). Υποθέτουμε ότι $\varphi(\sqrt{3}) = a + b\sqrt{3}$. Επειδή ο φ είναι αυτομορφισμός έχουμε ότι $3 = \varphi(3) = \varphi((\sqrt{3})^2) = (a + b\sqrt{3})^2$. Από την σχέση αυτή εύκολα έπεται ότι $a = 0$ και $b = \pm 1$. Οπότε έχουμε μόνο δύο αυτομορφισμούς του σώματος $\mathbb{Q}(\sqrt{3})$, τον ταυτοτικό και τον αυτομορφισμό ϑ με $\vartheta(a + b\sqrt{3}) = a - b\sqrt{3}$.

Γενικά είναι πολύ δύσκολο να υπολογίσουμε την ομάδα αυτομορφισμών ενός τυχαίου σώματος. Στα επόμενα (ιδέ σελίδα 437), θα υπολογίσουμε την ομάδα αυτομορφισμών ενός πεπερασμένου σώματος.

Έστω $\mathbb{E}$ ένα σώμα και $\mathbb{F}$ ένα υπόσωμά του ($\mathbb{F} \leq \mathbb{E}$). Θεωρούμε το εξής σύνολο $G(\mathbb{E}, \mathbb{F}) = \{ \sigma \mid \sigma \in Aut(\mathbb{E})$ με την ιδιότητα $\sigma(r) = r$ για κάθε $r \in \mathbb{F} \}$. Είναι εύκολο να δούμε ότι το σύνολο $G(\mathbb{E}, \mathbb{F})$ είναι υποομάδα της $Aut(\mathbb{E})$.

Τα στοιχεία της ομάδας $G(\mathbb{E}, \mathbb{F})$ ονομάζονται $\mathbb{F}$-αυτομορφισμοί.

Έστω $\mathbb{F} \leq \mathbb{K} \leq \mathbb{E}$, τότε προφανώς (γιατί;) ισχύει $G(\mathbb{E}, \mathbb{K}) \leq G(\mathbb{E}, \mathbb{F})$.

Α΄.2 Ο δακτύλιος των πολυωνύμων

Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{F}[x]$ ο δακτύλιος πολυωνύμων με συντελεστές από το σώμα $\mathbb{F}$. Ένα πολυώνυμο $\phi(x) \in \mathbb{F}[x]$, ως γνωστόν, είναι της μορφής:

$$\phi(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad \text{με } a_i \in \mathbb{F}.$$

Έστω k ο μεγαλύτερος δείκτης (αν υπάρχει), έτσι ώστε ο αντίστοιχος συντλεστής a_k να είναι μη μηδενικός. Ο k ονομάζεται **βαθμός** του πολυωνύμου και συμβολίζεται με $deg(\phi(x))$, ενώ ο a_k ονομάζεται **μεγιστοβάθμιος** συντελεστής. Αν ο μεγιστοβάθμιος συντελεστής σε ένα πολυώνυμο είναι

το 1, τότε το πολυώνυμο ονομάζεται ***μονικό***. Για παράδειγμα, αν $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, με $a_n \neq 0$[3], τότε το πολυώνυμο $a_n^{-1}\phi(x)$ προφανώς είναι μονικό. Το πολυώνυμο, του οποίου όλοι οι συντελεστές είναι μηδενικοί, ονομάζεται το **μηδενικό** πολυώνυμο, το συμβολίζουμε με **0** (ή απλά 0) και **δεν** του προσάπτουμε βαθμό. Προφανώς, τα πολυώνυμα μηδενικού βαθμού είναι τα μη μηδενικά στοιχεία του σώματος $\mathbb{F}$, τα **σταθερά** πολυώνυμα.

Για τον βαθμό του αθροίσματος και του γινομένου δύο πολυωνύμων με συντελεστές από ένα σώμα ισχύει η ακόλουθη πρόταση, της οποίας η απόδειξη είναι άμεση.

Πρόταση Α΄.2.1. *Έστω $\phi(x)$ και $\theta(x)$ μη μηδενικά πολυώνυμα. Τότε ισχύει:*

1. *Είτε $\phi(x)+\theta(x) = \mathbf{0}$ είτε $deg(\,\phi(x)+\theta(x)\,) \leq \max(\,deg(\phi(x)),\ deg(\theta(x))\,)$.*

   Η ανισότητα στην προηγούμενη σχέση είναι γνήσια μόνο στην περίπτωση που τα δύο πολυώνυμα έχουν τον ίδιο βαθμό και αντίθετους μεγιστοβάθμιους συντελεστές

2. $deg(\,\phi(x)\cdot\theta(x)\,) = deg(\phi(x)) + deg(\theta(x))$.

Α΄.2.1 Διαιρετότητα πολυωνύμων

Στον δακτύλιο $\mathbb{F}[x]$ μπορούμε να ορίσουμε μια διαίρεση πολυωνύμων ανάλογη με την γνωστή διαίρεση ακεραίων αριθμών.

Θεώρημα Α΄.2.2. ***Αλγόριθμος της διαίρεσης πολυωνύμων***

Έστω $\alpha(x),\ \beta(x) \in \mathbb{F}[x]$ με το $\beta(x)$ να μην είναι το μηδενικό πολυώνυμο. Τότε υπάρχουν μοναδικά $\pi(x),\ \upsilon(x) \in \mathbb{F}[x]$ τέτοια ώστε:

$$\alpha(x) = \pi(x)\cdot\beta(x) + \upsilon(x) \quad \textbf{\textit{και}} \quad \text{ή } \upsilon(x) = 0 \text{ ή } deg(\upsilon(x)) < deg(\beta(x)).$$

Το $\alpha(x)$ ονομάζεται διαιρεταίος, το $\beta(x)$ ονομάζεται διαιρέτης και τα $\pi(x)$, $\upsilon(x)$ πηλίκο και υπόλοιπο αντίστοιχα.

[3] Εις το εξής, όταν γράφουμε $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, θα εννοούμε ότι $a_n \neq 0$.

Απόδειξη. Έστω $\mathcal{A} = \{\, \alpha(x) - \beta(x)\,\tau(x),\ \textit{όπου}\ \tau(x) \in \mathbb{F}[x]\,\}$. Αν το μηδενικό πολυώνυμο ανήκει στο σύνολο $\mathcal{A}$, τότε υπάρχει $\pi(x) \in \mathbb{F}[x]$, έτσι ώστε $\alpha(x) - \beta(x)\,\pi(x) = \mathbf{0}$, οπότε τα $\pi(x)$ και $\upsilon(x) = \mathbf{0}$ πληρούν τις υποθέσεις του Θεωρήματος.

Υποθέτουμε ότι το μηδενικό πολυώνυμο δεν ανήκει στο σύνολο $\mathcal{A}$. Έστω $\upsilon(x) = \alpha(x) - \beta(x)\,\pi(x)$ ένα στοιχείο του συνόλου $\mathcal{A}$ με τον μικρότερο δυνατό βαθμό. Τότε $\alpha(x) = \beta(x)\,\pi(x) + \upsilon(x)$.

Θα δείξουμε ότι $deg(\,\upsilon(x)\,) < deg(\,\beta(x)\,)$. Πράγματι, υποθέτουμε ότι:

$$\begin{aligned}
&\upsilon(x) = \alpha(x) - \beta(x)\pi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0,\\
&\beta(x) = bx^m + bx^{m-1} + \cdots + b_1 x + b_0 \quad \text{και}\\
&deg(\upsilon(x)) = n \geq m = deg(\beta(x)).
\end{aligned}$$

Τότε τα πολυώνυμα $\upsilon(x)$ και $(a_n b_m^{-1})x^{n-m} \cdot \beta(x)$ είναι του ιδίου βαθμού και έχουν αντίθετους συντελεστές, επομένως το πολυώνυμο $\upsilon(x) - (a_n b_m^{-1})x^{n-m} \cdot \beta(x)$, έχει βαθμό (γνήσια) μικρότερο από το βαθμό του $\upsilon(x)$ και επιπλέον:

$$\begin{aligned}
\upsilon(x) - (a_n b_m^{-1})x^{n-m} \cdot \beta(x) &= \alpha(x) - \beta(x)\pi(x) - (a_n b_m^{-1})x^{n-m} \cdot \beta(x)\\
&= \alpha(x) - (\pi(x) + (a_n b_m^{-1})x^{n-m}) \cdot \beta(x) \in \mathcal{A}.
\end{aligned}$$

Τούτο είναι άτοπο από την εκλογή του πολυωνύμου $\upsilon(x)$ ως πολυώνυμο με τον μικρότερο βαθμό από όλα τα πολυώνυμα που ανήκουν στο σύνολο $\mathcal{A}$. Επομένως $deg(\,\upsilon(x)\,) < deg(\,\beta(x)\,)$.

Τα πολυώνυμα $\pi(x)$ και $\upsilon(x)$ με την ιδιότητα $\alpha(x) = \beta(x) \cdot \pi(x) + \upsilon(x)$ και $deg(\,\upsilon\,) < deg(\,\beta(x)\,)$ είναι μοναδικά. Πράγματι, υποθέτουμε ότι εκτός από τα $\pi(x)$ και $\upsilon(x)$ υπάρχουν και τα πολυώνυμα $\pi'(x)$ και $\upsilon'(x)$, τέτοια ώστε:

$$\alpha(x) = \beta(x) \cdot \pi'(x) + \upsilon'(x) \quad \text{και} \quad deg(\upsilon'(x)) < deg(\beta(x)).$$

Τότε αφαιρώντας κατά μέλη τις σχέσεις $\alpha(x) = \beta(x) \cdot \pi(x) + \upsilon(x)$ και $\alpha(x) = \beta(x) \cdot \pi'(x) + \upsilon'(x)$ έχουμε $\beta(x) \cdot (\,\pi(x) - \pi'(x)\,) = \upsilon(x) - \upsilon'(x)$. Αν $\upsilon(x) - \upsilon'(x) \neq \mathbf{0}$, τότε και $\pi(x) - \pi'(x) \neq \mathbf{0}$, οπότε από την Πρόταση Α΄.2.1 έχουμε ότι $deg(\,\upsilon(x) - \upsilon'(x)\,) \geq deg(\,\beta(x)\,)$. Τούτο είναι άτοπο, αφού $deg(\,\upsilon(x) - \upsilon'(x)\,) \leq \max(\,deg(\,\upsilon(x)\,),\ deg(\,\upsilon'(x)\,)) < deg(\,\beta(x)\,)$. Άρα $\upsilon(x) = \upsilon'(x)$ και $\pi(x) = \pi'(x)$. ό.έ.δ.

Παρατηρήσεις Α΄.2.3. 1. Στο προηγούμενο Θεώρημα, αν ισχύει $\alpha(x) = \mathbf{0}$ ή $deg(\alpha(x)) < deg(\beta(x))$, τότε προφανώς $\pi(x) = \mathbf{0}$ και $\upsilon(x) = \alpha(x)$.

2. Το προηγούμενο Θεώρημα (φαινομενικά) δεν μας δίνει ένα τρόπο υπολογισμού του πηλίκου και του υπολοίπου της διαίρεσης ενός πολυωνύμου δι' ενός άλλου πολυωνύμου. Αν όμως παρατηρήσουμε καλύτερα την απόδειξη, θα ("αναγνωρίσουμε") τη γνωστή σε όλους μας μέθοδο διαίρεσης πολυωνύμων.

Θα λέμε ότι το πολυώνυμο $\beta(x) \in \mathbb{F}[x]$ διαιρεί το πολυώνυμο $\alpha(x) \in \mathbb{F}[x]$ στο σώμα $\mathbb{F}$ (και θα συμβολίζουμε με $\beta(x) \mid \alpha(x)$), αν το υπόλοιπο $\upsilon(x)$, στη διαίρεση του $\alpha(x)$ με το $\beta(x)$, είναι το μηδενικό πολυώνυμο. Ισοδύναμα λέμε ότι το $\alpha(x)$ διαιρείται (ή είναι πολλαπλάσιο του) από το $\beta(x)$.

Ας δούμε μερικές άμεσες συνέπειες των προηγουμένων, τις οποίες θα χρησιμοποιούμε συχνά στα επόμενα χωρίς ιδιαίτερη αναφορά.

1. Το μηδενικό πολυώνυμο διαιρείται από κάθε άλλο πολυώνυμο. Πράγματι, για κάθε $\phi(x) \in \mathbb{F}[x]$ ως γνωστόν ισχύει $\phi(x) \cdot \mathbf{0} = \mathbf{0}$.

   Οπότε, το μηδενικό πολυώνυμο $\mathbf{0}$ διαιρεί μόνο το μηδενικό πολυώνυμο. Επομένως στα επόμενα, όταν γράφουμε $\phi(x) \mid \theta(x)$ θα εννοούμε (σιωπηλά) ότι $\phi(x) \neq \mathbf{0}$.

2. Υποθέτουμε ότι $\phi(x) \mid \theta(x)$, με $\phi(x) \neq \mathbf{0}$. Τότε υπάρχει μοναδικό $\pi(x) \in \mathbb{F}[x]$, τέτοιο ώστε $\theta(x) = \phi(x)\,\pi(x)$. Πράγματι, αν υπήρχε και ένα άλλο $\pi'(x) \in \mathbb{F}[x]$ με $\theta(x) = \phi(x)\,\pi'(x)$, τότε θα είχαμε $\theta(x) = \phi(x)\,\pi(x) = \phi(x)\,\pi'(x)$. Δηλαδή $\phi(x)\,(\,\pi(x) - \pi'(x)\,) = \mathbf{0}$ και επειδή το $\phi(x)$ δεν είναι το μηδενικό πολυώνυμο έχουμε $\pi(x) - \pi'(x) = \mathbf{0}$, άρα $\pi(x) = \pi'(x)$.

3. Υποθέτουμε ότι $\phi(x) \mid \theta(x)$. Τότε $deg(\phi(x)) \leq deg(\theta(x))$, οπότε:

   $$\text{αν } \phi(x) \mid \theta(x) \text{ και } \theta(x) \mid \phi(x), \text{ τότε } deg(\phi(x)) = deg(\theta(x)).$$

4. Κάθε (μη μηδενικό) σταθερό πολυώνυμο c διαιρεί κάθε άλλο πολυώνυμο. Πράγματι, για κάθε $\pi(x) \in \mathbb{F}[x]$ έχουμε $\phi(x) = c \cdot (\,c^{-1} \cdot \phi(x)\,)$.

5. Αν $\phi(x) \mid \theta(x)$, τότε για κάθε $0 \neq c \in \mathbb{F}[x]$ έχουμε ότι $c \cdot \phi(x) \mid \theta(x)$. Άρα αν $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$, τότε το μονικό πολυώνυμο $a_n^{-1} \cdot \phi(x)$ διαιρεί το $\theta(x)$.

6. Υποθέτουμε ότι το πολυώνυμο $\phi(x)$ διαιρεί το πολυώνυμο $\theta(x)$ και ότι το πολυώνυμο $\theta(x)$ διαιρεί το πολυώνυμο $\sigma(x)$. Τότε, προφανώς, το $\phi(x)$ διαιρεί το $\sigma(x)$.

7. Υποθέτουμε ότι το πολυώνυμο $\phi(x)$ διαιρεί τα πολυώνυμα $\theta_1(x)$ και $\theta_2(x)$. Τότε (γιατί;) το $\phi(x)$ διαιρεί το πολυώνυμο $\alpha(x)\cdot\theta_1(x)+\beta(x)\cdot\theta_2(x)$, για όλα τα πολυώνυμα $\alpha(x),\ \beta(x) \in \mathbb{F}[x]$.

8. Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{E}$ μια επέκτασή του, τότε για τα πολυώνυμα $\beta(x)$, $\alpha(x) \in \mathbb{F}[x]$ ισχύει: Το $\beta(x)$ διαιρεί το $\alpha(x)$ στο σώμα $\mathbb{F}$, αν και μόνο αν το $\beta(x)$ διαιρεί το $\alpha(x)$ στο σώμα $\mathbb{E}$.

Πρόταση Α΄.2.4. *Ο δακτύλιος των πολυωνύμων $\mathbb{F}[x]$ είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Έστω I ένα ιδεώδες του $\mathbb{F}[x]$. Αν το I είναι το μηδενικό ιδεώδες, τότε αυτό προφανώς είναι κύριο. Υποθέτουμε ότι $\mathrm{I} \neq \{\,0\,\}$. Επιλέγουμε ένα $p(x) \in \mathrm{I}$ ελαχίστου βαθμού. Τότε το $p(x)$ διαιρεί κάθε στοιχείο του I. Πράγματι, έστω $\alpha(x) \in \mathrm{I}$, από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχουν $\pi(x),\ \upsilon(x) \in \mathbb{F}[x]$, τέτοια ώστε $\alpha(x) = p(x) \cdot \pi(x) + \upsilon(x)$ με $\upsilon(x) = \mathbf{0}$ ή $deg(\upsilon(x)) < deg(p(x))$. Αλλά $\upsilon(x) = \alpha(x) - p(x) \cdot \pi(x) \in \mathrm{I}$ (γιατί;) Επομένως, από τον τρόπο εκλογής του $p(x)$, έχουμε ότι, αναγκαστικά, $\upsilon(x) = \mathbf{0}$. Δηλαδή $\mathrm{I} = \{\, r(x) \cdot p(x) \mid r(x) \in \mathbb{F}[x] \,\} = \langle\, p(x) \,\rangle$. ό.έ.δ.

Παρατήρηση Α΄.2.5. Επειδή ισχύει $\langle\, p(x) \,\rangle = \langle\, ap(x) \,\rangle$ για κάθε μη μηδενικό $a \in \mathbb{F}$ (γιατί ισχύει;) μπορούμε να αναδιατυπώσουμε την προηγούμενη πρόταση ως εξής: "Για κάθε μη μηδενικό ιδεώδες I του δακτυλίου $\mathbb{F}[x]$ υπάρχει μοναδικό μονικό πολυώνυμο $q(x)$, έτσι ώστε $\mathrm{I} = \langle\, q(x) \,\rangle$".

Ένα μη σταθερό πολυώνυμο $p(x) \in \mathbb{F}$ θα λέγεται **ανάγωγο** επί του $\mathbb{F}$ αν από τη σχέση $p(x) = \sigma(x) \cdot \tau(x)$, έπεται ότι ένα από τα $\sigma(x),\ \tau(x)$ είναι σταθερό πολυώνυμο.

Από τον ορισμό του αναγώγου πολυωνύμου έπεται ότι όλα τα πολυώνυμα με βαθμό ένα είναι ανάγωγα. Το να αποφανθούμε όμως, αν ένα πολυώνυμο με βαθμό μεγαλύτερο του ένα είναι ανάγωγο δεν είναι καθόλου εύκολο και εξαρτάται από το σώμα $\mathbb{F}$ των συντελεστών. Για παράδειγμα, το πολυώνυμο x^2-3 είναι ανάγωγο επί του σώματος των ρητών αριθμών $\mathbb{Q}$, αλλά **δεν** είναι ανάγωγο επί του σώματος των πραγματικών αριθμών $\mathbb{R}$, αφού $x^2-3 = (x-\sqrt{3})(x+\sqrt{3})$.

Εδώ δεν θα επεκταθούμε περισσότερο όσον αφορά τα ανάγωγα πολυώνυμα επί ενός σώματος $\mathbb{F}$. Αργότερα (βλέπε σελίδα 438) θα επανέλθουμε εστιαζόμενοι στην μελέτη των αναγώγων πολυωνύμων με συντελεστές από ένα πεπερασμένο σώμα.

Α΄.2.2 Μέγιστος Κοινός Διαιρέτης Πολυωνύμων

Πριν δώσουμε τον ορισμό του μέγιστου κοινού διαιρέτη πολυωνύμων, θα θέλαμε να παρατηρήσουμε ότι, αν $\phi(x),\ \theta(x) \in \mathbb{F}[x]$, τότε, όπως έχουμε επισημάνει, κάθε σταθερό (μη μηδενικό) πολυώνυμο c διαιρεί και τα δύο πολυώνυμα. Δηλαδή για τα πολυώνυμα αυτά υπάρχουν *κοινοί διαιρέτες*. Επομένως, έπεται ότι υπάρχουν κοινοί διαιρέτες δύο πολυωνύμων οι οποίοι είναι μονικά πολυώνυμα.

Ορισμός Α΄.2.6. *Έστω $\phi(x),\ \theta(x) \in \mathbb{F}[x]$ όχι και τα δύο μηδενικά πολυώνυμα. Ένα πολυώνυμο $d(x) \in \mathbb{F}[x]$ θα λέγεται* **μέγιστος κοινός διαιρέτης** *των $\phi(x)$ και $\theta(x)$ και θα συμβολίζεται με $d(x) = \text{μκδ}(\phi(x),\ \theta(x))$ ή απλά $d(x) = (\phi(x),\ \theta(x))$ αν:*

(i) $d(x) \mid \phi(x)$ και $d(x) \mid \theta(x)$. Δηλαδή το πολυώνυμο $d(x)$ είναι κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$.

(ii) Το $d(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\delta(x) \in \mathbb{F}[x]$ με $\delta(x) \mid \phi(x)$ και $\delta(x) \mid \theta(x)$, τότε $\delta(x) \mid d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$ είναι διαιρέτης του $d(x)$.

Ο ορισμός δεν εξασφαλίζει την υπάρξη ενός μ.κ.δ. δύο πολυωνύμων εκ των οποίων τουλάχιστον το ένα είναι μη μηδενικό.

Μπορούμε όμως να δούμε εύκολα ότι αν υπάρχει μ.κ.δ. των $\phi(x)$ και $\theta(x)$, τότε αυτός είναι μοναδικός. Πράγματι υποθέτουμε ότι υπάρχουν δύο πολυώνυμα $d_1(x)$ και $d_2(x)$ με τις ιδιότητες του ορισμού. Τότε από τις (i) και (iii) του ορισμού έχουμε ότι $d_1(x) \mid d_2(x)$ και $d_2(x) \mid d_1(x)$. Δηλαδή υπάρχει $c \in \mathbb{F}[x]$, τέτοιο ώστε $d_1(x) = c\,d_2(x)$. Αλλά τα $d_1(x)$, $d_2(x)$ είναι μονικά. Άρα $d_1(x) = d_2(x)$.

Πριν αποδείξουμε ότι ο μ.κ.δ. δύο πολυωνύμων υπάρχει, επισημαίνουμε ότι αν και τα δύο πολυώνυμα είναι μηδενικά πολυώνυμα, τότε ο μ.κ.δ. δεν ορίζεται, αφού η (iii) στον ορισμό δεν ικανοποιείται (γιατί;).

Θα αποδείξουμε τώρα ένα Θεώρημα το οποίο όχι μόνο μας εξασφαλίζει την ύπαρξη του μ.κ.δ. δύο πολυωνύμων, αλλά μας δίνει και μία έκφραση του ως (γραμμικό) συνδυασμό των δύο πολυωνύμων.

Θεώρημα Α΄.2.7. *Έστω $\phi(x),\ \theta(x) \in \mathbb{F}[x]$ όχι και τα δύο μηδενικά πολυώνυμα. Τότε υπάρχει ο (μοναδικός) μ.κ.δ. των $\phi(x)$ και $\theta(x)$. Επιπλέον, υπάρχουν $\alpha(x),\ \beta(x) \in \mathbb{F}[x]$, τέτοια ώστε* $\mu\kappa\delta(\,\phi(x), \theta(x)\,) \;=\; \alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x)$

Απόδειξη. Έστω $\mathcal{U} \;=\; \{\,\lambda(x)\cdot\phi(x) + \kappa(x)\cdot\theta(x) \;\mid\; \lambda(x),\, \kappa(x) \in \mathbb{F}[x]\,\}$. Παρατηρούμε ότι στο σύνολο $\mathcal{U}$ ανήκουν τα πολυώνυμα $\phi(x)$ και $\theta(x)$ (γιατί;). Επίσης, στο σύνολο $\mathcal{U}$ ανήκουν μονικά πολυώνυμα. Πράγματι, αν $\eta(x) \;=\; \lambda(x)\cdot\phi(x) + \kappa(x)\cdot\theta(x)$ είναι ένα (μη μηδενικό) στοιχείο του $\mathcal{U}$ με συντελεστή του μεγιστοβαθμίου όρου c, τότε το πολυώνυμο $c^{-1}\eta(x) \;=\; (c^{-1}\lambda(x))\cdot\phi(x) + (c^{-1}\kappa(x))\cdot\theta(x)$ είναι μονικό και ανήκει στο σύνολο $\mathcal{U}$.

Από τις προηγούμενες παρατηρήσεις έπεται ότι μπορούμε να επιλέξουμε ένα στοιχείο:

$$d(x) \;=\; \alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x)$$

του $\mathcal{U}$, το οποίο να είναι μονικό και να έχει τον μικρότερο βαθμό από όλα τα (μη μηδενικά) στοιχεία του $\mathcal{U}$.

Το $d(x)$ είναι μονικό, άρα πληροί τη συνθήκη (ii) του ορισμού.

Έστω $\delta(x) \in \mathbb{F}[x]$ με $\delta(x) \mid \phi(x)$ και $\delta(x) \mid \theta(x)$, τότε προφανώς $\delta(x) \mid d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$ είναι διαιρέτης του $d(x)$. Άρα, το $d(x)$ πληροί τη συνθήκη (iii) του ορισμού.

Απομένει να αποδείξουμε τη συνθήκη (i).

Έστω $\tau(x) = \lambda(x)\cdot\phi(x) + \kappa(x)\cdot\theta(x)$ ένα στοιχείο του συνόλου $\mathcal{U}$. Θα δείξουμε ότι $d(x) \mid \tau(x)$.

Από τον αλγόριθμο διαίρεσης πολυωνύμων υπάρχουν μοναδικά πολυώνυμα $\pi(x), \upsilon(x) \in \mathbb{F}[x]$, τέτοια ώστε:

$$\tau(x) = \pi(x)\,d(x) + \upsilon(x) \quad \text{με } \upsilon(x) = \mathbf{0} \text{ ή } deg(\,\upsilon(x)\,) < deg(\,d(x)\,).$$

Επομένως, έχουμε:

$$\begin{aligned}\upsilon(x) &= \tau(x) - \pi(x)\,d(x)\\ &= \lambda(x)\cdot\phi(x) + \kappa(x)\cdot\theta(x) - \pi(x)\cdot(\,\alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x)\,)\\ &= (\,\lambda(x) - \pi(x)\,\alpha(x)\,)\cdot\phi(x) + (\,\kappa(x) - \pi(x)\,\beta(x)\,)\cdot\theta(x) \in \mathcal{U}.\end{aligned}$$

Υποθέτουμε ότι το $\upsilon(x)$ δεν είναι το μηδενικό πολυώνυμο. Αν c είναι ο συντελεστής του μεγιστοβαθμίου όρου του, τότε το πολυώνυμο $c^{-1}\upsilon(x)$ είναι μονικό, ανήκει στο $\mathcal{U}$ και έχει βαθμό ίσο με τον βαθμό του $\upsilon(x)$, ο οποίος είναι (γνήσια) μικρότερος από το βαθμό του $d(x)$. Αυτό είναι άτοπο από την επιλογή του πολυωνύμου $d(x)$. Αρα $\upsilon(x) = \mathbf{0}$. Δηλαδή το $d(x)$ είναι κοινός διαιρέτης όλων των στοιχείων του συνόλου $\mathcal{U}$, άρα και των $\phi(x)$ και $\theta(x)$. ό.έ.δ.

Παρατηρήσεις Α΄.2.8. 1. Όπως προκύπτει από τον ορισμό και προηγούμενες παρατηρήσεις ο μ.κ.δ. δύο πολυωνύμων έχει το μεγαλύτερο βαθμό από όλους τους κοινούς διαιρέτες των δύο πολυωνύμων.

2. Έστω $\phi(x)$ και $\theta(x)$ δύο πολυώνυμα με το $\phi(x)$ να διαιρεί το $\theta(x)$. Τότε προφανώς $\mu\kappa\delta(\,\phi(x),\ \theta(x)\,) = c^{-1}\phi(x)$, όπου c είναι ο συντελεστής του μεγιστοβαθμίου όρου του $\phi(x)$.

3. Έστω $\phi(x)$ και $\theta(x)$ δύο πολυώνυμα και c_1, c_2 δύο μη μηδενικά στοιχεία του σώματος $\mathbb{F}$. Τότε προφανώς:

$$\mu\kappa\delta(\,\phi(x),\ \theta(x)) = \mu\kappa\delta(\,c_1\,\phi(x),\ c_2\,\theta(x)\,) \quad \text{(γιατί;)}.$$

Επομένως, στην αναζήτηση του μέγιστου κοινού διαιρέτη δύο πολυωνύμων μπορούμε να "περιορισθούμε" σε μονικά πολυώνυμα.

4. Έστω $\mathbb{F}$ ένα σώμα, $\mathbb{E}$ μια επέκτασή του και $\phi(x)$, $\theta(x) \in \mathbb{F}[x]$. Αν ισχύει ότι $\mu\kappa\delta(\phi(x), \theta(x)) = d(x) \in \mathbb{F}[x]$ και $\mu\kappa\delta(\phi(x), \theta(x)) = \delta(x) \in \mathbb{E}[x]$, τότε $d(x) = \delta(x)$.

Το προηγούμενο Θεώρημα δεν μας δίνει μια μέθοδο υπολογισμού του μ.κ.δ. δύο πολυωνύμων $\phi(x)$ και $\theta(x)$, πολύ δε περισσότερο πώς μπορούμε να υπολογίσουμε πολυώνυμα συντελεστές $\alpha(x)$ και $\beta(x)$ στην έκφραση:

$$\mu\kappa\delta(\,\phi(x),\,\theta(x)\,) \;=\; \alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x).$$

Η επόμενη πρόταση είναι πολύ σημαντική και αποτελεί το κύριο βήμα για τον υπολογισμό του μέγιστου κοινού διαιρέτη δύο πολυωνύμων.

Πρόταση Α΄.2.9. *Έστω $\phi(x)$ και $\theta(x)$ μη μηδενικά πολυώνυμα. Αν $\upsilon(x)$ είναι το υπόλοιπο της διαίρεσης του $\theta(x)$ δια του $\phi(x)$, τότε:*

$$\mu\kappa\delta(\,\theta(x),\;\phi(x)\,) = \mu\kappa\delta(\,\upsilon(x),\;\phi(x)\,).$$

Απόδειξη. Από την ταυτότητα της διαίρεσης έχουμε ότι υπάρχει (μοναδικό) $\pi(x) \in \mathbb{F}[x]$, τέτοιο ώστε:

$$\theta(x) \;=\; \pi(x)\,\phi(x) + \upsilon(x).$$

Έστω: $d_1(x) = \mu\kappa\delta(\theta(x), \phi(x))$ και $d_2(x) = \mu\kappa\delta(\upsilon(x), \phi(x))$. Τότε προφανώς το $d_1(x)$ είναι ένας κοινός διαιρέτης των $\upsilon(x) \;=\; \theta(x) - \pi(x)\,\phi(x)$ και $\phi(x)$, άρα $d_1(x) \mid d_2(x)$. Επίσης, το πολυώνυμο $d_2(x)$ είναι ένας κοινός διαιρέτης των $\phi(x)$ και $\theta(x) \;=\; \pi(x)\,\phi(x) + \upsilon(x)$, άρα $d_2(x) \mid d_1(x)$. Όποτε, επειδή τα $d_1(x)$ και $d_2(x)$ είναι μονικά, έχουμε ότι $d_1(x) = d_2(x)$. ό.έ.δ.

Εφαρμόζοντας διαδοχικά την προηγούμενη πρόταση και το γεγονός ότι "Το υπόλοιπο της διαίρεσης δύο πολυωνύμων είναι ή το μηδενικό πολυώνυμο ή έχει βαθμό γνήσια μικρότερο από το βαθμό του διαιρέτη", σε πεπερασμένα βήματα θα φτάσουμε σε μηδενικό υπόλοιπο. Το προτελευταίο (μονικό) υπόλοιπο αυτής της διαδικασίας είναι ο ζητούμενος μ.κ.δ.

Πράγματι, έστω $\theta(x),\ \phi(x) \in \mathbb{F}[x]$ με το $\phi(x)$ μη μηδενικό. Τότε από τον αλγόριθμο της διαίρεσης διαδοχικά έχουμε:

$$\begin{aligned}
\theta(x) &= \pi_1(x)\phi(x) + \upsilon_1(x), && deg(\upsilon_1(x)) < deg(\phi(x))\\
\phi(x) &= \pi_2(x)\upsilon_1(x) + \upsilon_2(x), && deg(\upsilon_2(x)) < deg(\upsilon_1(x))\\
\upsilon_1(x) &= \pi_3(x)\upsilon_2(x) + \upsilon_3(x), && deg(\upsilon_3(x)) < deg(\upsilon_2(x))\\
\upsilon_2(x) &= \pi_4(x)\upsilon_3(x) + \upsilon_4(x), && deg(\upsilon_4(x)) < deg(\upsilon_3(x))\\
&\vdots && \vdots\\
\upsilon_{n-2}(x) &= \pi_n(x)\upsilon_{n-1}(x) + \upsilon_n(x), && deg(\upsilon_n(x)) < deg(\upsilon_{n-1}(x))\\
\upsilon_{n-1}(x) &= \pi_{n+1}(x)\upsilon_n(x) + \mathbf{0}.
\end{aligned}$$

Μετά από n βήματα, ο αριθμός των οποίων δεν ξεπερνά τον βαθμό του $\phi(x)$, το τελευταίο υπόλοιπο $\upsilon_{n+1}(x)$ είναι το μηδενικό πολυώνυμο, αφού:

$$deg(\,\phi(x)\,) > deg(\,\upsilon_1(x)\,) > deg(\,\upsilon_2(x)\,) > deg(\,\upsilon_3(x)\,) > \cdots.$$

Επομένως, έχουμε:

$$\text{μκδ}(\theta(x), \phi(x)) = \text{μκδ}(\phi(x), \upsilon_1(x)) = \text{μκδ}(\upsilon_1(x), \upsilon_2(x)) = \cdots = \text{μκδ}(\upsilon_n(x), \mathbf{0}).$$

Οπότε το αντίστοιχο μονικό πολυώνυμο του $\upsilon_n(x)$ είναι ο ζητούμενος μέγιστος κοινός διαιρέτης.

Για τον υπολογισμό των πολυωνύμων συντελεστών $\alpha(x)$ και $\beta(x)$, στην έκφραση $\text{μκδ}(\,\phi(x),\, \theta(x)\,) = \alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x)$, εφαρμόζουμε αντίστροφη πορεία, ξεκινώντας από την προτελευταία σχέση έχουμε:

$$\upsilon_n(x) = \upsilon_{n-2}(x) - \pi_n(x)\,\upsilon_{n-1}(x).$$

Αλλά

$$\begin{aligned}
\upsilon_{n-1}(x) &= \upsilon_{n-3}(x) - \pi_{n-1}(x)\upsilon_{n-2}(x) \quad \text{και}\\
\upsilon_{n-2}(x) &= \upsilon_{n-4}(x) - \pi_{n-2}(x)\upsilon_{n-3}(x).
\end{aligned}$$

ο Οπότε, αντικαθιστώντας στην προηγούμενη σχέση, έχουμε μια παράσταση της μορφής:

$$\upsilon_n(x) = \beta_{n-3}(x)\,\upsilon_{n-4}(x) + \alpha_{n-2}(x)\,\upsilon_{n-3}(x).$$

Συνεχίζοντας με την ίδια διαδικασία καταλήγουμε σε μια παράσταση της μορφής:

$$\upsilon_n(x) = \beta_2(x)\upsilon_1(x) + \alpha_3(x)\upsilon_2(x)$$

και τελικά $\upsilon_n(x) = \beta_1(x)\theta(x) + \alpha_2(x)\phi(x)$.

Έστω r ο μεγιστοβάθμιος συντελεστής του $\upsilon_n(x)$, τότε προφανώς τα ζητούμενα πολυώνυμα συντελεστές είναι:

$$\alpha(x) = r^{-1}\alpha_2(x) \quad \text{και} \quad \beta(x) = r^{-1}\beta_1(x).$$

Ο αλγόριθμος που περιγράψαμε είναι ο γνωστός ***Ευκλείδειος Αλγόριθμος***.

Άσκηση: Έστω $\phi(x) = 2x^2 - 3x + 2$, $\theta(x) = x^3 - x^2 + 2x - 1 \in \mathbb{Q}[x]$. Να υπολογίσετε τον μκδ$(\,\phi(x),\ \theta(x)\,)$ και να βρεθούν πολυώνυμα $\alpha(x)$, $\beta(x) \in \mathbb{Q}[x]$, έτσι ώστε μκδ$(\,\phi(x),\ \theta(x)\,) = \alpha(x)\phi(x) + \beta(x)\theta(x)$.

Παρατήρηση: Μπορούμε να ορίσουμε τον μέγιστο κοινό διαιρέτη περισσοτέρων, από δύο, πολυωνύμων.

Έστω $\phi_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$ όχι όλα μηδενικά πολυώνυμα. Ένα πολυώνυμο $d(x) \in \mathbb{F}[x]$ θα λέγεται ***μέγιστος κοινός διαιρέτης*** των $\phi_i(x)$ και θα συμβολίζεται με $d(x) = \text{μκδ}(\,\phi_1(x), \phi_2(x), \ldots, \phi_n(x)\,)$ ή απλά:

$$d(x) = (\,\phi_1(x), \phi_2(x), \ldots, \phi_n(x)\,)$$

αν: (i) $d(x) \mid \phi_i(x)$ για κάθε $i = 1, 2, \ldots, n$. Δηλαδή το πολυώνυμο $d(x)$ είναι κοινός διαιρέτης των $\phi_i(x)$.

(ii) Το $d(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\delta(x) \in \mathbb{F}[x]$ με $\delta(x) \mid \phi_i(x)$, τότε $\delta(x) \mid d(x)$. Δηλαδή κάθε κοινός διαιρέτης των $\phi_i(x)$ είναι διαιρέτης του $d(x)$.

Η ύπαρξη, η μοναδικότητα και ο υπολογισμός του μέγιστου κοινού διαιρέτη περισσοτέρων των δύο πολυωνύμων βασίζεται στην εξής απλή παρατήρηση.

Έστω $\phi(x), \theta(x), \sigma(x) \in \mathbb{F}[x]$, τότε υπάρχει ο μκδ$(\,\phi(x), \theta(x), \sigma(x)\,)$ και ισχύει μκδ$(\,\phi(x), \theta(x), \sigma(x)\,) = \text{μκδ}(\,\text{μκδ}(\,\phi(x), \theta(x)\,), \sigma(x)\,)$. Πράγματι έστω:

$$d_1(x) = \text{μκδ}(\,\phi(x), \theta(x)\,) \qquad \text{και} \qquad d_2(x) = \text{μκδ}(\text{μκδ}(\phi(x), \theta(x)), \sigma(x)) = \text{μκδ}(\,d_1(x), \sigma(x)).$$

Έστω $d(x)$ ένας κοινός διαιρέτης των $\phi(x)$, $\theta(x)$ και $\sigma(x)$, άρα $d(x) \mid d_1(x)$. Το $d(x)$ είναι και διαιρέτης του $\sigma(x)$, επομένως $d(x) \mid d_2(x)$. Αλλά $d_2(x) \mid d_1(x)$ και το $d_1(x)$ διαιρεί το $\phi(x)$ και το $\theta(x)$, άρα το $d_2(x)$ είναι ένας κοινός διαιρέτης των $\phi(x)$ και $\theta(x)$, επίσης $d_2(x) \mid \sigma(x)$. Δηλαδή το $d_2(x)$ είναι ένας κοινός διαιρέτης των $\phi(x)$, $\theta(x)$ και $\sigma(x)$, ο οποίος διαιρείται από τον (τυχαίο) κοινό διαιρέτη $d(x)$. Συνεπώς $d_2(x) = \text{μκδ}(\,\phi(x),\, \theta(x),\, \sigma(x)\,)$.

Από την προηγούμενη έκφραση του μ.κ.δ. των πολυωνύμων $\phi(x)$, $\theta(x)$, $\sigma(x)$ εύκολα προκύπτει ότι και στην περίπτωση αυτή ισχύει ένα θεώρημα ανάλογο με το Θεώρημα Α΄.2.7 (Ως άσκηση προσπάθηστε να διατυπώσετε και να αποδείξετε το αντίστοιχο αποτέλεσμα).

Δύο πολυώνυμα $\theta(x)$ και $\phi(x)$ θα λέγονται ***σχετικά πρώτα*** ή ***πρώτα μεταξύ τους*** αν $\text{μκδ}(\,\theta(x),\, \phi(x)\,) = 1$.

Θεώρημα Α΄.2.10. *Έστω* $\phi(x),\ \theta(x),\ \sigma(x) \in \mathbb{F}[x]$ *με* $\text{μκδ}(\,\phi(x),\, \theta(x)\,) = 1$ *και* $\phi(x) \mid \theta(x)\,\sigma(x)$. *Τότε* $\phi(x) \mid \sigma(x)$.

Απόδειξη. Επειδή $\text{μκδ}(\,\phi(x),\, \theta(x)\,) = 1$ υπάρχουν πολυώνυμα $\alpha(x)$ και $\beta(x)$, τέτοια ώστε $\text{μκδ}(\,\phi(x), \theta(x)\,) = \alpha(x)\cdot\phi(x) + \beta(x)\cdot\theta(x) = 1$. Πολλαπλασιάζοντας και τα δύο μέλη της τελευταίας σχέσης με το πολυώνυμο $\sigma(x)$ έχουμε $\alpha(x)\cdot\phi(x)\cdot\sigma(x) + \beta(x)\cdot\theta(x)\cdot\sigma(x) = \sigma(x)$. Το πολυώνυμο $\phi(x)$ διαιρεί το $\beta(x)\cdot\theta(x)\cdot\sigma(x)$. Από την υπόθεση, προφανώς διαιρεί και το $\alpha(x)\cdot\phi(x)\cdot\sigma(x)$, άρα διαιρεί και το άθροισμα $\alpha(x)\cdot\phi(x)\cdot\sigma(x) + \beta(x)\cdot\theta(x)\cdot\sigma(x) = \sigma(x)$.

ό.έ.δ.

Πόρισμα Α΄.2.11. *Έστω* $\phi(x),\ \theta(x),\ \sigma(x) \in \mathbb{F}[x]$ *με* $\text{μκδ}(\,\phi(x),\, \theta(x)\,) = 1$, $\phi(x) \mid \sigma(x)$ *και* $\theta(x) \mid \sigma(x)$. *Τότε* $\phi(x)\,\theta(x) \mid \sigma(x)$

Πρόταση Α΄.2.12. *Έστω* $p(x), p_1(x), \ldots, p_n(x) \in \mathbb{F}[x]$ *ανάγωγα πολυώνυμα. Υποθέτουμε ότι το πολυώνυμο* $p(x)$ *διαιρεί το γινόμενο* $p_1(x)\cdots p_n(x)$, *τότε υπάρχει* $c \in \mathbb{F}$ *έτσι ώστε* $p(x) = c\,p_i(x)$ *για κάποιο δείκτη* i.

Απόδειξη. Επειδή το πολυώνυμο $p(x)$ είναι ανάγωγο, οπότε θα ισχύει ότι: είτε $p(x) \mid p_1(x)$ είτε $\text{μκδ}(\,p(x),\, p_1(x)\,) = 1$ (γιατί;). Αν $p(x) \mid p_1(x)$ έχει καλώς, αν $\text{μκδ}(\,p(x),\, p_1(x)\,) = 1$, τότε από την υπόθεση και την προηγούμενη πρόταση έχουμε ότι το πολυώνυμο $p(x)$ διαιρεί το γινόμενο $p_2(x)\cdots p_n(x)$.

Οπότε πάλι είτε $p(x) \mid p_2(x)$ είτε μκδ$(\, p(x),\ p_2(x)\,) = 1$. Συνεχίζοντας αυτή τη διαδικασία σε πεπερασμένα βήματα θα καταλήξουμε ότι υπάρχει $1 \leq i \leq n$, έτσι ώστε $p(x) \mid p_i(x)$. Τα πολυώνυμα όμως $p(x)$ και $p_i(x)$ είναι ανάγωγα οπότε αναγκαστικά θα υπάρχει $c \in \mathbb{F}$, έτσι ώστε $p(x) = c\, p_i(x)$. ό.έ.δ.

Πρόταση Α΄.2.13. *Κάθε μη σταθερό πολυώνυμο $\phi(x)$ διαιρείται από (τουλάχιστον) ένα ανάγωγο πολυώνυμο.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή στο βαθμό, έστω n, του $\phi(x)$. Αν το $\phi(x)$ είναι ανάγωγο, τότε αυτό διαιρείται από τον εαυτό του. Υποθέτουμε ότι το $\phi(x)$ δεν είναι ανάγωγο και ότι όλα τα μη σταθερά πολυώνυμα με βαθμό μικρότερο του n διαιρούνται από ένα ανάγωγο πολυώνυμο. Για το $\phi(x)$ υπάρχουν μη σταθερά πολυώνυμα $\phi_1(x)$ και $\phi_2(x)$, τέτοια ώστε $\phi(x) = \phi_1(x)\phi_2(x)$. Τα $\phi_1(x)$ και $\phi_2(x)$ έχουν βαθμό μικρότερο του n και, επομένως, από την υπόθεση της επαγωγής κάθε ένα από αυτά διαιρείται από ένα ανάγωγο πολυώνυμο, άρα και το $\phi(x)$ διαιρείται από ένα ανάγωγο πολυώνυμο. ό.έ.δ.

Θεώρημα Α΄.2.14. *Κάθε μη σταθερό πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ γράφεται ως γινόμενο αναγώγων πολυωνύμων στο $\mathbb{F}[x]$ κατά μοναδικό τρόπο. Συγκεκριμένα υπάρχουν μοναδικά μονικά ανάγωγα πολυώνυμα $p_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$ και μοναδικό $c \in \mathbb{F}$, τέτοια ώστε $\phi(x) = c\, p_1(x) p_2(x) \cdots p_n(x)$.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή στον βαθμό του πολυωνύμου $\phi(x)$. Αν $deg(\, \phi(x)\,) = 1$, τότε το πολυώνυμο $\phi(x)$ είναι ανάγωγο και το θεώρημα ισχύει (εδώ θεωρούμε ότι έχουμε γινόμενο με ένα ανάγωγο όρο). Υποθέτουμε ότι το θεώρημα ισχύει για όλα τα πολυώνυμα με βαθμό μικρότερου του βαθμού του $\phi(x)$. Αν το $\phi(x)$ είναι ανάγωγο, τότε πάλι το θεώρημα ισχύει. Υποθέτουμε ότι το $\phi(x)$ δεν είναι ανάγωγο. Άρα υπάρχουν μη σταθερά πολυώνυμα $\phi_1(x)$ και $\phi_2(x)$, τέτοια ώστε $\phi(x) = \phi_1(x)\phi_2(x)$. Ο βαθμός των $\phi_1(x)$ και $\phi_2(x)$ είναι μικρότερος του βαθμού του $\phi(x)$, άρα το θεώρημα ισχύει για αυτά τα πολυώνυμα, όποτε και το $\phi(x)$ μπορεί να γραφεί στη μορφή $\phi(x) = c\, p_1(x) p_2(x) \cdots p_n(x)$ με $c \in \mathbb{F}[x]$ και τα $p_i(x)$ μονικά και ανάγωγα.

Ας υποθέσουμε τώρα ότι:

$$\phi(x) = c_1 p_1(x) p_2(x) \cdots p_n(x) = c_2 q_1(x) q_2(x) \cdots q_m(x), \quad \text{όπου } c_1, c_2 \in \mathbb{F}$$

και τα πολυώνυμα:

$$p_1(x), p_2(x), \ldots, p_n(x), q_1(x), q_2(x), \ldots, q_m(x)$$

είναι μονικά και ανάγωγα επί του $\mathbb{F}$. Το πολυώνυμο $q_m(x)$ διαιρεί το γινόμενο $c_1\, p_1(x)\, p_2(x) \cdots p_n(x)$, επομένως, σύμφωνα με την προηγούμενη πρόταση, υπάρχει $c \in \mathbb{F}$, έτσι ώστε $q_m(x) = c p_i(x)$ για κάποιο δείκτη i. Αλλά τα $q_m(x)$ και $p_i(x)$ είναι μονικά, οπότε $q_m(x) = p_i(x)$ και αλλάζοντας, εν ανάγκη, τη σειρά των παραγόντων μπορούμε να υποθέσουμε ότι $q_m(x) = p_n(x)$. Τώρα από τη σχέση $c_1\, p_1(x) p_2(x) \cdots p_n(x) = c_2\, q_1(x) q_2(x) \cdots q_m(x)$ έχουμε ότι:

$$c_1 p_1(x) p_2(x) \cdots p_{n-1}(x) = c_2 q_1(x) q_2(x) \cdots q_{m-1}(x).$$

Ο βαθμός όμως του πολυωνύμου $c_1\, p_1(x) p_2(x) \cdots p_{n-1}(x)$ είναι μικρότερος από τον βαθμό του $\phi(x)$, επομένως από την υπόθεση της επαγωγής έχουμε ότι $c_1 = c_2$, $n-1 = m-1$ και αλλάζοντας, εν ανάγκη, την σειρά των παραγόντων $p_i(x) = q_i(x)$. ό.έ.δ.

Παρατηρήσεις Α΄.2.15. 1. Στην προηγούμενη γραφή ενός πολυωνύμου ως γινόμενο αναγώγων μονικών πολυωνύμων οι παράγοντες $p_i(x)$ δεν είναι κατ' ανάγκη διακεκριμένοι, οπότε θα μπορούσαμε να γράψουμε το πολυώνυμο στη μορφή $\phi(x) = c_1\, p_1^{\lambda_1}(x) p_2^{\lambda_2}(x) \cdots p_m^{\lambda_m}(x)$, όπου τώρα τα πολυώνυμα $p_i(x)$ είναι διακεκριμένα και τα λ_i είναι θετικοί ακέραιοι αριθμοί. Η (μοναδική) αυτή γραφή ονομάζεται **ανάλυση του** $\phi(x)$ **σε γινόμενο μονικών αναγώγων πολυωνύμων**.

2. Όπως έχουμε επισημάνει, έχει σημασία επί ποίου σώματος συντελεστών εξετάζουμε αν ένα πολυώνυμο είναι ανάγωγο. Επομένως, θα έχουμε και την αντίστοιχη ανάλυση ενός πολυωνύμου σε γινόμενο μονικών αναγώγων πολυωνύμων. Για παράδειγμα, το πολυώνυμο $x^4 - x^2 - 2 \in \mathbb{R}[x]$ έχει την ανάλυση $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$, ενώ το ίδιο πολυώνυμο, αν θεωρηθεί ως στοιχείο του $\mathbb{C}[x]$, έχει την ανάλυση:

$$x^4 - x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})(x - i)(x + i).$$

3. Όπως βλέπουμε, η προηγούμενη απόδειξη δεν μας δίνει μια μέθοδο (αλγόριθμο) για να υπολογίζουμε τους ανάγωγους παράγοντες στην ανάλυση ένος πολυωνύμου. Το πρόβλημα του προσδιορισμού των αναγώγων παραγόντων ενός πολυωνύμου είναι αρκετά δύσκολο και είναι ανάλογο με το πρόβλημα του προσδιορισμού των πρώτων παραγόντων στους οποίους αναλύεται ένας ακέραιος αριθμός.

Α΄.2.3 Ελάχιστο κοινό πολλαπλάσιο πολυωνύμων

Πριν δώσουμε τον ορισμό του ελαχίστου κοινού πολλαπλασίου δύο πολυωνύμων, θα θέλαμε να παρατηρήσουμε ότι, αν $\phi(x),\ \theta(x) \in \mathbb{F}[x]$, τότε το πολυώνυμο $\phi(x)\,\theta(x)$ διαιρείται από τα δύο πολυώνυμα $\phi(x)$ και $\theta(x)$. Δηλαδή είναι ένα *κοινό πολλαπλάσιο* των $\phi(x)$ και $\theta(x)$. Όμως, αν ένα πολυώνυμο $\sigma(x)$ με συντελεστή μεγιστοβαθμίου όρου c είναι πολλαπλάσιο ενός πολυωνύμου, έστω $\delta(x)$, τότε και το πολυώνυμο $c^{-1}\,\sigma(x)$ είναι πολλαπλάσιο του $\delta(x)$ (γιατί;). Επομένως, για τα πολυώνυμα $\phi(x)$ και $\theta(x)$ υπάρχουν μονικά κοινά πολλαπλάσια.

Ορισμός Α΄.2.16. *Έστω $\phi(x),\ \theta(x) \in \mathbb{F}[x]$. Ένα πολυώνυμο $m(x) \in \mathbb{F}[x]$ θα λέγεται* **ελάχιστο κοινό πολλαπλάσιο** *των $\phi(x)$ και $\theta(x)$ και θα συμβολίζεται με $m(x) = \text{εκπ}(\,\phi(x),\ \theta(x)\,)$ ή απλά $m(x) = [\,\phi(x),\ \theta(x)\,]$ αν:*

(i) $\phi(x) \mid m(x)$ και $\theta(x) \mid m(x)$. Δηλαδή το πολυώνυμο $m(x)$ είναι κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$.

(ii) Το $m(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\mu(x) \in F[x]$ με $\phi(x) \mid \mu(x)$ και $\theta(x) \mid \mu(x)$, τότε $m(x) \mid \mu(x)$. Δηλαδή κάθε κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$ είναι πολλαπλάσιο του $m(x)$.

Ο ορισμός δεν εξασφαλίζει την υπάρξη ενός ε.κ.π. δύο πολυωνύμων.

Μπορούμε όμως να δούμε εύκολα ότι αν υπάρχει ε.κ.π. των $\phi(x)$ και $\theta(x)$, τότε αυτό είναι μοναδικό. Πράγματι υποθέτουμε ότι υπάρχουν δύο πολυώνυμα $m_1(x)$ και $m_2(x)$ με τις ιδιότητες του ορισμού. Τότε από τις (i) και (iii) του ορισμού έχουμε ότι $m_1(x) \mid m_2(x)$ και $m_2(x) \mid m_1(x)$. Δηλαδή υπάρχει $c \in \mathbb{F}$, τέτοιο ώστε $m_1(x) = cm_2(x)$. Αλλά τα $m_1(x)$, $m_2(x)$ είναι μονικά. Άρα $m_1(x) = m_2(x)$.

Πριν αποδείξουμε ότι το ε.κ.π. δύο πολυωνύμων υπάρχει επισημαίνουμε ότι αν (τουλάχιστον) ένα από τα δύο πολυώνυμα είναι το μηδενικό πολυώνυμο, τότε το μηδενικό πολυώνυμο είναι το μοναδικό κοινό πολλαπλάσιο των δύο πολυωνύμων. Επομένως, μπορούμε να υποθέτουμε ότι τα δύο πολυώνυμα είναι μη μηδενικά.

Πρόταση Α΄.2.17. *Έστω δύο μη μηδενικά πολυώνυμα* $\phi(x),\ \theta(x) \in \mathbb{F}[x]$. *Τότε το ε.κ.π. των δύο πολυωνύμων είναι το μονικό πολυώνυμο με τον μικρότερο βαθμό, το οποίο διαιρείται από το* $\phi(x)$ *και* $\theta(x)$.

Απόδειξη. Έστω:

$$\mathcal{V} = \{\, \sigma(x) \in \mathbb{F}[x] \mid \sigma(x) \text{ κοινό πολλαπλάσιο των } \phi(x) \text{ και } \theta(x) \,\}.$$

Το σύνολο $\mathcal{V}$ περιέχει μη μηδενικά πολυώνυμα (γιατί;). Επίσης, όπως έχουμε παρατηρήσει, το $\mathcal{V}$ περιέχει (και) μονικά πολυώνυμα. Έστω $m(x) \in \mathcal{V}$ ένα μονικό πολυώνυμο με τον μικρότερο βαθμό.

Το $m(x)$ διαιρεί κάθε πολυώνυμο που ανήκει στο σύνολο $\mathcal{V}$. Πράγματι, αν $\sigma(x)$ είναι ένα στοιχείο του συνόλου $\mathcal{V}$, τότε από τον αλγόριθμο της διαίρεσης έχουμε ότι υπάρχουν (μοναδικά) πολυώνυμα $\pi(x),\ \upsilon(x) \in F[x]$, τέτοια ώστε $\sigma(x) = \pi(x)\, m(x) + \upsilon(x)$ με $deg(\,\upsilon(x)\,) < deg(\,m(x)\,)$, εκτός εάν το πολυώνυμο $\upsilon(x)$ είναι το μηδενικό πολυώνυμο. Τα πολυώνυμα $\phi(x)$ και $\theta(x)$ διαιρούν το πολυώνυμο $\sigma(x) - \pi(x)\, m(x) = \upsilon(x)$ (γιατί;). Δηλαδή το $\upsilon(x)$ είναι κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)\,\}$, άρα ένα στοιχείο του συνόλου $\mathcal{V}$. Τούτο είναι άτοπο από την επιλογή του πολυωνύμου $m(x)$. Άρα $\upsilon(x) = \mathbf{0}$. ό.έ.δ.

Παρατήρηση Α΄.2.18. Έστω δύο μη μηδενικά πολυώνυμα $\phi(x),\ \theta(x) \in \mathbb{F}[x]$. Αν υποθέσουμε ότι οι μεγιστοβάθμιοι συντελεστές των $\phi(x)$ και $\theta(x)$ είναι αντίστοιχα c και r, τότε προφανώς:

$$\varepsilon\kappa\pi(\phi(x), \theta(x)) = \varepsilon\kappa\pi(c^{-1}\phi(x), r^{-1}\theta(x)).$$

Επομένως, για την εύρεση του ε.κ.π. δύο πολυωνύμων αρκεί να περιορισθούμε σε μονικά πολυώνυμα.

Σχόλιο Για το ελάχιστο κοινό πολλαπλάσιο δύο πολυωνύμων δεν ισχύει ένα θεώρημα *ανάλογο* με το Θεώρημα Α΄.2.7. Πολύ δε περισσότερο δεν ισχύει

κάτι ανάλογο με τον Ευκλείδειο Αλγόριθμο για τον υπολογισμό του ελαχίστου κοινού πολλαπλασίου δύο πολυωνύμων. Ισχύει όμως η εξής σημαντική σχέση που συνδέει τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο μονικών πολυωνύμων $\phi(x)$ και $\theta(x)$:

$$\text{εκπ}(\phi(x), \theta(x)) \cdot \text{μκδ}(\phi(x), \theta(x)) = \phi(x) \cdot \theta(x),$$

η απόδειξη της οποίας αφίεται ως άσκηση.

Μπορούμε να ορίσουμε το ελάχιστο κοινό πολλαπλάσιο περισσοτέρων, από δύο, πολυωνύμων.

Έστω $\phi_i(x) \in \mathbb{F}[x]$, $i = 1, 2, \ldots, n$ μη μηδενικά πολυώνυμα. Ένα πολυώνυμο $m(x) \in \mathbb{F}[x]$ θα λέγεται ***ελάχιστο κοινό πολλαπλάσιο*** των $\phi_i(x)$ και θα συμβολίζεται με $m(x) = \text{εκπ}(\, \phi_1(x), \phi_2(x), \ldots, \phi_n(x)\,)$ ή απλά:

$$m(x) = [\, \phi_1(x), \phi_2(x), \ldots, \phi_n(x)\,].$$

Αν: (i) $\phi_i(x) \mid m(x)$. Δηλαδή το πολυώνυμο $m(x)$ είναι κοινό πολλαπλάσιο των $\phi_i(x)$.

(ii) Το $m(x)$ είναι μονικό πολυώνυμο.

(iii) Αν $\mu(x) \in \mathbb{F}[x]$ με $\phi_i(x) \mid \mu(x)$, τότε $m(x) \mid \mu(x)$. Δηλαδή κάθε κοινό πολλαπλάσιο των $\phi_i(x)$ είναι πολλαπλάσιο του $m(x)$.

Παρατηρήσεις Α΄.2.19. 1. Η ύπαρξη, η μοναδικότητα και ο υπολογισμός του ελαχίστου κοινού πολλαπλασίου περισσοτέρων των δύο πολυωνύμων βασίζεται στην εξής απλή παρατήρηση. Έστω $\phi(x), \theta(x), \sigma(x) \in \mathbb{F}[x]$. Τότε υπάρχει το $\text{εκπ}(\, \phi(x), \theta(x), \sigma(x)\,)$ και ισχύει:

$$\text{εκπ}(\phi(x), \theta(x), \sigma(x)) = \text{εκπ}(\text{εκπ}(\phi(x), \theta(x)), \sigma(x)).$$

Πράγματι, έστω:

$$m_1(x) = \text{εκπ}(\phi(x), \theta(x)) \quad \text{και}$$
$$m_2(x) = \text{εκπ}(\text{εκπ}(\phi(x), \theta(x)), \sigma(x)) = \text{εκπ}(m_1(x), \sigma(x)).$$

Έστω $m(x)$ ένα κοινό πολλαπλάσιο των $\phi(x)$, $\theta(x)$ και $\sigma(x)$, άρα ισχύει ότι $m_1(x) \mid m(x)$. Το $m(x)$ είναι όμως και πολλαπλάσιο του $\sigma(x)$, επομένως $m_2(x) \mid m(x)$. Αλλά $m_1(x) \mid m_2(x)$ και το $m_1(x)$ είναι πολλαπλάσιο

των $\phi(x)$ και $\theta(x)$, άρα το $m_2(x)$ είναι ένα κοινό πολλαπλάσιο των $\phi(x)$ και $\theta(x)$, επίσης το $\sigma(x) \mid m_2(x)$. Άρα το $m_2(x)$ είναι ένα κοινό πολλαπλάσιο των $\phi(x)$, $\theta(x)$ και $\sigma(x)$, το οποίο διαιρεί το (τυχαίο) κοινό πολλαπλάσιο $m(x)$. Συνεπώς $m_2(x) = \text{εκπ}(\,\phi(x),\, \theta(x),\, \sigma(x)\,)$.

2. Χρησιμοποιώντας την ανάλυση ενός πολυωνύμου σε γινόμενο αναγώγων πολυωνύμων μπορούμε να υπολογίσουμε τον μέγιστο κοινό διαιρέτη και το ελάχιστο κοινό πολλαπλάσιο δύο πολυωνύμων.

   Έστω δύο πολυώνυμα $\phi(x)$ και $\theta(x) \in \mathbb{F}[x]$ και έστω:

$$\phi(x) = c_1 p_1^{\lambda_1}(x) p_2^{\lambda_2}(x) \cdots p_m^{\lambda_m}(x) \quad \text{και} \quad \theta(x) = c_2 p_1^{\nu_1}(x) p_2^{\nu_2}(x) \cdots p_m^{\nu_m}(x)$$

   οι αναλύσεις τους σε γινόμενο μονικών αναγώγων πολυωνύμων, όπου τα λ_i και ν_i ενδέχεται να είναι και μηδέν όταν ένας παράγοντας δεν εμφανίζεται στην αντίστοιχη ανάλυση του πολυωνύμου. Θέτουμε $\mu_i = min(\,\lambda_i, \nu_i\,)$ και $M_i = max(\,\lambda_i, \nu_i\,)$. Τότε μπορούμε να αποδείξουμε ότι:

$$\begin{aligned} \text{μκδ}(\phi(x), \theta(x)) &= p_1^{\mu_1}(x) p_2^{\mu_2}(x) \cdots p_m^{\mu_m}(x) \quad \text{και} \\ \text{εκπ}(\phi(x), \theta(x)) &= p_1^{M_1}(x) p_2^{M_2}(x) \cdots p_m^{M_m}(x). \end{aligned}$$

Α΄.2.4 Ρίζες πολυωνύμων

Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{E}$ μια επέκταση του $\mathbb{F}$. Αν $c \in \mathbb{E}$, ορίζουμε την απεικόνιση $\varphi_c : \mathbb{F}[x] \longrightarrow \mathbb{E}$ ως εξής: Αν $\sigma(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, τότε $\varphi_c(\sigma(x)) =: \sigma(c) = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0$. Δηλαδή η εικόνα του $\sigma(x)$ μέσω της φ_c είναι η τιμή του πολυωνύμου $\sigma(x)$ στη θέση c. Αν $\sigma(x) \in \mathbb{F}[x]$, έτσι ώστε $\sigma(c) = 0$, τότε το c θα ονομάζεται **ρίζα** του $\sigma(x)$.

Προφανώς, ένα $c \in \mathbb{E}$ είναι ρίζα του $\sigma(x) \in \mathbb{F}[x]$, αν και μόνο αν υπάρχει $\pi(x) \in \mathbb{E}[x]$, έτσι ώστε $\sigma(x) = (x - c) \cdot \pi(x)$. [Προσοχή! το $\pi(x)$ δεν έχει κατ' ανάγκη συντελεστές από το σώμα $\mathbb{F}$.] Επομένως, συμπεραίνουμε ότι ο αριθμός των ριζών ενός μη μηδενικού πολυωνύμου δεν υπερβαίνει τον βαθμό του.

Πρόταση Α΄.2.20. *Έστω $\varphi(x)$, $\vartheta(x) \in \mathbb{F}[x]$ δύο πολυώνυμα βαθμού (το πολύ) n. Υποθέτουμε ότι υπάρχουν διακεκριμένα $c_1, c_2, \ldots, c_{n+1} \in \mathbb{E}$ σε μια επέ-*

κταση του $\mathbb{F}$, έτσι ώστε $\varphi(c_i) = \vartheta(c_i)$ για όλα τα $i = 1, 2, \ldots, n+1$, τότε τα δύο πολυώνυμα $\varphi(x)$, $\vartheta(x)$ είναι ίσα.

Απόδειξη. Από τη σχέση $\varphi(c_i) = \vartheta(c_i)$ έπεται ότι $\varphi(c_i) - \vartheta(c_i) = 0$ για όλα τα $i = 1, 2, \ldots, n+1$. Δηλαδή το πολυώνυμο $(\varphi - \vartheta)(x) \in \mathbb{F}[x]$, το οποίο είναι βαθμού το πολύ n, έχει $n+1$ το πλήθος ρίζες. Αυτό σημαίνει ότι το $(\varphi - \vartheta)(x)$ είναι το μηδενικό πολυώνυμο. Άρα $\varphi(x) = \vartheta(x)$. ό.έ.δ.

Η απεικόνιση φ_c είναι ομομορφισμός δακτυλίων (ο έλεγχος είναι εύκολος). Αν $p(x)$ είναι ένα στοιχείο του πυρήνα της φ_c, τότε $\varphi_c(p(x)) = p(c) = 0$. Δηλαδή ο πυρήνας της φ_c αποτελείται από όλα τα πολυώνυμα του $\mathbb{F}[x]$, τα οποία έχουν ρίζα το στοιχείο c.

Αν ο πυρήνας $Ker\,\varphi_c$ είναι μη μηδενικό ιδεώδες, δηλαδή υπάρχει μη μηδενικό πολυώνυμο $p(x)$ με συντελεστές από το σώμα $\mathbb{F}$, του οποίου ρίζα είναι το στοιχείο c, τότε το c θα λέγεται **αλγεβρικό** επί του σώματος $\mathbb{F}$. Διαφορετικά ονομάζεται **υπερβατικό** επί του $\mathbb{F}$.

Αν κάθε στοιχείο μιας επέκτασης $\mathbb{E}$ του σώματος $\mathbb{F}$ είναι αλγεβρικό, τότε η $\mathbb{E}$ ονομάζεται αλγεβρική επέκταση του $\mathbb{F}$.

Πρόταση Α΄.2.21. *Μια πεπερασμένη επέκταση $\mathbb{E}$ του σώματος $\mathbb{F}$ είναι αλγεβρική.*

Απόδειξη. Έστω $[\mathbb{E} : \mathbb{F}] = n$ ο βαθμός επέκτασης. Τότε για κάθε $c \in \mathbb{E}$ τα στοιχεία $1, c, c^2, \ldots, c^n$ είναι γραμμικά εξαρτημένα. Οπότε, ως άσκηση, μπορείτε να συμπεράνετε ότι για κάθε $c \in \mathbb{E}$ υπάρχει μη μηδενικό πολυώνυμο $\phi_c(x) \in \mathbb{F}[x]$, του οποίου ρίζα είναι το στοιχείο c. ό.έ.δ.

Πρόταση Α΄.2.22. *Έστω $c \in \mathbb{E}$ ένα στοιχείο αλγεβρικό επί του $\mathbb{F}$. Τότε υπάρχει μοναδικό ανάγωγο μονικό πολυώνυμο $m_c(x) \in \mathbb{F}[x]$ με ρίζα το στοιχείο c.*

Απόδειξη. Ο πυρήνας $Ker\,\varphi_c$ είναι ιδεώδες του $\mathbb{F}[x]$. Από την Παρατήρηση Α΄.2.5 έπεται ότι υπάρχει μοναδικό μονικό πολυώνυμο $m_c(x) \in \mathbb{F}[x]$, έτσι ώστε $Ker\,\varphi_c = \langle m_c(x) \rangle$. Θα δείξουμε ότι το $m_c(x)$ είναι ανάγωγο. Υποθέτουμε ότι $m_c(x) = p_1(x) \cdot p_2(x)$ με $p_1(x), p_2(x) \in \mathbb{F}[x]$. Τότε έχουμε $m_c(c) =$

$p_1(c)\cdot p_2(c) = 0 \in \mathbb{E}$. Δηλαδή $p_1(c) = 0$ ή $p_2(c) = 0$. Αλλά το $m_c(x)$ είναι ελαχίστου βαθμού με αυτή την ιδιότητα, άρα αναγκαστικά ένα από τα $p_i(x)$ είναι σταθερό πολυώνυμο. ό.έ.δ.

Το πολυώνυμο $m_c(x)$ ομομάζεται **ελάχιστο** πολυώνυμο του στοιχείου c.

Πρόταση Α΄.2.23. *Έστω* $\mathbf{0} \neq r(x) \in \mathbb{F}[x]$.

i) Τα στοιχεία του δακτυλίου πηλίκων $\mathbb{F}[x]/\langle\, r(x)\,\rangle$ *είναι της μορφής* $\alpha(x) + \langle\, r(x)\,\rangle$, *όπου* $\alpha(x) = \mathbf{0}$ *ή ο βαθμός του* $\alpha(x)$ *είναι μικρότερος από τον βαθμό του* $r(x)$.

ii) Ένα στοιχείο $\alpha(x) + \langle\, r(x)\,\rangle \in \mathbb{F}[x]/\langle\, r(x)\,\rangle$ *είναι αντιστρέψιμο, αν και μόνο αν* $\text{μκδ}(\,\alpha(x),\ r(x)\,) = 1$.

Απόδειξη. Το πρώτο μέρος έπεται από την ταυτότητα της διαίρεσης και τον ορισμό του συμπλόκου (βλέπε σελίδα 399).

Ένα $\alpha(x) + \langle\, r(x)\,\rangle \in \mathbb{F}[x]/\langle\, r(x)\,\rangle$ είναι αντιστρέψιμο, αν και μόνο αν υπάρχει $\beta(x) + \langle\, r(x)\,\rangle \in \mathbb{F}[x]/\langle\, r(x)\,\rangle$, έτσι ώστε $(\alpha(x) + \langle\, r(x)\,\rangle)\cdot(\beta(x) + \langle\, r(x)\,\rangle) = 1 + \langle\, r(x)\,\rangle$, αν και μόνο αν $\alpha(x)\cdot\beta(x) - 1 \in \langle\, r(x)\,\rangle$, αν και μόνο αν υπάρχει πολυώνυμο $s(x) \in \mathbb{F}[x]$, έτσι ώστε $\alpha(x)\cdot\beta(x) - 1 = s(x)\cdot r(x)$, αν και μόνο αν $\text{μκδ}(\,\alpha(x),\ r(x)\,) = 1$ (βλέπε Θεώρημα Α΄.2.7). ό.έ.δ.

Πόρισμα Α΄.2.24. *Έστω* $r(x) \in \mathbb{F}[x]$. *Ο δακτύλιος πηλίκων* $\mathbb{F}[x]/\langle\, r(x)\,\rangle$ *είναι σώμα, αν και μόνο αν το πολυώνυμο* $r(x)$ *είναι ανάγωγο επί του* $\mathbb{F}$.

Απόδειξη. Ο $\mathbb{F}[x]/\langle\, r(x)\,\rangle$ είναι σώμα, αν και μόνο αν κάθε μη μηδενικό στοιχείο του έχει αντίστροφο, αν και μόνο αν (σύμφωνα με την προηγούμενη πρόταση) κάθε μη μηδενικό πολυώνυμο με βαθμό μικρότερο από το βαθμό του $r(x)$ είναι πρώτο προς το $r(x)$, αν και μόνο αν το $r(x)$ είναι ανάγωγο. ό.έ.δ.

Έστω $\varphi_c : \mathbb{F}[x] \longrightarrow \mathbb{E}$ ο ομομορφισμός που ορίσαμε στην αρχή της παραγράφου και $\mathbb{F}[c] = \text{Im}\,\varphi_c = \{\,\sigma(c) \mid \sigma(x) \in \mathbb{F}[x]\,\}$.

Πόρισμα Α΄.2.25. *Ο δακτύλιος εικόνα* $\mathbb{F}[c]$ *είναι σώμα, αν και μόνο αν το στοιχείο* $c \in \mathbb{E}$ *είναι αλγεβρικό επί του* $\mathbb{F}$.

Απόδειξη. Η απόδειξη είναι άμεση από το $1^ο$ Θεώρημα Ισομορφισμών και τις Προτάσεις Α΄.2.22 και Α΄.2.23. ό.έ.δ.

Σχόλιο Α΄.2.26. Προφανώς, στην περίπτωση που το στοιχείο c είναι αλγεβρικό επί του $\mathbb{F}$, ισχύει $\mathbb{F}[c] = \mathbb{F}(c)$ και ο βαθμός επέκτασης $[\mathbb{F}(c) : \mathbb{F}]$ είναι πεπερασμένος (γιατί;).

Άσκηση. Να αποδείξετε ότι ο βαθμός επέκτασης $[\mathbb{F}(c) : \mathbb{F}]$ είναι ίσος με τον βαθμό του ελαχίστου πολυωνύμου του c.

Έστω $\mathbb{F}$ ένα σώμα και $\phi(x) \in \mathbb{F}[x]$. Ένα πρόβλημα που αντιμετωπίζουμε, είναι κατά πόσον υπάρχει μια επέκταση $\mathbb{F} \mid \mathbb{E}$ στην οποία το πολυώνυμο $\phi(x)$ έχει (τουλάχιστον) μια ρίζα και κατόπιν να υπολογίσουμε (αν είναι δυνατόν) μια ρίζα του $\phi(x)$.

Το πρόβλημα αυτό είναι δυϊκό του προβλήματος κατά πόσον ένα στοιχείο μιας επέκτασης του σώματος $\mathbb{F}$ είναι αλγεβρικό επί του $\mathbb{F}$.

Έστω $\phi(x) = p_1(x)p_2(x)\cdots p_k(x)$ η ανάλυση του $\phi(x)$ σε γινόμενο αναγώγων πολυωνύμων. Υποθέτουμε ότι το $\phi(x)$ έχει μια ρίζα ξ σε μια επέκταση του $\mathbb{F}$. Τότε το ξ είναι ρίζα ενός από τους παράγοντες $p_i(x)$. Αντίστροφα, αν ένας από τους παράγοντες $p_i(x)$ έχει μια ρίζα, τότε προφανώς και το πολυώνυμο $\phi(x)$ έχει μια ρίζα. Επομένως, αρκεί να εξασφαλίσουμε ότι τα ανάγωγα πολυώνυμα έχουν ρίζες.

Θεώρημα Α΄.2.27. *Για κάθε ανάγωγο πολυώνυμο $p(x) \in \mathbb{F}[x]$ υπάρχει μια επέκταση $\mathbb{F} \mid \mathbb{E}$ και ένα $c \in \mathbb{E}$ με $p(c) = 0$.*

Απόδειξη. Από το Πόρισμα Α΄.2.24, επειδή το $p(x)$ είναι ανάγωγο, έχουμε ότι ο δακτύλιος πηλίκων $\mathbb{F}[x]/\langle\, p(x)\,\rangle$ είναι σώμα.

Μέσω του φυσικού ομομορφισμού $\varphi : \mathbb{F}[x] \longrightarrow \mathbb{F}[x]/\langle\, p(x)\,\rangle$ το σώμα $\mathbb{F}$ εμφυτεύεται στο σώμα $\mathbb{E} = \mathbb{F}[x]/\langle\, p(x)\,\rangle$. [Ο περιορισμός της φ στο $\mathbb{F}$ είναι μονομορφισμός (γιατί;).] Έστω $c = x + \langle\, p(x)\,\rangle \in \mathbb{E}$. Τότε έχουμε:

$$p(c) = p(x + \langle\, p(x)\,\rangle) = p(x) + \langle\, p(x)\,\rangle = 0 \in \mathbb{E}.$$

ό.έ.δ.

Πόρισμα Α΄.2.28. *Για κάθε πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ υπάρχει μια επέκταση $\mathbb{F} \mid \mathbb{E}$, έτσι ώστε το $\phi(x)$ να αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο $\mathbb{E}[x]$. Δηλαδή το $\phi(x)$ έχει όλες τις ρίζες του στο σώμα $\mathbb{E}$.*

Απόδειξη. Έστω n ο βαθμός του πολυωνύμου $\phi(x)$. Αν $n = 1$, τότε $\mathbb{E} = \mathbb{F}$. Υποθέτουμε ότι ο ισχυρισμός ισχύει για όλα τα πολυώνυμα με βαθμό μικρότερο του n. Από τα προηγούμενα μπορούμε να υποθέσουμε ότι το $\phi(x)$ είναι ανάγωγο (γιατί;). Από το προηγούμενο θεώρημα υπάρχει επέκταση $\mathbb{E}_0$ του $\mathbb{F}$ και $c \in \mathbb{E}_0$, έτσι ώστε $\phi(x) = (x-c)\cdot\tau(x)$ με $\tau(x) \in \mathbb{E}_0[x]$. Από την υπόθεση της επαγωγής υπάρχει επέκταση $\mathbb{E}$ του $\mathbb{E}_0$, όπου το $\tau(x)$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων. Άρα το $\phi(x) = (x-c)\cdot\tau(x)$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο σώμα $\mathbb{E}$. ό.έ.δ.

Άσκηση. Έστω $\varphi(x),\ \vartheta(x)$ δύο πολυώνυμα με συντελεστές από το σώμα $\mathbb{F}$. Υποθέτουμε ότι τα δύο πολυώνυμα έχουν μια κοινή ρίζα και ότι το πολυώνυμο $\varphi(x)$ είναι ανάγωγο επί του $\mathbb{F}$. Δείξτε ότι το $\varphi(x)$ διαιρεί το $\vartheta(x)$.

Ορισμός Α΄.2.29. *Έστω $\mathbb{F}$ ένα σώμα και $\phi(x) \in \mathbb{F}[x]$. Μια επέκταση $\mathbb{E}$ του $\mathbb{F}$ ονομάζεται* ***σώμα ριζών*** *του πολυωνύμου $\phi(x)$, αν το $\phi(x)$ αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο $\mathbb{E}[x]$ και, αν υπάρχει σώμα $\mathbb{K}$ με $\mathbb{F} \le \mathbb{K} \le \mathbb{E}$, έτσι ώστε το το $\phi(x)$ να αναλύεται σε γινόμενο πρωτοβαθμίων παραγόντων στο $\mathbb{K}[x]$, τότε $\mathbb{K} = \mathbb{E}$.*

Πρόταση Α΄.2.30. *Κάθε πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ έχει ένα σώμα ριζών.*

Απόδειξη. Από το Πόρισμα Α΄.2.24 έπεται ότι υπάρχει μια επέκταση $\mathbb{E}$, η οποία περιέχει όλες τις ρίζες του $\phi(x)$. Έστω $\xi_1,\ \xi_2,\ \dots,\ \xi_k \in \mathbb{E}$ οι διακεκριμένες ρίζες του $\phi(x)$. Το σώμα $\mathbb{F}(\xi_1,\ \xi_2,\ \dots,\ \xi_k)$ που προκύπτει με την προσάρτηση των ριζών του $\phi(x)$ στο σώμα $\mathbb{F}$ είναι προφανώς ένα σώμα ριζών του $\phi(x)$, αφού πληροί τις ιδιότητες του ορισμού. ό.έ.δ.

Από τα προηγούμενα δεν αποκλείεται ένα πολυώνυμο να έχει πολλά σώματα ριζών. Στην πραγματικότητα όμως υπάρχει μοναδικό σώμα ριζών ενός πολυωνύμου.

Θεώρημα Α΄.2.31. *Έστω $\phi(x) \in \mathbb{F}[x]$ ένα πολυώνυμο και $\mathbb{K},\ \mathbb{L}$ δύο σώματα ριζών του $\phi(x)$. Τα $\mathbb{K}$ και $\mathbb{L}$ είναι ισόμορφα.*

Η απόδειξη του προηγουμένου Θεωρήματος, αν και σαν ιδέα δεν είναι πολύ δύσκολη, είναι μακροσκελής και παραλείπεται. Για μια απόδειξη θα μπορούσατε να ανατρέξετε στο Ανδρεαδάκης [1992].

Στο εξής όμως εμείς θα ταυτίζουμε τα ισόμορφα σώματα ριζών ενός πολυωνύμου και θα λέμε **το** σώμα ριζών του πολυωνύμου.

Για παράδειγμα, το σώμα ριζών του πολυωνύμου $x^2-2 \in \mathbb{Q}[x]$ είναι το $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2-2 \rangle$.

Έστω $\phi(x) \in \mathbb{F}[x]$ ένα πολυώνυμο και c μια ρίζα του σε μια επέκταση $\mathbb{E}$. Τότε το $x-c$ διαιρεί το $\phi(x)$ στον δακτύλιο $\mathbb{E}[x]$. Έστω $(x-c)^m$ η μεγαλύτερη δύναμη του $x-c$, η οποία διαιρεί το $\phi(x)$. Δηλαδή $\phi(x) = (x-c)^m \cdot \sigma(x)$ με $\sigma(x) \in \mathbb{E}[x]$ και $\sigma(c) \neq 0$. Στην περίπτωση αυτή η ρίζα c ονομάζεται ρίζα **πολλαπλότητας** m.

Έστω $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ και $\phi'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in \mathbb{F}[x]$ η (τυπική) παράγωγος του πολυωνύμου $\phi(x)$. Είναι εύκολο να αποδείξουμε τους γνωστούς κανόνες παραγώγισης.

(i) $(\phi(x)+\theta(x))' = \phi'(x)+\theta'(x)$

(ii) $(\phi(x)\cdot\theta(x))' = \phi'(x)\cdot\theta(x)+\phi(x)\cdot\theta'(x)$.

Υποθέτουμε ότι το μη σταθερό πολυώνυμο $\phi(x)$ δεν έχει πολλαπλές ρίζες. Αν c είναι μια ρίζα του, τότε $\phi(x) = (x-c)\cdot\sigma(x)$ και $\sigma(c) \neq 0$. Οπότε έχουμε ότι $\phi'(x) = \sigma(x) + (x-c)\cdot\sigma'(x)$. Από την τελευταία σχέση έχουμε ότι $\phi'(c) = \sigma(c) \neq 0$. Άρα η παράγωγος $\phi'(x)$ είναι μη μηδενικό πολυώνυμο. Επομένως, αποδείξαμε την εξής πρόταση.

Πρόταση Α΄.2.32. *Αν ένα μη σταθερό πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ δεν έχει πολλαπλές ρίζες, τότε η παράγωγός του είναι μη μηδενικό πολυώνυμο.*

Στην περίπτωση που το πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ είναι ανάγωγο ισχύει και το αντίστροφο της προηγούμενης πρότασης.

Πρόταση Α΄.2.33. *Ένα ανάγωγο πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ δεν έχει πολλαπλές ρίζες, αν και μόνο αν η παράγωγος είναι μη μηδενικό πολυώνυμο.*

Απόδειξη. Απομένει να αποδείξουμε ότι αν $\phi'(x) \neq 0$, τότε το πολυώνυμο δεν έχει πολλαπλές ρίζες. Επειδή η παράγωγος $\phi'(x)$ δεν είναι το μηδενικό πολυώνυμο, έχει βαθμό μικρότερο από τον βαθμό του $\phi(x)$. Το $\phi(x)$ όμως είναι ανάγωγο, άρα πρώτο προς το $\phi'(x)$. Επομένως, υπάρχουν πολυώνυμα

$\lambda(x),\ \mu(x) \in \mathbb{F}[x]$, έτσι ώστε:

$$\lambda(x) \cdot \phi(x) + \mu(x) \cdot \phi'(x) = 1.$$

Αν c είναι μια πολλαπλή ρίζα του $\phi(x)$, από την τελευταία σχέση έπεται ότι $\phi'(c) \neq 0$. Αλλά από τη σχέση $\phi(x) = (x-c)^m \cdot \sigma(x)$ με $m > 1$ έπεται ότι $\phi'(c) = 0$, άτοπο. ό.έ.δ.

Πόρισμα Α΄.2.34. *Ένα πολυώνυμο $\phi(x) \in \mathbb{F}[x]$ έχει πολλαπλές ρίζες, αν και μόνο αν υπάρχει ανάγωγο πολυώνυμο $d(x) \in \mathbb{F}[x]$, το οποίο διαιρεί και το $\phi(x)$ και την παράγωγο $\phi'(x)$.*

Από την προηγούμενη πρόταση έπεται ότι αν το σώμα συντελεστών ενός αναγώγου πολυωνύμου $\phi(x)$ είναι το σώμα των ρητών αριθμών $\mathbb{Q}$ (γενικότερα αν είναι ένα σώμα χαρακτηριστικής μηδέν), τότε το $\phi(x)$ δεν έχει πολλαπλές ρίζες.

Στην περίπτωση όπου το σώμα $\mathbb{F}$ των συντελεστών ενός αναγώγου πολυωνύμου είναι χαρακτηριστικής $p \neq 0$, ενδέχεται το πολυώνυμο να έχει πολλαπλές ρίζες. Στην περίπτωση αυτή το πολυώνυμο έχει μια ειδική μορφή. Έστω $\phi(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$. Υποθέτουμε ότι το $\phi(x)$ έχει πολλαπλές ρίζες. Από την προηγούμενη πρόταση έχουμε ότι η παράγωγος $\phi'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$ είναι το μηδενικό πολυώνυμο. Αυτό σημαίνει ότι οι συντελεστές $ia_i = (i \cdot 1)a_i$, όπου 1 είναι το μοναδιαίο του σώματος, είναι ίσοι με το μηδέν για όλα τα $i = 1, 2, \ldots, n$. Δηλαδή αναγκαστικά, στην περίπτωση όπου $a_i \neq 0$, έχουμε ότι ο αντίστοιχος συντελεστής i είναι πολλαπλάσιο του p (γιατί;). Δηλαδή το πολυώνυμο είναι της μορφής:

$$\phi(x) = b_m x^{pm} + b_{m-1}x^{p(m-1)} + \cdots + b_1 x^p + b_0 = g(x^p).$$

Στα επόμενα (Α΄.3.18) θα δούμε ότι αν έχουμε ως σώμα συντελεστών ενός αναγώγου πολυωνύμου ένα πεπερασμένο σώμα, τότε το πολυώνυμο δεν έχει πολλαπλές ρίζες.

Ορισμοί Α΄.2.35. *1. Έστω $\phi(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο επί του $\mathbb{F}$. Το $\phi(x)$ καλείται **διαχωρίσιμο**, αν όλες οι ρίζες του είναι απλές.*

2. *Έστω $\mathbb{F}$ ένα σώμα και $\mathbb{E} \mid \mathbb{F}$ μια επέκτασή του. Ένα στοιχείο $c \in \mathbb{E}$ θα καλείται* ***διαχωρίσιμο*** *επί του $\mathbb{F}$, αν είναι ρίζα ενός διαχωρισίμου πολυωνύμου με συντελεστές από το σώμα $\mathbb{F}$.*

   Αν όλα τα στοιχεία του $\mathbb{E}$ είναι διαχωρίσιμα, τότε η επέκταση $\mathbb{FE} \mid \mathbb{F}$ ονομάζεται ***διαχωρίσιμη*** *επί του $\mathbb{F}$.*

Έστω $\phi(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο και $\mathbb{E}$ το σώμα ριζών του. Για κάθε ρίζα ξ του $\phi(x)$ και κάθε αυτομορφισμό $\sigma \in G(\mathbb{E}, \mathbb{F})$ έχουμε ότι $\phi(\sigma(\xi)) = 0$ (γιατί;). Δηλαδή κάθε $\mathbb{F}$-αυτομορφισμός μεταθέτει τις ρίζες του πολυωνύμου $\phi(x)$.

Θα κλείσουμε την παράγραφο με την εξής απλή, αλλά σημαντική παρατήρηση. Σύμφωνα με την Παρατήρηση Α΄.2.8$_4$ αν έχουμε δύο πολυώνυμα $\phi(x)$, $\theta(x) \in \mathbb{F}[x]$, τότε αυτά έχουν μια κοινή ρίζα, έστω ξ, σε μια επέκταση $\mathbb{F} \mid \mathbb{E}$, αν και μόνο αν έχουν έναν κοινό ανάγωγο παράγοντα $d(x) \in \mathbb{F}[x]$.

Παρεμβολή Lagrange

Ως γνωστόν, μια ευθεία είναι πλήρως καθορισμένη από δύο σημεία της. Δηλαδή ένα πολυώνυμο $\varphi(x) = ax + b$ με συντελεστές από ένα σώμα βαθμού ένα είναι πλήρως καθορισμένο αν, για δύο διακεκριμμένα στοιχεία a_1, a_2 του σώματος, γνωρίζουμε τις τιμές $\varphi(a_1) = b_1$ και $\varphi(a_2) = b_2$.

Θα δούμε ότι κάτι αντίστοιχο συμβαίνει και σε πολυώνυμα οποιουδήποτε βαθμού.

Θεώρημα Α΄.2.36. ***(Παρεμβολή Lagrange)*** *Έστω $\mathbb{F}$ ένα σώμα και $a_1, a_2, \ldots, a_n$ διακεκριμένα στοιχεία του $\mathbb{F}$. Επίσης, έστω $b_1, b_2, \ldots, b_n$ (όχι κατ' ανάγκη διακεκριμένα) στοιχεία του $\mathbb{F}$. Τότε υπάρχει μοναδικό πολυώνυμο $\varphi(x) \in \mathbb{F}[x]$ βαθμού το πολύ $n-1$ με την ιδιότητα $\varphi(a_i) = b_i$ για όλα τα $i = 1, 2, \ldots, n$.*

Απόδειξη. Αναζητούμε ένα πολυώνυμο $\varphi(x) = \lambda_0 + \lambda_1 x + \cdots \lambda_{n-1} x^{n-1} \in \mathbb{F}[x]$ με την ιδιότητα $\lambda_0 + \lambda_1 a_i + \cdots \lambda_{n-1} a_i^{n-1} = b_i$ για όλα τα $i = 1, 2, \ldots, n$. Από

τη σχέση αυτή προκύπτει το γραμμικό σύστημα:

$$(\lambda_0, \lambda_1, \ldots, \lambda_{n-1}) \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_1^2 & a_2^2 & \cdots & a_{n-1}^2 & a_n^2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_1^{n-2} & a_2^{n-2} & \cdots & a_{n-1}^{n-2} & a_n^{n-2} \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_{n-1}^{n-1} & a_n^{n-1} \end{pmatrix} = (b_1, b_2, \ldots, b_{n-1}, b_n)$$

(τα λ_j είναι οι άγνωστοι). Ο πίνακας του συστήματος:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \\ a_1^2 & a_2^2 & \cdots & a_{n-1}^2 & a_n^2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ a_1^{n-2} & a_2^{n-2} & \cdots & a_{n-1}^{n-2} & a_n^{n-2} \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_{n-1}^{n-1} & a_n^{n-1} \end{pmatrix}$$

είναι ένας πίνακας Vandermonde, άρα αντιστρέψιμος, καθότι η ορίζουσά του ισούται με $\Pi_{i<j}(a_i - a_j) \neq 0$, αφού τα a_i είναι διακεκριμμένα. Επομένως, το σύστημα έχει μοναδική λύση.

Λύνοντας το σύστημα αυτό υπολογίζουμε τα λ_j και άρα το ζητούμενο πολυώνυμο, το οποίο (αν για τη λύση του συστήματος εφαρμόσουμε την μέθοδο Cramer) εύκολα βλέπουμε ότι είναι το:

$$\varphi(x) = \Sigma_{i=1}^{n} b_i \frac{(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_n)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)}.$$

ό.έ.δ.

Σχόλιο Α΄.2.37. Από την Πρόταση Α΄.2.20 έπεται *εμμέσως* (χωρίς να υπολογίσουμε την ορίζουσά του) ότι ένας πίνακας Vandermonde είναι αντιστρέψιμος.

Μια σημαντική εφαρμογή του προηγουμένου θεωρήματος είναι το ακόλουθο:

Πόρισμα Α΄.2.38. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $f : \mathbb{F} \longrightarrow \mathbb{F}$ μια απεικόνιση. Τότε υπάρχει πολυώνυμο $\varphi(x) \in \mathbb{F}[x]$ βαθμού το πολύ $q-1$, ούτως ώστε $\varphi(x) = f(x)$.*

Απόδειξη. Έστω $\mathbb{F} = \{a_1, a_2, \dots, a_q\}$, θέτουμε $b_i = f(a_i)$, $i = 1, 2, \dots, q$. Από το προηγούμενο θεώρημα υπάρχει μοναδικό πολυώνυμο $\varphi(x) \in \mathbb{F}[x]$ βαθμού το πολύ $q-1$ με την ιδιότητα $\varphi(a_i) = b_i$ για όλα τα $i = 1, 2, \dots, q$. Οπότε έπεται ότι $\varphi(x) = f(x)$. ό.έ.δ.

Επισημαίνουμε ότι εδώ η ισότητα $\varphi(x) = f(x)$ ισχύει θεωρώντας το πολυώνυμο $\varphi(x)$ ως απεικόνιση.

Α΄.3 Πεπερασμένα Σώματα

Στην παράγραφο αυτή θα ασχοληθούμε με τα πεπερασμένα σώματα, καθώς και με ιδιότητες πολυωνύμων με συντελεστές από ένα πεπερασμένο σώμα.

Έστω $\mathbb{F}$ ένα πεπερσμένο σώμα. Τότε, προφανώς, η χαρακτηριστική του είναι πεπερασμένη, έστω p. Επομένως, το $\mathbb{F}$ είναι μια πεπερασμένη επέκταση του σώματος $\mathbb{Z}_p$. Αν $[\mathbb{F} : \mathbb{Z}_p] = n$ είναι ο βαθμός επέκτασης, τότε προφανώς $|\ \mathbb{F}\ | = p^n$. Δηλαδή το πλήθος των στοιχείων ενός πεπερασμένου σώματος είναι ίσο με μια δύναμη ενός πρώτου αριθμού.

Α΄.3.1 Τα πεπερασμένα σώματα ως σώματα ριζών πολυωνύμων

Λήμμα Α΄.3.1. *Έστω $\mathbb{F}$ ένα σώμα χαρακτηριστικής p. Τότε για κάθε θετικό ακέραιο n ισχύει $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$, για όλα τα $a, b \in \mathbb{F}$.*

Απόδειξη. Για p πρώτο και για $1 \leq k \leq p$ ο δυωνυμικός συντελεστής $\binom{p}{k}$ είναι πολλαπλάσιο του p (γιατί;). Οπότε $(a \pm b)^p = a^p \pm b^p$, με τις λεπτομέρειες να αφήνονται ως άσκηση. ό.έ.δ.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα χαρακτηριστικής p με $|\mathbb{F}| = p^n = q$. Η πολλαπλασιαστική του ομάδα περιέχει $q-1$ το πλήθος στοιχεία, οπότε για κάθε στοιχείο $a \in \mathbb{F}$ ισχύει $a^{q-1} = 1$,[4] δηλαδή $a^q = a$ για κάθε $a \in \mathbb{F}$.

[4] Εδώ χρησιμοποιούμε, χωρίς να αποδεικνύουμε, το εξής αποτέλεσμα από τη Θεωρία Ομάδων: " Έστω G πεπερασμένη ομάδα. Τότε, για κάθε $g \in G$ ισχύει $g^{|G|} = 1$. ". Βλέπε για παράδειγμα Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη [2013], παρ. 4.4.

Από τη σχέση αυτή βλέπουμε ότι κάθε στοιχείο του σώματος $\mathbb{F}$ είναι ρίζα του πολυωνύμου $x^q - x \in \mathbb{Z}_p[x]$. Επειδή δε το πλήθος των ριζών του $x^q - x$ είναι το πολύ q, έχουμε ότι το σώμα $\mathbb{F}$ είναι τόσο το σύνολο ριζών του $x^q - x$, όσο και το σώμα ριζών του. Δηλαδή έχουμε αποδείξει ότι κάθε σώμα $\mathbb{F}$ με q το πλήθος στοιχεία είναι σώμα ριζών του πολυωνύμου $x^q - x$. Έχουμε όμως αναφέρει (Θεώρημα Α΄.2.31), ότι δύο σώματα ριζών ενός πολυωνύμου είναι ισόμορφα, επομένως έπεται ότι όλα τα πεπερασμένα σώματα με το ίδιο πλήθος στοιχείων είναι ισόμορφα.

Προηγουμένως αποδείξαμε ότι ένα πεπερασμένο σώμα είναι το σώμα ριζών ενός πολυωνύμου. Θα δείξουμε ότι για κάθε πρώτο p και κάθε θετικό ακέραιο n υπάρχει ένα σώμα $\mathbb{F}$ με $p^n = q$ το πλήθος στοιχεία.

Έστω $x^q - x \in \mathbb{Z}_p[x]$ και $\mathbb{E}$ το σώμα ριζών του. Για δύο ρίζες $\zeta, \xi \in \mathbb{E}$ δεν είναι δύσκολο να δούμε ότι $(\zeta \pm \xi)^q = \zeta \pm \xi$ (δες το Λήμμα Α΄.3.1). Επίσης $(\zeta \cdot \xi^{-1})^q = \zeta \cdot \xi^{-1}$. Δηλαδή τα $\zeta \pm \xi$ και $\zeta \cdot \xi^{-1}$ είναι ρίζες του πολυωνύμου $x^q - x$. Άρα, αν K είναι το σύνολο ριζών του $x^q - x$, τότε το K είναι σώμα που περιέχεται στο $\mathbb{E}$, δηλαδή $\mathrm{K} = \mathbb{E}$.

Το $x^q - x$ όμως έχει διακεκριμένες ρίζες. Πράγματι, η παράγωγος του $x^q - x$ είναι ίση με $(x^q - x)' = qx^{q-1} - 1 = -1 \in \mathbb{Z}_p[x]$, οπότε από το Πόρισμα Α΄.2.34 έχουμε ότι οι ρίζες του $x^q - x$ είναι διακεκριμένες. Επομένως, το σώμα ριζών $\mathbb{E}$ έχει $q = p^n$ το πλήθος στοιχεία.

Τα προηγούμενα αποτελούν την απόδειξη του επομένου θεωρήματος.

Θεώρημα Α΄.3.2. *Για κάθε δύναμη ενός πρώτου αριθμού ($q = p^n$) υπάρχει μοναδικό (μέσω ισομορφισμού) σώμα $\mathbb{F}$ με $q = p^n$ το πλήθος στοιχεία, το οποίο είναι το σώμα (και σύνολο) ριζών του πολυωνύμου $x^q - x \in \mathbb{Z}_p[x]$.*

Α΄.3.2 Τα υποσώματα ενός πεπερασμένου σώματος

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία και $\mathbb{K}$ ένα υπόσωμά του. Το $\mathbb{K}$ έχει p^d το πλήθος στοιχεία. Θα δείξουμε ότι το d διαιρεί το n.

Πράγματι, από τη σχέση (σελίδα 401) που μας δίνει τον βαθμό διαδοχικών επεκτάσεων, έχουμε ότι $d \mid n$.

Αντίστροφα, έστω d ένας διαιρέτης του n, θα δείξουμε ότι υπάρχει ένα (μοναδικό) υπόσωμα $\mathbb{K}$ του $\mathbb{F}$ με p^d το πλήθος στοιχεία.

Από τη σχέση $d \mid n$ έπεται ότι $p^d - 1 \mid p^n - 1$ (γιατί;) Οπότε έχουμε $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$, δηλαδή $x^{p^d} - x \mid x^{p^n} - x$. Το σώμα $\mathbb{F}$ είναι το σώμα ριζών του πολυωνύμου $x^{p^n} - x$, επομένως περιέχει το σώμα ριζών, έστω $\mathbb{K}$, του πολυωνύμου $x^{p^d} - x$. Το σώμα δεν μπορεί να περιέχει και άλλο σώμα με p^d το πλήθος στοιχεία, διότι τότε θα είχαμε περισσότερες ρίζες για το πολυώνυμο $x^{p^d} - x$ απ' ότι είναι ο βαθμός του.

Θεώρημα Α΄.3.3. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με p^n το πλήθος στοιχεία.*

1. *Το πλήθος των υποσωμάτων του $\mathbb{F}$ είναι ίσο με το πλήθος των θετικών διαιρετών του n.*

2. *Έστω $\mathbb{K}$ είναι ένα υπόσωμα του $\mathbb{F}$ με p^m το πλήθος στοιχεία, ένα στοιχείο $c \in \mathbb{F}$ ανήκει στο υπόσωμα $\mathbb{K}$, αν και μόνο αν $c^{p^m} = c$.*

   Ειδικότερα, ένα στοιχείο $c \in \mathbb{F}$ ανήκει στο (υπό)σωμα $\mathbb{Z}_p$, αν και μόνο αν $c^p = c$.

3. *Για κάθε δύναμη q του p όλα τα στοιχεία $c \in \mathbb{F}$ με την ιδιότητα: $c^q = c$, αποτελούν ένα υπόσωμα του $\mathbb{F}$.*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Παράδειγμα Α΄.3.4. Τα υποσώματα ενός σώματος $\mathbb{F}_{12}$ με 2^{12} το πλήθος στοιχεία είναι τα εξής: $\mathbb{F}_6, \mathbb{F}_4, \mathbb{F}_3, \mathbb{F}_2, \mathbb{F}_1$, όπου ο δείκτης δηλώνει έναν διαιρέτη του 12. Μάλιστα δε, μπορούν να διαταχθούν ως εξής:

$$\mathbb{F}_{12} \geq \mathbb{F}_6 \geq \mathbb{F}_3 \geq \mathbb{F}_1$$
$$\mathbb{F}_{12} \geq \mathbb{F}_4 \geq \mathbb{F}_2 \geq \mathbb{F}_1$$
$$\mathbb{F}_{12} \geq \mathbb{F}_6 \geq \mathbb{F}_2 \geq \mathbb{F}_1.$$

Θεώρημα Α΄.3.5. *Η πολλαπλασιαστική ομάδα ενός πεπερασμένου σώματος είναι κυκλική.*

Απόδειξη. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία. Η πολλαπλασιαστική του ομάδα είναι αβελιανή και έχει $q-1$ το πλήθος στοιχεία. Υποθέτουμε ότι δεν είναι κυκλική, δηλαδή κανένα στοιχείο της δεν έχει τάξη ίση με $q-1$. Τότε (σύμφωνα με το επόμενο Λήμμα) υπάρχει $1 < r < q-1$, έτσι ώστε για κάθε μη μηδενικό στοιχείο a του σώματος $\mathbb{F}$ να ισχύει $a^r = 1$, δηλαδή κάθε μη μηδενικό στοιχείο του $\mathbb{F}$ είναι ρίζα του πολυωνύμου $x^r - 1$. Αυτό είναι άτοπο, διότι ένα πολυώνυμο δεν μπορεί να έχει περισσότερες ρίζες από τον βαθμό του. Άρα, αναγκαστικά $r = q-1$ και η πολλαπλασιαστική ομάδα του $\mathbb{F}$ είναι κυκλική. ό.έ.δ.

Το Λήμμα που επικαλούμαστε στην προηγούμενη απόδειξη χρησιμοποιεί ορισμένα αποτελέσματα από τη στοιχειώδη θεωρία των αβελιανών ομάδων.

Λήμμα Α΄.3.6. *Έστω G πεπερασμένη αβελιανή ομάδα και ένα $a \in G$ με την μεγαλύτερη δυνατή τάξη, έστω r, τότε $g^r = 1$ για κάθε $g \in G$.*

Απόδειξη. Υποθέτουμε ότι υπάρχει ένα $b \in G$ με τάξη ίση με s, η οποία δεν διαιρεί την τάξη του a.

Υποθέτουμε ότι το r και το s είναι πρώτα μεταξύ τους. Τότε προφανώς η τάξη του στοιχείου $a \cdot b$ είναι ίση με το γινόμενο rs (γιατί;). Αυτό είναι άτοπο, διότι υποθέσαμε ότι το r είναι η μεγαλύτερη δυνατή τάξη των στοιχείων της G.

Έστω ότι υπάρχει ένας πρώτος διαιρέτης p του s, ο οποίος δεν διαιρεί το r, τότε τα στοιχεία a και $b^{s/p}$ έχουν τάξεις r και p αντίστοιχα, επομένως το στοιχείο $a \cdot b^{s/p}$ έχει τάξη ίση με rp, πάλι άτοπο.

Απομένει η περίπτωση, όπου κάθε πρώτος διαιρέτης του s είναι και διαιρέτης του r. Επειδή έχουμε υποθέσει ότι η τάξη του b δεν διαιρεί την τάξη του a, υπάρχει πρώτος p τέτοιος ώστε η μεγαλύτερη δυνατή δύναμή του, έστω p^ν, που διαιρεί το s να είναι (γνήσια) μεγαλύτερη από τη μεγαλύτερη δυνατή δύναμή, έστω p^λ που διαιρεί το r, δηλαδή $\nu > \lambda$. Η τάξη του στοιχείου a^{p^λ} είναι ίση με r/p^λ και η τάξη του στοιχείου b^{s/p^ν} είναι ίση με p^ν. Τα r/p^λ και p^ν όμως είναι πρώτα μεταξύ τους, επομένως η τάξη του στοιχείου $a^{p^\lambda} \cdot b^{s/p^\nu}$ είναι ίση με το γινόμενο $(r/p^\lambda)p^\nu$, το οποίο είναι μεγαλύτερο από το r, άτοπο.

Άρα τελικά δεν υπάρχει στοιχείο της ομάδας G με τάξη που να μην διαιρεί την τάξη του στοιχείου a. ό.έ.δ.

Το προηγούμενο θεώρημα μας επιτρέπει να περιγράφουμε τα στοιχεία ενός πεπερασμένου σώματος $\mathbb{F}$ ως δυνάμεις ενός μόνο στοιχείου του, του γεννήτορα της πολλαπλασιαστικής ομάδας.

Επομένως, αν c είναι ο γεννήτορας της πολλαπλασιαστικής ομάδας $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ και $a, b \in \mathbb{F}^*$ με $a = c^\kappa$, $b = c^\lambda$, τότε $a \cdot b = c^\kappa \cdot c^\lambda = c^{\kappa+\lambda}$. Αλλά, ενώ υπάρχει εκθέτης μ ώστε $a + b = c^\kappa + c^\lambda = c^\mu$, γενικά δεν είναι εύκολο να προσδιοριστεί.

Πρόταση Α΄.3.7. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα και H μια μη τετριμμένη υποομάδα της πολλαπλασιαστικής ομάδας του $\mathbb{F}$. Το άθροισμα των στοιχείων της H ισούται με μηδέν.*

Απόδειξη. Η υποομάδα H είναι κυκλική, ως υποομάδα κυκλικής. Άρα υπάρχει ένα στοιχείο $a \in H$, έτσι ώστε $H = \{a, a^2, \ldots, a^n = 1\}$, όπου n είναι η τάξη της υποομάδας H. Από τη σχέση $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ έπεται το αποτέλεσμα. ό.έ.δ.

Πόρισμα Α΄.3.8. *Το άθροισμα των στοιχείων ενός πεπερασμένου σώματος ισούται με μηδέν.*

Άσκηση. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Δείξτε ότι $\sum_{a \in \mathbb{F}} a^r = 0$, για κάθε r με $1 \leq r < q - 1$.

Άσκηση. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Δείξτε ότι $\prod_{a \in \mathbb{F} \setminus 0} a = -1$.

Ένας γεννήτορας της πολλαπλασιαστικής ομάδας $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ θα ονομάζεται **πρωταρχικό** στοιχείο του σώματος.

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με $q = p^n$ το πλήθος στοιχεία και c ένα πρωταρχικό στοιχείο. Το c δεν είναι το μοναδικό πρωταρχικό στοιχείο του $\mathbb{F}$. Μια δύναμη του c για να είναι πρωταρχικό στοιχείο πρέπει να είναι γεννήτορας της κυκλικής ομάδας $\mathbb{F}^*$, δηλαδή πρέπει να έχει τάξη ίση με $q-1$. Ως γνωστόν (γιατί;) όμως, η τάξη του c^r είναι ίση με την τάξη του c, αν και μόνο αν το r και το $q-1$ είναι πρώτα μεταξύ τους, επομένως υπάρχουν $\varphi(q-1)$

το πλήθος πρωταρχικά στοιχεία, όπου φ είναι η είναι η γνωστή συνάρτηση Euler, της οποίας η τιμή $\varphi(n)$ για κάθε θετικό ακέραιο αριθμό n είναι ίση με το πλήθος των ακεραίων μεταξύ του 1 και του n, οι οποίοι είναι πρώτοι προς τον n.

Αν τώρα πάρουμε ένα υπόσωμα $\mathbb{K}$ του σώματος $\mathbb{F}$, το οποίο έχει $s = p^d$ το πλήθος στοιχεία, η πολλαπλασιαστική του ομάδα, ως υποομάδα της πολλαπλασιαστικής ομάδας του $\mathbb{F}$, είναι κυκλική και ένας γεννήτορας της θα είναι της μορφής $a = c^k$ και θα έχει τάξη ίση με $s-1$. Γνωρίζουμε όμως ότι η τάξη του c^k είναι ίση με $(q-1)/\,\mu\kappa\delta(k, q-1)$ (γιατί;), άρα για να βρούμε έναν γεννήτορα της πολλαπλασιαστικής ομάδας του υποσώματος $\mathbb{K}$ πρέπει και αρκεί να βρούμε όλους τους ακεραίους $1 \leq k \leq q-1$, για τους οποίους ισχύει $s-1 = (q-1)/\,\mu\kappa\delta(k, q-1)$. Ένας από αυτούς προφανώς είναι και ο $(q-1)/(s-1)$, οπότε έχουμε $\mathbb{K} = \{0, a^i = c^{i(q-1)/(s-1)}, i = 1, \ldots, s-1\}$. Από τα προηγούμενα έχουμε ότι κάθε άλλο πρωταρχικό στοιχείο του $\mathbb{K}$ είναι της μορφής $c^{j(q-1)/(s-1)}$, όπου το j είναι πρώτο προς το $s-1$.

Στο Θεώρημα Α΄.3.3 είχαμε δει ότι ένα στοιχείο b του σώματος $\mathbb{F}$ ανήκει στο υπόσωμα $\mathbb{K}$, αν και μόνο αν $b^{p^d} = b$. Εδώ μπορούμε να δούμε μια άλλη απόδειξη. Πράγματι, αν $b \in \mathbb{F}$, τότε $b = c^\mu$ για κάποιο θετικό ακέραιο μ, οπότε $b \in \mathbb{K}$ αν και μόνο αν $b = c^{(q-1)/(s-1)\cdot\nu}$ για κάποιο θετικό ακέραιο ν, αν και μόνο αν $c^\mu = c^{(q-1)/(s-1)\cdot\nu}$, αν και μόνο αν $c^{\mu\cdot(s-1)} = c^{(q-1)\cdot\nu} = 1$, αν και μόνο αν $b = c^\mu = c^{\mu\cdot s} = b^s = b^{p^d}$.

Από την άλλη πλευρά γνωρίζουμε ότι κάθε πεπερασμένο σώμα είναι το σώμα ριζών ενός πολυωνύμου. Θα δούμε πώς μπορούμε να συνδυάσουμε τα πρωταρχικά στοιχεία ένος σώματος με τις ρίζες πολυωνύμων.

Έστω c ένα πρωταρχικό στοιχείο του $\mathbb{F}$. Τότε προφανώς ισχύει $\mathbb{F} = \mathbb{Z}_p(c)$. Δηλαδή κάθε πεπερασμένο σώμα είναι απλή επέκταση του $\mathbb{Z}_p$ για κάποιον πρώτο αριθμό p.

Ο βαθμός της επέκτασης $[\mathbb{F} : \mathbb{Z}_p]$ είναι ίσος με τον βαθμό του ελαχίστου πολυωνύμου $m_c(x) \in \mathbb{Z}_p[x]$ του c (βλέπε Σχόλιο Α΄.2.26). Επίσης, από την Πρόταση Α΄.2.22 έχουμε ότι $\mathbb{F} = \mathbb{Z}_p(c) \simeq \mathbb{Z}_p[x]/\langle m_c(x)\rangle$. Επομένως, κάθε στοιχείο του $\mathbb{F}$ θα μπορούσε να εκφρασθεί ως η τιμή ενός πολυωνύμου στη θέση c (βλέπε Πρόταση Α΄.2.23).

Στο επόμενο παράδειγμα θα περιγράψουμε τα στοιχεία ενός σώματος $\mathbb{F}$ με 16 στοιχεία.

Παράδειγμα Α΄.3.9. Έστω $\mathbb{F}$ το σώμα με 16 στοιχεία.

Το σώμα $\mathbb{F}$ είναι το σώμα ριζών του πολυωνύμου $x^{2^4}-x \in \mathbb{Z}_2[x]$ (Θεώρημα Α΄.3.2).

Έστω το πολυώνυμο $x^4+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$. Το πολυώνυμο αυτό είναι ανάγωγο επί του $\mathbb{Z}_2[x]$ (μπορείτε να κάνετε τον έλεγχο). Επομένως, ο δακτύλιος πηλίκων $\mathbb{Z}_2[x]/\langle x^4+x^3+x^2+x+1\rangle$ είναι (ισόμορφος με) το σώμα $\mathbb{F}$. Έστω c μια ρίζα του $x^4+x^3+x^2+x+1$, τότε τα στοιχεία του $\mathbb{F}$ είναι τα 0, 1, c, $c+1$, c^2, c^2+1, c^2+c, c^2+c+1, c^3, c^3+1, c^3+c, c^3+c^2, c^3+c+1, c^3+c^2+1, c^3+c^2+c, c^3+c^2+c+1.

Η ρίζα c του πολυωνύμου $x^4+x^3+x^2+x+1$ πληροί τη σχέση $c^4 = c^3+c^2+c+1$. Από τη σχέση αυτή βλέπουμε ότι $c^5 = c(c^3+c^2+c+1) = c^4+c^3+c^2+c = (c^3+c^2+c+1)+(c^3+c^2+c) = 1$, δηλαδή είναι τάξης 5. Άρα δεν είναι πρωταρχικό στοιχείο του σώματος $\mathbb{F}$.

Άσκηση. Δείξτε ότι το στοιχείο $1+c$ είναι πρωταρχικό στοιχείο. Να βρεθεί θετικός ακέραιος k ώστε $c = (1+c)^k$.

(Συνέχεια του παραδείγματος.)

Αν αντί του πολυωνύμου $x^4+x^3+x^2+x+1$ πάρουμε το πολυώνυμο $x^4+x+1 \in \mathbb{Z}_2[x]$, τότε το πολυώνυμο αυτό είναι ανάγωγο και, επομένως, πάλι έχουμε ότι ο δακτύλιος $\mathbb{Z}_2[x]/\langle x^4+x+1\rangle$ είναι (ισόμορφος με) το σώμα $\mathbb{F}$. Όπως προηγουμένως αν ζ είναι μια ρίζα του x^4+x+1, τότε μπορούμε να εκφράσουμε τα στοιχεία του $\mathbb{F}$ ως τις τιμές πολυωνύμων βαθμού το πολύ 3 στη θέση ζ. Εδώ όμως ισχύει $\zeta^4 = \zeta+1$. Από τη σχέση αυτή βλέπουμε ότι $\zeta^3 \neq 1$, όπως επίσης $\zeta^5 \neq 1$. Άρα, η τάξη του ζ είναι ίση με 15. Δηλαδή το ζ είναι πρωταρχικό στοιχείο του $\mathbb{F}$ και τα υπόλοιπα μη μηδενικά στοιχεία του είναι οι δυνάμεις του ζ.

Θα μπορούσαμε να εκφράσουμε τα μη μηδενικά στοιχεία του $\mathbb{F}$ τόσο ως δυνάμεις του ζ, όσο και ως πολυώνυμα ως προς ζ. Δηλαδή έχουμε:

$$\zeta, \zeta^2, \zeta^3, \zeta^4 = \zeta+1, \zeta^5 = \zeta^4\cdot\zeta = (\zeta+1)\zeta = \zeta^2+\zeta, \ldots, \zeta^{15} = 1.$$

Ενδιαφέρον είναι να προσπαθήσετε να βρείτε πώς εκφράζεται το ίδιο

στοιχείο του σώματος $\mathbb{F}$ ως η τιμή ενός πολυωνύμου στη θέση c και ως μια δύναμη του ζ. Συγκεκριμένα θα πρέπει να ορισθεί ένας ισομορφισμός μεταξύ των σωμάτων $\mathbb{Z}_2[x]/\langle x^4+x+1\rangle$ και $\mathbb{Z}_2[x]/\langle x^4+x^3+x^2+x+1\rangle$.

Ορισμός Α΄.3.10. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα, $\mathbb{E}$ μια πεπερασμένη επέκτασή του και ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$. Το ελάχιστο πολυώνυμο του ζ επί του $\mathbb{F}$ θα λέγεται* ***πρωταρχικό*** *πολυώνυμο του $\mathbb{E}$ επί του $\mathbb{F}$.*

Στο προηγούμενο παράδειγμα βλέπουμε ότι το πολυώνυμο x^4+x+1 είναι πρωταρχικό πολυώνυμο για το σώμα με 16 στοιχεία επί του σώματος $\mathbb{Z}_2$.

Η εύρεση των πρωταρχικών πολυωνύμων ενός σώματος δεν είναι εύκολη. Πριν δούμε ορισμένες ιδιότητές τους, θα μελετήσουμε τους αυτομορφισμούς ενός πεπερασμένου σώματος.

Α΄.3.3 Η ομάδα αυτομορφισμών ενός πεπερασμένου σώματος

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με p^n το πλήθος στοιχεία, όπου p πρώτος. Η απεικόνιση $\varphi : \mathbb{F} \longrightarrow \mathbb{F}$ με $\varphi(c) = c^p$ είναι εύκολο (επειδή $(a+b)^p = a^p+b^p$) να ελέγξουμε ότι είναι ένας αυτομορφισμός του σώματος $\mathbb{F}$.

Επειδή τα στοιχεία του σώματος $\mathbb{F}$ ικανοποιούν τη σχέση $c^{p^n} = c$, έπεται ότι $\varphi^n(c) = c$ για κάθε $c \in \mathbb{F}$, δηλαδή η φ^n είναι ο ταυτοτικός αυτομορφισμός. Υποθέτουμε ότι υπάρχει $0 < m < n$ με $\varphi^m = 1$, ο ταυτοτικός αυτομορφισμός, δηλαδή $\varphi^m(c) = c$ για όλα τα $c \in \mathbb{F}$. Αυτό σημαίνει ότι όλα τα στοιχεία του σώματος $\mathbb{F}$ είναι ρίζες του πολυωνύμου $x^{p^m} - x$, άτοπο, αφού ο βαθμός p^m αυτού του πολυωνύμου είναι γνήσια μικρότερος από το πλήθος p^n των στοιχείων του σώματος. Συνεπώς, η τάξη του αυτομορφισμού φ είναι ίση με n.

Όπως είναι γνωστό (σελ. 435) το σώμα $\mathbb{F}$ είναι απλή επέκταση του $\mathbb{Z}_p$, δηλαδή $\mathbb{F} = \mathbb{Z}_p(c)$ και επειδή $[\mathbb{F} : \mathbb{Z}_p] = n$, ο βαθμός του ελαχίστου πολυωνύμου $m_c(x) \in \mathbb{Z}_p[x]$ του στοιχείου c είναι ίσος με n. Αν θ είναι ένας αυτομορφισμός του $\mathbb{F}$, επειδή ο περιορισμός του στο πρώτο σώμα $\mathbb{Z}_p$ είναι ο ταυτοτικός αυτομορφισμός (Πρόταση Α΄.1.18), ο θ είναι πλήρως (γιατί;) καθορισμένος από την εικόνα $\theta(c)$. Αλλά $m_c(\theta(c)) = \theta(m_c(c)) = 0$. Δηλαδή η εικόνα $\theta(c)$ είναι μια από τις n το πλήθος ρίζες του ελαχίστου πολυωνύμου

$m_c(x)$, άρα υπάρχουν το πολύ n το πλήθος αυτομορφισμοί του σώματος $\mathbb{F}$. Έχουμε όμως αποδείξει ότι υπάρχουν ήδη τουλάχιστον n το πλήθος αυτομορφισμοί (οι διακεκριμένες δυνάμεις του φ).

Συνεπώς, η ομάδα αυτομορφισμών $Aut(\mathbb{F})$ είναι κυκλική και παράγεται από τον αυτομορφισμό $\varphi : \mathbb{F} \longrightarrow \mathbb{F}$ με $\varphi(c) = c^p$.

Θεώρημα Α΄.3.11. *Η ομάδα αυτομορφισμών ενός πεπεραμένου σώματος με p^n το πλήθος στοιχεία, όπου p πρώτος, είναι κυκλική τάξης n με γεννήτορα τον αυτομορφισμό $\varphi : \mathbb{F} \longrightarrow \mathbb{F}$ με $\varphi(c) = c^p$.*

Απόδειξη. Η απόδειξη έχει προηγηθεί. ό.έ.δ.

Ο αυτομορφισμός φ ονομάζεται **αυτομορφισμός του Frobenius**.

Συνδυάζοντας το προηγούμενο θεώρημα με το Θεώρημα Α΄.3.3 έχουμε το εξής σημαντικό:

Πόρισμα Α΄.3.12. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με p^n το πλήθος στοιχεία, όπου p πρώτος.*

Υπάρχει μια 1-1 και επί αντιστοιχία μεταξύ των υποσωμάτων του σώματος $\mathbb{F}$ και των υποομάδων της ομάδας αυτομορφισμών $Aut(\mathbb{F}) = \langle \varphi \rangle$.

Απόδειξη. Ως γνωστόν σε κάθε κυκλική ομάδα $\langle a \rangle$ τάξης n για κάθε θετικό διαιρέτη m του n υπάρχει ακριβώς μία υποομάδα τάξης m, οπότε το αποτέλεσμα έπεται από το Θεώρημα Α΄.3.3. ό.έ.δ.

Παρατήρηση Α΄.3.13. Το προηγούμενο πόρισμα είναι η εκδοχή του Θεμελιώδους Θεωρήματος του Galois για τα πεπερασμένα σώματα.

Α΄.3.4 Ανάγωγα πολυώνυμα με συντελεστές από πεπερασμένα σώματα

Πριν μελετήσουμε ιδιότητες αναγώγων πολυωνύμων με συντελεστές από ένα πεπερασμένο σώμα, θα αποδείξουμε την ύπαρξη αναγώγων πολυωνύμων με οποιονδήποτε βαθμό.

Θεώρημα Α΄.3.14. *Για κάθε πεπερασμένο σώμα $\mathbb{F}$ και κάθε θετικό ακέραιο αριθμό n υπάρχει ανάγωγο πολυώνυμο με συντελεστές από το $\mathbb{F}$ και βαθμό ίσο με n.*

Απόδειξη. Έστω q το πλήθος των στοιχείων του σώματος $\mathbb{F}$. Το q είναι δύναμη ενός πρώτου αριθμού, έστω p. Επομένως, το q^n είναι δύναμη πρώτου αριθμού, άρα υπάρχει σώμα έστω $\mathbb{E}$ με q^n το πλήθος στοιχεία (Θεώρημα Α΄.3.2). Το σώμα $\mathbb{E}$ είναι επέκταση του σώματος $\mathbb{F}$. Έστω ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$, τότε $\mathbb{F}(\zeta) = \mathbb{E}$. Επομένως, από τη σχέση $[\mathbb{E} : \mathbb{F}] = [\mathbb{F}(\zeta) : \mathbb{F}] = n$ έχουμε ότι ο βαθμός του ελαχίστου πολυωνύμου του ζ επί του $\mathbb{F}$ είναι ίσος με n. ό.έ.δ.

Παρατήρηση Α΄.3.15. Από την προηγούμενη απόδειξη έπεται ότι για κάθε θετικό ακέραιο n δεν υπάρχει μόνο ανάγωγο πολυώνυμο με συντελεστές από ένα πεπερασμένο σώμα με βαθμό n, αλλά ένα πρωταρχικό πολυώνυμο βαθμού n.

Θα περιγράψουμε το σώμα ριζών ενός αναγώγου πολυωνύμου με συντελεστές από ένα πεπερασμένο σώμα.

Θεώρημα Α΄.3.16. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Αν ξ είναι μια ρίζα του, τότε το σώμα ριζών του $\sigma(x)$ είναι το σώμα $\mathbb{F}(\xi)$.*

Απόδειξη. Έστω $\mathbb{E}$ το σώμα ριζών του $\sigma(x)$ και ξ μια ρίζα του. Προφανώς έχουμε ότι $\mathbb{F} \leq \mathbb{F}(\xi) \leq \mathbb{E}$. Ο βαθμός επέκτασης $[\mathbb{F}(\xi) : \mathbb{F}]$ είναι ίσος με d. Επομένως, το σώμα $\mathbb{F}(\xi)$ έχει q^d το πλήθος στοιχεία και είναι το σώμα (σύνολο) ριζών του πολυωνύμου $x^{q^d} - x$ (Θεώρημα Α΄.3.2). Μια από τις ρίζες του $x^{q^d} - x$ είναι και το ξ, άρα το ανάγωγο πολυώνυμο $\sigma(x)$, που έχει και αυτό ρίζα το ξ, διαιρεί το $x^{q^d} - x$ (γιατί;). Επομένως όλες οι ρίζες του $\sigma(x)$ είναι και ρίζες του $x^{q^d} - x$, δηλαδή $\mathbb{F}(\xi) = \mathbb{E}$. ό.έ.δ.

Πόρισμα Α΄.3.17. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Το $\sigma(x)$ διαιρεί το πολυώνυμο $x^{q^n} - x$, αν και μόνο αν ο d διαιρεί τον n.*

Απόδειξη. Έστω $\mathbb{K}$ το σώμα ριζών του πολυωνύμου $\sigma(x)$ και $\mathbb{E}$ το σώμα ριζών του πολυωνύμου $x^{q^n} - x$. Από το προηγούμενο θεώρημα έπεται ότι το $\mathbb{K}$ έχει q^d το πλήθος στοιχεία. Από την απόδειξη του Θεωρήματος Α΄.3.3 έπεται ότι το $\mathbb{K}$ είναι υπόσωμα του $\mathbb{E}$, αν και μόνο αν το d διαιρεί το n.

Έπομένως, η απόδειξη ανάγεται στο ότι το ανάγωγο πολυώνυμο $\sigma(x)$ διαιρεί το $x^{q^n} - x$, αν και μόνο αν $\mathbb{K} \leq \mathbb{E}$.

Προφανώς, αν το $\sigma(x)$ διαιρεί το $x^{q^n} - x$, τότε κάθε ρίζα του $\sigma(x)$ είναι και ρίζα του $x^{q^n} - x$, οπότε $\mathbb{K} \leq \mathbb{E}$.

Αντίστροφα, αν $\mathbb{K} \leq \mathbb{E}$, τότε επειδή το $\mathbb{E}$ είναι το σύνολο ριζών του $x^{q^n} - x$, κάθε ρίζα του $\sigma(x)$ είναι και ρίζα του $x^{q^n} - x$. Το $\sigma(x)$ όμως είναι ανάγωγο, άρα είναι το ελάχιστο πολυώνυμο (πολλαπλασιασμένο ίσως με ένα στοιχείο του σώματος $\mathbb{F}$) μιας ρίζας του $x^{q^n} - x$, επομένως διαιρεί το $x^{q^n} - x$. ό.έ.δ.

Στο Θεώρημα Α΄.3.16 είδαμε ότι αν $\mathbb{F}$ είναι ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d, τότε το σώμα ριζών του $\sigma(x)$ προκύπτει με την επισύναψη μόνο μιας ρίζας ξ στο σώμα $\mathbb{F}$.

Μπορούμε να λεπτολογήσουμε περισσότερο και να υπολογίσουμε όλες τις ρίζες ενός αναγώγου πολυωνύμου, αρκεί να γνωρίζουμε μόνο μία από αυτές.

Θεώρημα Α΄.3.18. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\sigma(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Αν ξ είναι μια ρίζα του, τότε οι υπόλοιπες ρίζες του $\sigma(x)$ είναι οι $\xi^q, \xi^{q^2}, \ldots, \xi^{q^{d-1}}$.*

Μάλιστα δε, ο d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\xi^{q^d} = \xi$.

Απόδειξη. Το πεπερασμένο σώμα $\mathbb{F}$ έχει q το πλήθος στοιχεία και το q είναι ίσο με μια δύναμη ενός πρώτου p, την χαρακτηριστική του σώματος. Από το Λήμμα Α΄.3.1 και το γεγονός ότι $a^q = a$ για κάθε $a \in \mathbb{F}$ έπεται εύκολα ότι $\sigma(\xi^q) = (\sigma(\xi))^q = 0$. Δηλαδή το ξ^q είναι ρίζα του $\sigma(x)$. Όμοια αποδεικνύεται ότι τα $\xi^{q^2}, \ldots, \xi^{q^{d-1}}$ είναι ρίζες του $\sigma(x)$.

Για να τελειώσουμε πρέπει να αποδείξουμε ότι οι ρίζες $\xi, \xi^q, \xi^{q^2}, \ldots, \xi^{q^{d-1}}$ είναι διακεκριμένες. Υποθέτουμε ότι $\xi^{q^\kappa} = \xi^{q^\lambda}$ με $0 \leq \kappa < \lambda \leq d-1$. Τότε $\xi^{q^\kappa} = \xi^{q^\lambda} = (\xi^{q^\kappa})^{q^{\lambda-\kappa}}$, δηλαδή $(\xi^{q^\kappa})^{q^{\lambda-\kappa}} - \xi^{q^\kappa} = 0$. Από την τελευταία σχέση

έχουμε ότι το ξ^{q^κ} είναι ρίζα του πολυωνύμου $x^{q^{\lambda-\kappa}}-x$. Άρα το ξ^{q^κ} είναι κοινή ρίζα του ανάγωγου πολυωνύμου $\sigma(x)$ και του πολυωνύμου $x^{q^{\lambda-\kappa}}-x$. Δηλαδή το $\sigma(x)$ διαιρεί το $x^{q^{\lambda-\kappa}}-x$. Από το Πόρισμα Α΄.3.17 έπεται ότι το d πρέπει να διαιρεί το $\lambda-\kappa$, άτοπο. ό.έ.δ.

Παρατηρήσεις Α΄.3.19. 1. Στην απόδειξη του προηγουμένου θεωρήματος θα μπορούσαμε να αποδείξουμε ότι η απεικόνιση $\alpha : \mathbb{F}(\xi) \longrightarrow \mathbb{F}(\xi)$ με $\alpha(c) = c^q$ για κάθε $c \in \mathbb{F}(\xi)$ είναι ένας $\mathbb{F}$-αυτομορφισμός του σώματος. Επομένως, πράγματι οι υπόλοιπες ρίζες του $\sigma(x)$ είναι οι $\xi^q, \xi^{q^2}, \ldots, \xi^{q^{d-1}}$.

2. Το σώμα ριζών του αναγώγου πολυωνύμου $\sigma(x) \in \mathbb{F}[x]$ βαθμού d έχει q^d το πλήθος στοιχεία, επομένως η πολλαπλασιαστική του ομάδα έχει q^d-1 το πλήθος στοιχεία. Οι δυνάμεις q^i είναι πρώτες ως προς τον q^d-1, άρα όλες οι ρίζες ξ, ξ^q, ξ^{q^2}, ... , $\xi^{q^{d-1}}$ του πολυωνύμου $\sigma(x)$ έχουν την ίδια τάξη ως στοιχεία της πολλαπλασιαστικής ομάδας του σώματος ριζών του. Επομένως, αν το ξ είναι πρωταρχικό στοιχείο του σώματος ριζών του $\sigma(x)$, τότε και οι υπόλοιπες δυνάμεις ξ^q, ξ^{q^2}, ... , $\xi^{q^{d-1}}$ είναι πρωταρχικά στοιχεία.

3. Συμφωνα με τον Ορισμό Α΄.2.35 κάθε ανάγωγο πολυώνυμο με συντελεστές από ένα πεπερασμένο σώμα είναι διαχωρίσιμο.

Το προηγούμενο θεώρημα θα μπορούσε να χρησιμεύσει στον υπολογισμό του ελαχίστου πολυωνύμου $m_c(x) \in \mathbb{F}[x]$ ενός αλγεβρικού στοιχείου c, το οποίο βρίσκεται σε μια επέκταση $\mathbb{E}$ του $\mathbb{F}$.

Πόρισμα Α΄.3.20. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και c ένα αλγεβρικό στοιχείο επί του $\mathbb{F}$. Το ελάχιστο πολυώνυμο του c είναι το πολυώνυμο $m_c(x) = (x-c)(x-c^q)\cdots(x-c^{q^{d-1}})$, όπου d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $c^{q^d} = c$. Μάλιστα δε, τα $c, c^q, \cdots, c^{q^{d-1}}$ έχουν το ίδιο ελάχιστο πολυώνυμο.*

Παρατηρήσεις Α΄.3.21. 1. Στη σχέση $m_c(x) = (x-c)(x-c^q)\cdots(x-c^{q^{d-1}})$ ο πολλαπλασιασμός στο δεύτερο μέρος γίνεται σε μια επέκταση του σώματος $\mathbb{F}$ (συγκεκριμένα στο σώμα ριζών $\mathbb{F}(c)$ του $m_c(x)$), αλλά οι

συντελεστές του $m_c(x)$, μετά τις πράξεις και την αναγωγή ομοίων όρων, βρίσκονται στο σώμα $\mathbb{F}$.

2. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathbb{K}$ μια πεπερασμένη επέκταση βαθμού m. Αν $c \in \mathbb{K}$, τότε όλες οι δυνάμεις c^{q^i}, $i = 0, 1, 2, \ldots$ ονομάζονται τα **συζυγή** στοιχεία του c (ως προς το σώμα $\mathbb{F}$). Από τα προηγούμενα έπεται ότι μόνον τα c, c^q, c^{q^2}, $\ldots$, $c^{q^{d-1}}$ είναι διακεκριμένα, όπου d είναι ο βαθμός του ελαχίστου πολυωνύμου του c επί του $\mathbb{F}$. Δηλαδή όλα τα συζυγή στοιχεία του c έχουν το ίδιο ελάχιστο πολυώνυμο επί του $\mathbb{F}$.

Πρόταση Α΄.3.22. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathbb{K}$ μια πεπερασμένη επέκταση βαθμού m. Στο σώμα $\mathbb{K}$ ορίζουμε μια σχέση ως εξής: Για $a, b \in \mathbb{K}$, $a \sim b$, αν και μόνο αν υπάρχει μη αρνητικός ακέραιος r, τέτοιος ώστε $b = a^{q^r}$. Η σχέση $\sim$ είναι σχέση ισοδυναμίας.*

Απόδειξη. Το ότι η σχέση αυτή είναι αυτοπαθής, συμμετρική και μεταβατική είναι εύκολο να αποδειχθεί και αφίεται ως άσκηση. ό.έ.δ.

Έστω $a \in \mathbb{K}$, τότε, σύμφωνα με την προηγουμένη παρατήρηση, η κλάση ισοδυναμίας C_a του a αποτελείται από τα συζυγή του, δηλαδή:

$$C_a = \{a, a^q, a^{q^2}, \ldots, a^{q^{d-1}}\},$$

όπου d είναι ο βαθμός του ελαχίστου πολυωνύμου του a επί του $\mathbb{F}$. Για τον λόγο αυτό, οι κλάσεις ισοδυναμίας στις οποίες διαμερίζεται το σώμα $\mathbb{K}$ ονομάζονται **κλάσεις συζυγίας**. Μάλιστα δε, το πλήθος των στοιχείων της C_a ισούται με τον βαθμό του ελαχίστου πολυωνύμου του στοιχείου a.

Παράδειγμα Α΄.3.23. Στο παράδειγμα Α΄.3.9 περιγράφοντας τα στοιχεία ενός σώματος $\mathbb{F}$ με 16 στοιχεία είχαμε υπολογίσει τα ελάχιστα πολυώνυμα δύο στοιχείων του επί του $\mathbb{Z}_2$. Εδώ θα υπολογίσουμε τα ελάχιστα πολυώνυμα για όλα τα στοιχεία του και τις αντίστοιχες κλάσεις συζυγίας του σώματος.

Είχαμε δει ότι το πολυώνυμο $x^4 + x + 1$ είναι πρωταρχικό πολυώνυμο. Έστω ζ ένα πρωταρχικό στοιχείο του σώματος $\mathbb{F}$, το οποίο είναι ρίζα του

$x^4 + x + 1$. Επιπλέον, το ζ είναι ένας γεννήτορας της πολλαπλασιαστικής ομάδας του σώματος. Παρατηρούμε ότι:

(i) $\zeta^{2^4} = \zeta$, άρα τα $\zeta, \zeta^2, \zeta^4, \zeta^8$ έχουν το ίδιο ελάχιστο πολυώνυμο $m_\zeta(x) = (x-\zeta)(x-\zeta^2)(x-\zeta^4)(x-\zeta^8)$ επί του $\mathbb{Z}_2$.

(ii) $(\zeta^3)^{2^4} = \zeta^3$, άρα τα $\zeta^3, \zeta^6, \zeta^{12}, \zeta^{24} = \zeta^9$ έχουν το ίδιο ελάχιστο πολυώνυμο $m_{\zeta^3}(x) = (x-\zeta^3)(x-\zeta^6)(x-\zeta^{12})(x-\zeta^9)$.

(iii) $(\zeta^5)^{2^2} = \zeta^5$, άρα τα ζ^5, ζ^{10} έχουν το ίδιο ελάχιστο πολυώνυμο $m_{\zeta^5}(x) = (x-\zeta^5)(x-\zeta^{10})$.

(iv) $(\zeta^7)^{2^4} = \zeta^7$, άρα τα $\zeta^7, \zeta^{14}, \zeta^{28} = \zeta^{13}, \zeta^{56} = \zeta^{11}$ έχουν το ίδιο ελάχιστο πολυώνυμο $m_{\zeta^7}(x) = (x-\zeta^7)(x-\zeta^{14})(x-\zeta^{13})(x-\zeta^{11})$.

Χρησιμοποιώντας το γεγονός ότι το ζ είναι ρίζα του $x^4 + x + 1$, δηλαδή $\zeta^4 = \zeta + 1$, μπορούμε να εκφράσουμε τα ελάχιστα πολυώνυμα ως πολυώνυμα με συντελεστές από το σώμα $\mathbb{Z}_2$. Συγκεκριμένα έχουμε:

$m_\zeta(x) = x^4 + x + 1$ με αντίστοιχη κλάση συζυγίας την:

$$C_\zeta = \{\zeta, \zeta^2, \zeta^4, \zeta^8\}.$$

$m_{\zeta^3}(x) = x^4 + x^3 + x^2 + x + 1$ με αντίστοιχη κλάση συζυγίας την:

$$C_{\zeta^3} = \{\zeta^3, \zeta^6, \zeta^{12}, \zeta^{24} = \zeta^9\}.$$

$m_{\zeta^5}(x) = x^2 + x + 1$ με αντίστοιχη κλάση συζυγίας την:

$$C_{\zeta^5} = \{\zeta^5, \zeta^{10}\}.$$

$m_{\zeta^7}(x) = x^4 + x^3 + 1$ με αντίστοιχη κλάση συζυγίας την:

$$C_{\zeta^7} = \{\zeta^7, \zeta^{14}, \zeta^{28} = \zeta^{13}, \zeta^{56} = \zeta^{11}\}.$$

Για τα στοιχεία του πρώτου σώματος $\mathbb{Z}_2$ έχουμε:

$m_0(x) = x$ με αντίστοιχη κλάση συζυγίας την $C_0 = \{0\}$.

$m_1(x) = x + 1$ με αντίστοιχη κλάση συζυγίας την $C_1 = \{1\}$.

Από τα πολυώνυμα αυτά μόνο τα $m_\zeta(x) = x^4 + x + 1$ και $m_{\zeta^7}(x) = x^4 + x^3 + 1$ είναι πρωταρχικά.

Δεν είναι εύκολο να υπολογίσουμε όλα τα ανάγωγα πολυώνυμα ενός συγκεκριμένου βαθμού επί ενός πεπερασμένου σώματος. Θα μπορούσαμε όμως να υπολογίσουμε το πλήθος τους.

Θεώρημα Α΄.3.24. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και n ένας θετικός ακέραιος. Το πολυώνυμο $x^{q^n} - x$ είναι το γινόμενο όλων των (διακεκριμένων) αναγώγων πολυωνύμων επί του $\mathbb{F}$, των οποίων ο βαθμός είναι διαιρέτης του n.*

Απόδειξη. Γνωρίζουμε ότι (Πόρισμα Α΄.3.17) ένα ανάγωγο πολυώνυμο διαιρεί το $x^{q^n} - x$, αν και μόνο αν ο βαθμός του διαιρεί το n. Επομένως, η ανάλυση του $x^{q^n} - x$ σε γινόμενο αναγώγων πολυωνύμων περιλαμβάνει όλα τα ανάγωγα πολυώνυμα με βαθμό που είναι διαιρέτης του n.

Ένας ανάγωγος παράγοντας του $x^{q^n} - x$ εμφανίζεται μία μόνο φορά στην ανάλυση του $x^{q^n} - x$, διότι το $x^{q^n} - x$ δεν έχει πολλαπλές ρίζες (ιδέ την απόδειξη του Θεωρήματος Α΄.3.2). Άρα, πράγματι, ισχύει ο ισχυρισμός του θεωρήματος. ό.έ.δ.

Παράδειγμα Α΄.3.25. Από το προηγούμενο θεώρημα, επικαλούμενοι το Παράδειγμα Α΄.3.23, το πολυώνυμο $x^{2^4} - x \in \mathbb{Z}_2[x]$ αναλύεται ως γινόμενο αναγώγων πολυωνύμων ως εξής:

$$x^{2^4} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1).$$

Έστω $\alpha_q(d)$ ο αριθμός των μονικών αναγώγων πολυωνύμων βαθμού d επί του πεπερασμένου σώματος $\mathbb{F}$ με q το πλήθος στοιχεία. Από το προηγούμενο θεώρημα έπεται ότι $q^n = \sum_{d|n} d \cdot \alpha_q(d)$.

Στην τελευταία σχέση αν εφαρμόσουμε τον τύπο αντιστροφής του Möbius[5]

[5] Η συνάρτηση του Möbius για έναν θετικό ακέραιο m ορίζεται ως εξής:

$$\mu(m) = \begin{cases} 1, & \text{αν } m = 1 \\ (-1)^k, & \text{αν } m = p_1 p_2 \cdots p_k, \text{ όπου οι } p_i \text{ είναι διακεκριμένοι πρώτοι} \\ 0, & \text{διαφορετικά} \end{cases}.$$

Ο τύπος αντιστροφής του Möbius είναι ο εξής:

$$\text{Αν } g(n) = \textstyle\sum_{d|n} f(d), \text{ τότε έπεται ότι } f(n) = \sum_{d|n} g(n/d)\mu(d)\,.$$

έχουμε ότι:

$$\alpha_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}.$$

Για παράδειγμα, το πλήθος των μονικών αναγώγων πολυωνύμων βαθμού 12 είναι ίσο με:

$$\begin{aligned}\alpha_q(12) &= \frac{1}{12}(\mu(1)q^{12} + \mu(2)q^6 + \mu(3)q^4 + \mu(4)q^3 + \mu(6)q^2 + \mu(12)q)\\ &= \frac{1}{12}(q^{12} - q^6 - q^4 + q^2).\end{aligned}$$

Άσκηση. 1. Να βρεθούν όλα τα μονικά ανάγωγα πολυώνυμα με συντελεστές από το $\mathbb{Z}_2$ και με βαθμό το πολύ ισόν με 4.

2. Να βρεθούν όλα τα μονικά ανάγωγα πολυώνυμα με συντελεστές από το $\mathbb{Z}_3$ και με βαθμό το πολύ ισόν με 4.

3. Να βρεθούν όλα τα μονικά ανάγωγα πολυώνυμα με συντελεστές από το $\mathbb{Z}_5$ και με βαθμό το πολύ ισόν με 3.

Άσκηση. Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία, όπου ο q είναι δύναμη περιττού πρώτου και $\theta(x) = x^2 + ax + b \in \mathbb{F}[x]$.

1. Να βρεθεί ικανή και αναγκαία συνθήκη, έτσι ώστε το πολυώνυμο $\theta(x)$ να είναι ανάγωγο επί του $\mathbb{F}$.

2. Σταθεροποιούμε τον συντελεστή a και ο b διατρέχει όλα τα στοιχεία του $\mathbb{F}$. Να βρεθεί ο αριθμός των αναγώγων πολυωνύμων της μορφής x^2+ax+b, τα οποία είναι ανάγωγα επί του $\mathbb{F}$.

3. Σταθεροποιούμε τον συντελεστή b και ο a διατρέχει όλα τα στοιχεία του $\mathbb{F}$. Να βρεθεί ο αριθμός των αναγώγων πολυωνύμων της μορφής x^2+ax+b, τα οποία είναι ανάγωγα επί του $\mathbb{F}$.

Πρόταση Α΄.3.26. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Ένα μονικό ανάγωγο πολυωνυμο $f(x) \in \mathbb{F}[x]$ βαθμού d είναι πρωταρχικό (για κάποια επέκταση $\mathbb{E}$ του $\mathbb{F}$), αν και μόνο αν το $f(x)$ διαιρεί το πολυώνυμο $x^{q^d-1}-1$ και το $f(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής x^k-1 για κάθε $k < q^d - 1$.*

Για ιδιότητες της συνάρτησης του Möbius παραπέμπουμε σε κάθε εγχειρίδιο της Θεωρίας Αριθμών. Για παράδειγμα Niven, I. and Zuckerman, H.S. and Montgomery, H.L. [1991].

Απόδειξη. Έστω $f(x) \in \mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο βαθμού d. Από το Πόρισμα Α΄.3.17 έχουμε ότι το $f(x)$ διαιρεί το $x^{q^d-1}-1$. Μάλιστα δε, ο d είναι ο μικρότερος θετικός ακέραιος s με την ιδιότητα το $f(x)$ να διαιρεί το $x^{q^s-1}-1$.

Το σώμα ριζών του πολυωνύμου $f(x)$ είναι μια επέκταση $\mathbb{E}$ του $\mathbb{F}$ με q^d το πλήθος στοιχεία. Υποθέτουμε ότι το $f(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής x^k-1 για κάθε $k < q^d-1$. Άρα, καμία ρίζα ξ του $f(x)$ δεν έχει την ιδιότητα $\xi^k = 1$ για $k < q^d-1$. Αλλά κάθε ρίζα ζ του $f(x)$ έχει την ιδιότητα $\zeta^{q^d-1} = 1$. Δηλαδή το ζ είναι γεννήτορας της πολλαπλασιαστικής ομάδας του σώματος $\mathbb{E}$. Συνεπώς, το $f(x)$ είναι πρωταρχικό πολυώνυμο του σώματος ριζών του $\mathbb{E}$.

Υποθέτουμε τώρα ότι το ανάγωγο πολυώνυμο $f(x)$ είναι πρωταρχικό πολυώνυμο σε μια επέκταση $\mathbb{E}$ του $\mathbb{F}$, δηλαδή το ελάχιστο πολυώνυμο ενός πρωταρχικού στοιχείου ζ του $\mathbb{E}$. Θα δείξουμε ότι το $f(x)$ δεν διαιρεί κανένα πολυώνυμο της μορφής x^k-1 για κάθε $k < q^d-1$.

Εφόσον το ζ είναι ρίζα του $f(x)$ οι άλλες ρίζες του είναι οι $\zeta^q, \zeta^{q^2}, \ldots, \zeta^{q^{d-1}}$. Επομένως, το σώμα ριζών που περιέχει q^d το πλήθος στοιχεία, περιέχεται στο σώμα $\mathbb{E}$, το οποίο έχει το ίδιο πλήθος στοιχείων, άρα το $\mathbb{E}$ είναι το σώμα ριζών του $f(x)$. Το $f(x)$ δεν διαιρεί κανένα πολυνώνυμο της μορφής x^k-1 για κάθε $k < q^d-1$, διότι διαφορετικά θα είχαμε $\zeta^k = 1$, άτοπο, αφού η τάξη του ζ είναι ίση με q^d-1. ό.έ.δ.

Παρατηρήσεις Α΄.3.27.

1. Στην προηγούμενη πρόταση αποδείξαμε ότι οι έννοιες πρωταρχικό πολυώνυμο και πρωταρχικό στοιχείο του σώματος ριζών του συνδέονται με το γεγονός ότι όλες οι ρίζες του πρωταρχικού πολυωνύμου είναι πρωταρχικά στοιχεία του σώματος ριζών του (βλέπε και Παρατήρηση Α΄.3.19$_2$).

2. Αν $f(x) \in \mathbb{F}[x]$ είναι ένα μονικό ανάγωγο πολυώνυμο βαθμού m, τότε ως γνωστόν το στοιχείο $c = x + \langle f(x) \rangle \in \mathbb{F}[x]/\langle f(x) \rangle$ είναι ρίζα του $f(x)$. Επομένως, το πολυώνυμο $f(x)$ είναι πρωταρχικό στο σώμα $\mathbb{E} = \mathbb{F}[x]/\langle f(x) \rangle$, αν και μόνο αν το στοιχείο $c = x + \langle f(x) \rangle$ είναι πρωταρχικό στοιχείο του σώματος.

3. Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία και $\mathbb{E}$ μια επέκτασή του βαθμού m. Ως γνωστόν, το σώμα $\mathbb{E}$ έχει $\varphi(q^m-1)$ το πλήθος πρωταρχικά στοιχεία και για κάθε ένα από αυτά τα στοιχεία το αντίστοιχο ελάχιστο πολυώνυμο επί του $\mathbb{F}$, το οποίο είναι και πρωταρχικό, έχει βαθμό ίσον με m (Θεώρημα Α΄.3.18). Επομένως, μπορούμε να ταξινομήσουμε τα πρωταρχικά στοιχεία του σώματος $\mathbb{E}$ σε (ξένα ανά δύο) υποσύνολα με m το πλήθος στοιχεία (κάθε ένα από αυτά τα υποσύνολα είναι το σύνολο ριζών ενός πρωταρχικού πολυωνύμου). Δηλαδή υπάρχουν ακριβώς $\varphi(q^m-1)/m$ το πλήθος πρωταρχικά πολυώνυμα της επέκτασης $\mathbb{E}$ επί του $\mathbb{F}$.

4. Από την προηγουμένη παρατήρηση έχουμε μια απόδειξη του εξής αριθμοθεωρητικού αποτελέσματος:

   Έστω p πρώτος αριθμός και m ένας φυσικός αριθμός. Για κάθε διαιρέτη d του m ο d διαιρεί τον αριθμό $\varphi(p^m-1)$, όπου φ είναι η συνάρτηση του Euler.

   Προσπαθήστε να δώσετε μια απόδειξη μόνο με στοιχειώδη αριθμοθεωρητικά επιχειρήματα.

Έστω $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1+a_0\in\mathbb{F}[x]$. Το πολυώνυμο $\overline{f(x)}=a_n+a_{n-1}x+\cdots+a_1x^{n-1}+a_0x^n$ ονομάζεται το **αμοιβαίο** πολυώνυμο του $f(x)$[6].

Πρόταση Α΄.3.28. *Ένα πολυώνυμο $f(x)\in\mathbb{F}[x]$ με $f(x)\neq x$ είναι ανάγωγο/πρωταρχικό, αν και μόνο αν το αμοιβαίο πολυώνυμο $\overline{f(x)}$ είναι ανάγωγο/πρωταρχικό.*

Απόδειξη. Η απόδειξη είναι εύκολη, αρκεί να παρατηρήσουμε ότι σε μία κυκλική ομάδα G το στοιχείο $a\in G$ είναι γεννήτορας, αν και μόνο αν το a^{-1} είναι γεννήτορας. ό.έ.δ.

Ορισμός Α΄.3.29. *Έστω $f(x)\in\mathbb{F}[x]$ ένα ανάγωγο πολυώνυμο, επί του πεπερασμένου σώματος $\mathbb{F}$, με $f(0)\neq 0$. Η τάξη μιας ρίζας του (άρα όλων*

[6] Συνήθως για το αμοιβαίο πολυώνυμο γράφουμε $\overline{f(x)}=x^nf(x^{-1})$, παρότι η έκφραση $f(x^{-1})$ δεν είναι πολυώνυμο.

των ριζών του, από την Παρατήρηση Α΄.3.19$_2$), ως στοιχείο της πολλαπλασιαστικής ομάδας του σώματος ριζών του, ονομάζεται **τάξη** *του* $f(x)$.

Παρατηρήσεις Α΄.3.30. 1. Αν $f(x) \in \mathbb{F}[x]$ είναι ένα ανάγωγο πολυώνυμο με $f(0) \neq 0$ και με τάξη ίση με e, τότε το $f(x)$ διαιρεί το πολυώνυμο $x^e - 1$ (γιατί; βλέπε παρατήρηση στη σελίδα 430). Μάλιστα δε, ο εκθέτης e είναι ο μικρότερος θετικός ακέραιος k με την ιδιότητα: το $f(x)$ διαιρεί το $x^k - 1$. Για τον λόγο αυτό, ορισμένες φορές, η τάξη ενός (αναγώγου) πολυωνύμου αναφέρεται και ως **εκθέτης** του πολυωνύμου, ορισμός που ισχύει για κάθε (όχι κατ' ανάγκην ανάγωγο) πολυώνυμο $\phi(x)$ με $\phi(0) \neq 0$.

2. Αν $f(x) \in \mathbb{F}$ είναι ένα ανάγωγο πολυώνυμο με $f(0) \neq 0$ με τάξη ίση με e και βαθμό $deg(f(x)) = d$, τότε η τάξη του e διαιρεί τον αριθμό $q^d - 1$, όπου q είναι το πλήθος των στοιχείων του σώματος $\mathbb{F}$.

   Πράγματι, το σώμα ριζών του αναγώγου πολυωνύμου $f(x)$ είναι ένα σώμα $\mathbb{E}$ με q^d το πλήθος στοιχεία, επομένως κάθε ρίζα του $f(x)$ είναι και ρίζα του πολυωνύμου $x^{q^d-1} - 1$, συνεπώς έχει τάξη που διαιρεί τον εκθέτη $q^d - 1$. Οπότε από τον ορισμό της τάξης πολυωνύμου έπεται ο ισχυρισμός.

Συνδυάζοντας με την Πρόταση Α΄.3.26 έχουμε ότι:

Ένα πολυώνυμο $f(x) \in \mathbb{F}$ βαθμού d είναι πρωταρχικό, αν και μόνο αν είναι μονικό, $f(0) \neq 0$ και η τάξη/ο εκθέτης του ισούται με $q^d - 1$, όπου $q = |\mathbb{F}|$.

Α΄.3.5 Οι ρίζες της μονάδας επί πεπερασμένων σωμάτων

Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία χαρακτηριστικής p (το q είναι μια δύναμη του p) και $x^n - 1 \in \mathbb{F}[x]$. Υποθέτουμε ότι $n = m \cdot p^k$ με το m να είναι πρώτο προς το p. Τότε προφανώς $x^n - 1 = x^{m \cdot p^k} - 1 = (x^m - 1)^{p^k}$, οπότε η αναζήτηση των ριζών (και γενικά η μελέτη) του $x^n - 1$ ανάγεται στη μελέτη του πολυωνύμου $x^m - 1$, όπου το m είναι πρώτο προς το p (και φυσικά προς το q). Στα επόμενα, χωρίς άλλη μνεία, θα υποθέτουμε ότι το n και το q είναι σχετικά πρώτοι.

Έστω $\mathbb{E}$ το σώμα ριζών του $x^n - 1 \in \mathbb{F}[x]$ και $\mathcal{E}_n$ το σύνολο ριζών του. Τα στοιχεία του $\mathcal{E}_n$ ονομάζονται **n−οστές ρίζες της μονάδας** επί του σώματος $\mathbb{F}$. Οι ρίζες του $x^n - 1$ είναι διακεκριμένες (γιατί;), επομένως το $\mathcal{E}_n$ είναι ένα υποσύνολο της πολλαπλασιαστικής ομάδας του σώματος ριζών $\mathbb{E}$ με n το πλήθος στοιχεία.

Πρόταση Α΄.3.31. *1. Το σύνολο $\mathcal{E}_n$ είναι μια κυκλική ομάδα τάξης n.*

2. Ο βαθμός επέκτασης $[\mathbb{E} : \mathbb{F}] = s$ είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $q^s \equiv 1 \mod n$.

Απόδειξη. Έστω $\zeta, \xi \in \mathcal{E}_n$. Τότε $(\zeta \cdot \xi^{-1})^n = \zeta^n \cdot (\xi^n)^{-1} = 1$. Άρα $\zeta \cdot \xi^{-1} \in \mathcal{E}_n$. Επομένως, οι ρίζες του $x^n - 1$ αποτελούν μια (υπο)ομάδα της πολλαπλασιαστικής ομάδας του $\mathbb{E}$, η οποία όμως είναι κυκλική. Άρα και η $\mathcal{E}_n$ είναι κυκλική.

Το σώμα ριζών $\mathbb{E}$ έχει q^s το πλήθος στοιχεία, όπου s είναι ο βαθμός επέκτασης $[\mathbb{E} : \mathbb{F}]$. Οπότε η πολλαπλασιαστική ομάδα του $\mathbb{E}$ έχει $q^s - 1$ το πλήθος στοιχεία και, επομένως, η τάξη n της υποομάδας $\mathcal{E}_n$ διαιρεί το $q^s - 1$.

Έστω r θετικός ακέραιος έτσι ώστε το n να διαιρεί το $q^r - 1$. Τότε το πολυώνυμο $x^n - 1$ διαιρεί το πολυώνυμο $x^{q^r - 1} - 1$. Δηλαδή το σώμα ριζών $\mathbb{E}$ του πολυωνύμου $x^n - 1$ περιέχεται σε κάθε σώμα με q^r το πλήθος στοιχεία, αρκεί το n να διαιρεί το $q^r - 1$. Άρα είναι το σώμα με q^s το πλήθος στοιχεία, όπου s είναι ο μικρότερος θετικός ακέραιος, έτσι ώστε το n να διαιρεί το $q^s - 1$. ό.έ.δ.

Έστω ω ένας γεννήτορας της ομάδας $\mathcal{E}_n$ των n−οστών ριζών της ομάδας. Τότε κάθε άλλη n−οστή ρίζα της μονάδας είναι της μορφής ω^i, $i = 0, 1, \ldots, n-1$. Μια τέτοια ρίζα θα λέγεται **πρωταρχική** n−οστή ρίζα της μονάδας . Μια άλλη πρωταρχική n−οστή ρίζα της μονάδας θα είναι της μορφής ω^k, όπου $\mu\kappa\delta(n, k) = 1$ (γιατί;). Επομένως, υπάρχουν $\varphi(n)$ το πλήθος πρωταρχικές ρίζες της μονάδας, όπου φ παριστά τη συνάρτηση του Euler.

Πρόταση Α΄.3.32. *Το άθροισμα των n-οστών ριζών της μονάδας ισούται με μηδέν.*

Απόδειξη. Το αποτέλεσμα είναι άμεσο από την Πρόταση Α΄.3.7. ό.έ.δ.

Δεν πρέπει να συγχέουμε τις $n-$οστές πρωταρχικές ρίζες της μονάδας με τα πρωταρχικά στοιχεία του σώματος $\mathbb{E}$ ριζών του πολυωνύμου x^n-1.

Έστω ω μια πρωταρχική $n-$οστή ρίζα της μονάδας και ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$. Τότε η τάξη του ζ είναι ίση με q^s-1 και το ω είναι μια δύναμη του ζ, δηλαδή $\omega=\zeta^k$.

Γνωρίζουμε ότι η τάξη του ω είναι ίση με n. Από την άλλη πλευρά όμως η τάξη του ζ^k είναι ίση με $\dfrac{q^s-1}{\mu\kappa\delta(k,\, q^s-1)}$. Αλλά το n διαιρεί το q^s-1, δηλαδή $q^s-1=nr$. Οπότε η τελευταία σχέση γίνεται:

$$\frac{q^s-1}{\mu\kappa\delta(k,\, q^s-1)}=\frac{nr}{\mu\kappa\delta(k,\, nr)}.$$

Επομένως, το στοιχείο ζ^k είναι πρωταρχική $n-$οστή ρίζα της μονάδας, αν και μόνο αν $\dfrac{nr}{\mu\kappa\delta(k,\, nr)}=n$, αν και μόνο αν $\mu\kappa\delta(k,\, nr)=r$, αν και μόνο αν $k=rm$, όπου το m είναι πρώτο προς το n. Άρα, αποδείξαμε το εξής θεώρημα.

Θεώρημα Α΄.3.33. *Έστω ζ ένα πρωταρχικό στοιχείο του $\mathbb{E}$, του σώματος ριζών του πολυωνύμου $x^n-1\in\mathbb{F}[x]$. Το σύνολο των πρωταρχικών $n-$οστών ριζών της μονάδος είναι το σύνολο:*

$$\Omega=\{\zeta^k \mid k=\frac{q^s-1}{n}m,\, m<n \text{ και ο } m \text{ είναι πρώτος προς τον } n\}.$$

Πόρισμα Α΄.3.34. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία και $\mathbb{E}$ το σώμα ριζών του $x^n-1\in\mathbb{F}[x]$ με q^s το πλήθος στοιχεία. Αν Φ είναι το σύνολο των πρωταρχικών στοιχείων του σώματος $\mathbb{E}$, τότε $\Omega\cap\Phi=\emptyset$, εκτός εάν $n=q^s-1$, οπότε $\Omega=\Phi$.*

Το προηγούμενο πόρισμα κάνει σαφή τη διάκριση μεταξύ πρωταρχικών ριζών του πολυωνύμου x^n-1 και πρωταρχικών στοιχείων του σώματος ριζών του.

Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία και $x^n-1\in\mathbb{F}[x]$. Επειδή οι ρίζες του x^n-1 είναι διακεκριμένες, το πολυώνυμο x^n-1 είναι το γινόμενο των διακεκριμένων ελαχίστων πολυωνύμων των αντίστοιχων ριζών του.

Έστω $\mathbb{E}$ το σώμα ριζών του x^n-1. Το $\mathbb{E}$ έχει q^s το πλήθος στοιχεία. Αν ζ είναι ένα πρωταρχικό στοιχείο του $\mathbb{E}$, τότε από το προηγούμενο θεώρημα

το στοιχείο $\omega = \zeta^{(q^s-1)/n}$ είναι μια πρωταρχική $n-$οστή ρίζα της μονάδας. Επομένως, οι ρίζες του x^n-1 είναι οι $1, \omega, \omega^2, \dots, \omega^{n-1}$.

Το ελάχιστο πολυώνυμο $m_\omega(x)$ της ρίζας ω έχει ως ρίζες τις ω, $\omega^q, \dots,$ $\omega^{q^{d-1}}$, όπου d είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\omega^{q^d} = \omega$, δηλαδή $q^d \equiv 1 \mod n$. Επομένως, $m_\omega(x) = (x-\omega)(x-\omega^q)\cdots(x-\omega^{q^{d-1}})$. Όμοια για κάθε ρίζα ω^i το αντίστοιχο ελάχιστο πολυώνυμο είναι της μορφής $m_{\omega_i}(x) = (x-\omega^i)(x-\omega^{iq})\cdots(x-\omega^{iq^{d_i-1}})$, όπου d_i είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\omega^{iq^{d_i}} = \omega^i$, δηλαδή $iq^{d_i} \equiv i \mod n$.

Από τα προηγούμενα έχουμε ότι το x^n-1 ισούται με το γινόμενο όλων των διακεκριμένων ελαχίστων πολυωνύμων των ριζών $1, \omega, \omega^2, \dots, \omega^{n-1}$. Το σύνολο ριζών καθενός από αυτά τα πολυώνυμα είναι της μορφής $C_i = \{\omega^i, \omega^{iq}, \dots, \omega^{iq^{d_i-1}}\}$, όπου d_i είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $\omega^{iq^{d_i}} = \omega^i$, δηλαδή $iq^{d_i} \equiv i \mod n$. Τα σύνολα αυτά είναι κλάσεις συζυγίας στο σώμα ριζών $\mathbb{E}$ του x^n-1 και αποτελούν μια διαμέριση το συνόλου όλων των $n-$οστών ριζών της μονάδας (βλέπε Πόρισμα Α΄.3.20, Παρατήρηση Α΄.3.21$_2$ και Πρόταση Α΄.3.22).

Αν σε κάθε κλάση συζυγίας C_i πάρουμε το σύνολο $S_i = \{i, iq, \dots, iq^{d_i-1}\}$, των εκθετών της (πρωταρχικής) ρίζας ω, τότε αυτά τα σύνολα αποτελούν μια διαμέριση του συνόλου $\{0, 1, 2, \dots, n-1\}$ των ακεραίων $\mod n$. Κάθε ένα από τα σύνολα S_i αποτελεί την *τροχιά* της μετάθεσης ϱ_q σε n σύμβολα με $\varrho_q(i) = iq(\mod n)$.

Τα σύνολα S_i ονομάζονται **κυκλοτομικά σύμπλοκα** $\mod n$ επί του σώματος $\mathbb{F}$ (ή q-κυκλοτομικά σύμπλοκα).

Ως γνωστόν ένα πεπερασμένο σώμα $\mathbb{F}$, χαρακτηριστικής p, με $q = p^s$ το πλήθος στοιχεία, είναι το σώμα ριζών του πολυωνύμου $x^q - x \in \mathbb{Z}_p[x]$. Επομένως, σύμφωνα με τα προηγούμενα, για $n = q-1$, έχουμε ότι το σύνολο όλων των μη μηδενικών στοιχείων του σώματος διαμερίζεται σε κλάσεις συζυγίας. Κατά συνέπεια το σύνολο των ακεραίων $\{0, 1, 2, \dots, q-2\}$ $\mod q-1$ διαχωρίζεται σε κλάσεις ισοδυναμίας.

Παραδείγματα Α΄.3.35. 1. Στο Παράδειγμα Α΄.3.23 είχαμε υπολογίσει τα ελάχιστα πολυώνυμα επί του $\mathbb{Z}_2$ για όλα τα στοιχεία ενός σώματος $\mathbb{F}$ με 16 στοιχεία.

Συγκεκριμμένα, αν ζ είναι ένα πρωταρχικό στοιχείο της πολλαπλασιαστικής ομάδας του $\mathbb{F}$, είχαμε δει ότι τα ελάχιστα πολυώνυμα είναι τα:

$$m_{\zeta}(x) = x^4 + x + 1 \qquad m_{\zeta^3}(x) = x^4 + x^3 + x^2 + x + 1$$
$$m_{\zeta^5}(x) = x^2 + x + 1 \qquad m_{\zeta^7}(x) = x^4 + x^3 + 1.$$

Οπότε, σύμφωνα με τα προηγουμενα, για το πολυώνυμο $x^{15} - 1 \in \mathbb{Z}_2[x]$ έχουμε $x^{15} - 1 = (x+1) \cdot (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \cdot (x^2 + x + 1) \cdot (x^4 + x^3 + 1)$.

Τα αντίστοιχα κυκλοτομικά σύμπλοκα είναι τα:

$$S_0 = \{0\}, \qquad S_1 = \{1, 2, 4, 8\}, \qquad S_3 = \{3, 6, 12, 9\},$$
$$S_5 = \{5, 10\}, \qquad S_7 = \{7, 14, 13, 11\}.$$

2. Έστω $x^{13} - 1 \in \mathbb{Z}_3[x]$. Αν $\mathbb{E}$ είναι το σώμα ριζών του, τότε σύμφωνα με την Πρόταση Α΄.3.31 ο βαθμός επέκτασης $[\mathbb{E} : \mathbb{Z}_3]$ ισούται με 3. Μάλιστα, επειδή το πολυώνυμο $x^3 + 2x + 1$ είναι ανάγωγο επί του $\mathbb{Z}_3$, μπορούμε να υποθέσουμε ότι το σώμα $\mathbb{E}$ είναι (ισόμορφο με) το $\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$. Αν ζ είναι ένα πρωταρχικό στοιχείο του $\mathbb{E}$, τότε το στοιχείο $\omega = \zeta^{(3^3-1)/13} = \zeta^2$ είναι μια πρωταρχική 13-οστη ρίζα της μονάδας (επί του $\mathbb{Z}_3$). Επειδή $\omega^{3^3} = \omega$, έχουμε ότι $m_{\omega}(x) = (x-\omega)(x-\omega^3)(x-\omega^9)$. Όμοια $m_{\omega^2}(x) = (x-\omega^2)(x-\omega^6)(x-\omega^5)$, $m_{\omega^4}(x) = (x-\omega^4)(x-\omega^{12})(x-\omega^{10})$ και $m_{\omega^7}(x) = (x-\omega^7)(x-\omega^8)(x-\omega^{11})$.

Οπότε $x^{13-1} = (x-1) \cdot m_{\omega}(x) \cdot m_{\omega^2}(x) \cdot m_{\omega^4}(x) \cdot m_{\omega^7}(x)$.

Από τα προηγούμενα έπεται αμέσως ότι η διαμέριση του $\{0, 1, 2, \ldots, 12\}$ σε 3-κυκλοτομικά σύμπλοκα είναι η εξής:

$$S_0 = \{0\}, \qquad S_1 = \{1, 3, 9\}, \qquad S_2 = \{2, 6, 5\},$$
$$S_4 = \{4, 12, 10\} \qquad S_7 = \{7, 8, 11\}.$$

Στην προηγουμένη ανάλυση του $x^{13} - 1$ σε γινόμενο αναγώγων πολυωνύμων οι παράγοντες είναι μεν πολυώνυμα με συντελεστές από το σώμα $\mathbb{Z}_3$, αλλά εδώ είναι εκφρασμένοι ως πολυώνυμα στο σώμα ριζών $\mathbb{E}$. Αν

θελήσουμε να εκφράσουμε αυτά τα πολυώνυμα ως πολυώνυμα επί του $\mathbb{Z}_3$, πρέπει να συγκεκριμενοποιήσουμε το πρωταρχικό στοιχείο ζ του σώματος $\mathbb{E} = \mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$.

Έστω $\zeta = x + \langle x^3 + 2x + 1\rangle$, μπορούμε να δείξουμε (δείξτε το!) ότι το στοιχείο αυτό είναι πράγματι πρωταρχικό στοιχείο. (Εναλλακτικά μπορείτε να αποδείξετε, σύμφωνα με την Παρατήρηση Α΄.3.27 $_2$, ότι το πολυώνυμο $x^3 + 2x + 1$ είναι πρωταρχικό πολυώνυμο επί του $\mathbb{Z}_3$). Το στοιχείο ζ είναι ρίζα του x^3+2x+1, επομένως από τη σχέση $\zeta^3+2\zeta+1 = 0$ και το γεγονός ότι $\omega = \zeta^2$ έχουμε ότι $\omega^3 + \omega^2 + \omega = 1$. Από την τελευταία σχέση μπορούμε (προσπαθήστε το με υπομονή!) να δούμε ότι:

$$m_{\omega}(x) = x^3 + x^2 + x + 2 \qquad m_{\omega^2}(x) = x^3 + x^2 + 2$$
$$m_{\omega^4}(x) = x^3 + 2x^2 + 2x + 2 \qquad m_{\omega^7}(x) = x^3 + 2x + 2.$$

Άρα $x^{13-1} = (x-1)\cdot(x^3 + x^2 + x + 2)\cdot(x^3 + x^2 + 2)\cdot(x^3 + 2x^2 + 2x + 2)\cdot(x^3 + 2x + 2)$.

3. Έστω $x^9 - 1 \in \mathbb{Z}_2[x]$. Ο ελάχιστος θετικός ακέραιος k με την ιδιότητα $9 \mid 2^k - 1$ είναι ο $k = 6$, επομένως το σώμα ριζών του πολυωνύμου αυτού, έστω $\mathbb{E}$, είναι επέκταση του $\mathbb{Z}_2$ με βαθμό επέκτασης ίσον με 6. Το πολυώνυμο x^6+x+1 είναι ανάγωγο επί του $\mathbb{Z}_2$, διαιρεί το πολυώνυμο $x^{63} - 1$ και δεν διαιρεί κανένα άλλο πολυώνυμο της μορφής $x^k - 1$ για $1 \le k < 63$ (ελέγξτε το!), επομένως είναι πρωταρχικό (Πρόταση Α΄.3.26). Άρα, θεωρώντας ως σώμα ριζών το σώμα $\mathbb{Z}_2[x]/\langle x^6 + x + 1\rangle$ και ως πρωταρχικό στοιχείο το $\zeta = x + \langle x^6 + x + 1\rangle$, βλέπουμε ότι μια 9-ατη πρωταρχική ρίζα της μονάδος είναι το στοιχείο $\omega = \zeta^7$. Οι κλάσεις συζυγίας, οι οποίες ορίζονται από τις δυνάμεις της πρωταρχικής ρίζας ω είναι οι εξής:

$$C_{\omega^9=1} = \{1\}, \quad C_{\omega^3} = \{\omega^3, \omega^6\}, \quad C_{\omega} = \{\omega, \omega^2, \omega^4, \omega^8, \omega^{16} = \omega^7, \omega^{32} = \omega^5\}.$$

Η αντίστοιχη διαμέριση του συνόλου $\{0, 1, 2, \ldots, 8\}$ σε 2-κυκλοτομικά σύμπλοκα είναι η εξής:

$$S_0 = \{0\},\ S_3 = \{3, 6\} \text{ και } S_1 = \{1, 2, 4\, 8, 7, 5, \}.$$

Στην πρώτη κλάση αντιστοιχεί το πολυώνυμο $x-1$. Στη δεύτερη κλάση αντιστοιχεί το πολυώνυμο x^2+x+1, το οποίο είναι και το μοναδικό μονικό ανάγωγο πολυώνυμο βαθμού 2 επί του $\mathbb{Z}_2$. Στην τελευταία κλάση αντιστοιχεί ένα μονικό ανάγωγο πολυώνυμο βαθμού 6 επί του $\mathbb{Z}_2$. Δεδομένου ότι $\omega = \zeta^7 = \zeta^2 + \zeta$ (γιατί;), έπεται εύκολα (ελέγξτε το!) ότι $\omega^6 + \omega^3 + 1 = 0$, δηλαδή το ω είναι ρίζα του αναγώγου πολυωνύμου $x^6 + x^3 + 1$. Άρα, τελικά, $x^9 - 1 = (x-1)\cdot(x^2+x+1)\cdot(x^6+x^3+1)$.

Προφανώς θα μπορούσαμε να παραγοντοποιήσουμε το πολυώνυμο $x^9 - 1 \in \mathbb{Z}_2[x]$ στοιχειωδώς ως εξής: $x^9 - 1 = (x^3)^3 - 1 = (x^3-1)\cdot(x^6 + x^3 + 1) = (x-1)\cdot(x^2+x+1)\cdot(x^6+x^3+1)$.

Άσκηση. Να βρεθούν όλα τα 2-κυκλοτομικά σύμπλοκα $\mod 23$.

Προσπαθήστε να αναλύσετε το πολυώνυμο $x^{23} - 1 \in \mathbb{Z}_2[x]$ σε γινόμενο αναγώγων παραγόντων.

(*Υπόδειξη:* Δείξτε ότι το 23 διαιρεί το $2^{11} - 1$ και ότι δεν υπάρχει μικρότερος θετικός ακέραιος k, ώστε το 23 να διαιρεί το $2^k - 1$.)

Άσκηση. Να επαναλάβετε την προηγουμένη άσκηση για το πολυώνυμο $x^n - 1 \in \mathbb{Z}_q[x]$ για τα ζεύγη $q = 2$, $n = 45, q = 3$, $n = 41$.

Ο προηγούμενος τρόπος παραγοντοποίησης του πολυωνύμου $x^n - 1$, όπως φαίνεται και από τα παραδείγματα, έχει το μειονέκτημα ότι οι πράξεις πρέπει να γίνονται στο σώμα ριζών του.

Θα δούμε έναν άλλο τρόπο παραγοντοποίησης του πολυωνύμου $x^n - 1 \in \mathbb{F}[x]$.

Έστω ω μια πρωταρχική ρίζα του $x^n - 1$. Τότε όλες οι ρίζες είναι οι δυνάμεις ω^k. Αν το k είναι πρώτο προς το n, τότε έχουμε μια άλλη πρωταρχική ρίζα. Αν το k δεν είναι πρώτο προς το n, τότε η τάξη $m = \dfrac{n}{\mu\kappa\delta(k,\ n)}$ της ω^k ως στοιχείο της ομάδας $\mathcal{E}_n$ είναι ένας διαιρέτης του n. Δηλαδή η ω^k είναι $m-$οστή πρωταρχική ρίζα της μονάδος.

Αντίστροφα, για κάθε διαιρέτη m του n κάθε ρίζα του $x^m - 1$ είναι ρίζα του $x^n - 1$. Άρα, τελικά, όλες οι ρίζες του $x^n - 1$ είναι πρωταρχικές ρίζες στα πολυώνυμα $x^m - 1$ με m διαιρέτη του n.

Από τα προηγούμενα οδηγούμαστε στον επόμενο ορισμό.

Ορισμός Α΄.3.36. *Έστω $\mathbb{F}$ ένα σώμα με q το πλήθος στοιχεία και k ένας θετικός ακέραιος πρώτος προς τον q. Το* ***κυκλοτομικό*** *πολυώνυμο τάξης k επί του $\mathbb{F}$ είναι το μονικό πολυώνυμο $Q_k(x)$, του οποίου οι ρίζες είναι οι πρωταρχικές $k-$στές ρίζες της μονάδος.*

Γνωρίζουμε ότι οι πρωταρχικές $k-$στές ρίζες της μονάδας είναι $\varphi(k)$ το πλήθος, όπου φ είναι η συνάρτηση του Euler. Δηλαδή αν $\zeta_1, \zeta_2, \dots, \zeta_{\varphi(k)}$ είναι οι πρωταρχικές $k-$στές ρίζες της μονάδας, τότε:

$$Q_k(x) = (x-\zeta_1)(x-\zeta_2)\cdots(x-\zeta_{\varphi(k)}).$$

Από τη συζήτηση που προηγήθηκε του ορισμού έπεται άμεσα ότι:

$$x^n - 1 = \Pi_{d|n} Q_d(x).$$

Παρατηρήσεις Α΄.3.37.

1. Από τον τρόπο ορισμού των κυκλοτομικών πολυωνύμων δεν έπεται ότι οι συντελεστές τους είναι στοιχεία του σώματος $\mathbb{F}$. Αλλά, αν $x^n - 1 = m_1(x)\cdot m_2(x)\cdots m_\nu(x)$ είναι η ανάλυση του x^n-1 σε γινόμενο αναγώγων πολυωνύμων επί του $\mathbb{F}$, τότε από τη σχέση $x^n - 1 = m_1(x)\cdot m_2(x)\cdots m_\nu(x) = \Pi_{d|n} Q_d(x)$, αν ζ είναι μια ρίζα ενός $Q_d(x)$, αυτή θα είναι ρίζα ενός (μόνο) $m_i(x)$. Οπότε οι ρίζες του $m_i(x)$ είναι οι $\zeta, \zeta^q, \dots, \zeta^{q^{d-1}}$. Η ζ ως ρίζα του $Q_d(x)$ έχει τάξη ίση με d (ως πρωταρχική $d-$οστη ρίζα της μονάδας), οπότε όλες οι ρίζες $\zeta, \zeta^q, \dots, \zeta^{q^{d-1}}$ του $m_i(x)$ έχουν τάξη ίση με d (γιατί;). Επομένως, όλες είναι πρωταρχικές $d-$οστες ρίζες της μονάδας, άρα όλες είναι ρίζες του $Q_d(x)$, δηλαδή το $m_i(x)$ διαιρεί το $Q_d(x)$. Τελικά κάθε $Q_d(x)$ είναι το γινόμενο (κάποιων από τα) $m_i(x) \in \mathbb{F}[x]$, άρα και τα $Q_d(x) \in \mathbb{F}[x]$.

2. Υπάρχει ένας άλλος (αναδρομικός) τρόπος, με τον οποίο όχι μόνο διαπιστώνουμε ότι τα κυκλοτομικά πολυώνυμα έχουν συντελεστές από το σώμα $\mathbb{F}$, αλλά μπορούμε να τα υπολογίσουμε.

$$x^2-1 = Q_1(x)Q_2(x) \qquad x^3-1 = Q_1(x)Q_3(x)$$
$$x^4-1 = Q_1(x)Q_2(x)Q_4(x) \qquad x^5-1 = Q_1(x)Q_5(x)$$
$$x^6-1 = Q_1(x)Q_2(x)Q_3(x)Q_6(x)$$

και έπεται η συνέχεια.

Οπότε έχουμε:

$$Q_1(x) = x-1, \quad Q_2(x) = x+1, \quad Q_3(x) = x^2+x+1,$$
$$Q_4(x) = \frac{x^4-1}{Q_1(x)Q_2(x)} = x^2+1, \quad Q_5(x) = \frac{x^5-1}{Q_1(x)} = x^4+x^3+x^2+x+1,$$
$$Q_6(x) = \frac{x^6-1}{Q_1(x)Q_2(x)Q_3(x)} = x^2-x+1$$

και έπεται η συνέχεια.

3. Επίσης, με επαγωγή μπορούμε να αποδείξουμε ότι τα κυκλοτομοκά πολυώνυμα έχουν τους συντελεστές τους στο πρώτο σώμα $\mathbb{Z}_p$, όπου p είναι η χαρακτηριστική του σώματος $\mathbb{F}$ (προσπαθήστε το!).

4. Ο προηγούμενος τρόπος υπολογισμού των κυκλοτομικών πολυωνύμων είναι χρονοβόρος και λόγω της αναδρομικότητας μετά από ορισμένα βήματα στην πράξη είναι ατελέσφορος.

   Θα μπορούσαμε να υπολογίζουμε τα κυκλοτομικά πολυώνυμα απευθείας για κάθε τάξη k. Εφαρμόζουμε τον τύπο αντιστροφής του Möbius (βλέπε σελίδα 445) στη σχέση $x^n-1 = \prod_{d|n} Q_d(x)$ και έχουμε ότι $Q_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)} = \prod_{d|n}(x^{n/d}-1)^{\mu(d)}$. Αλλά προσοχή! Μερικοί από τους εκθέτες στο προηγούμενο γινόμενο ενδέχεται να είναι ίσοι με -1, οπότε πρέπει να γίνουν οι αντίστοιχες διαιρέσεις.

Παραδείγματα Α΄.3.38. 1. Έστω $x^{15}-1 = Q_1(x)Q_3(x)Q_5(x)Q_{15}(x) \in \mathbb{Z}_2[x]$. Σύμφωνα με τα προηγούμενα έχουμε ότι:

$$\begin{aligned}
Q_1(x) &= x-1,\\
Q_3(x) &= (x^3-1)(x-1)^{-1} = x^2+x+1,\\
Q_5(x) &= (x^5-1)(x-1)^{-1} = x^4+x^3+x^2+x+1,\\
Q_{15}(x) &= (x^{15}-1)(x^5-1)^{-1}(x^3-1)^{-1}(x-1) = \frac{(x^{15}-1)(x-1)}{(x^5-1)(x^3-1)}\\
&= x^8+x^7+x^5+x^4+x^3+x+1.
\end{aligned}$$

Οπότε έχουμε $x^{15}-1 = (x-1)\cdot(x^2+x+1)\cdot(x^4+x^3+x^2+x+1)\cdot(x^8+x^7+x^5+x^4+x^3+x+1)$.

Στο Παράδειγμα Α΄.3.35$_1$ είχαμε δει την ανάλυση του πολυωνύμου $x^{15}-1 \in \mathbb{Z}_2[x]$ ως εξής: $x^{15}-1 = (x+1)\cdot(x^4+x+1)\cdot(x^4+x^3+x^2+x+1)\cdot(x^2+x+1)\cdot(x^4+x^3+1)$. Εύκολα βλέπουμε ότι $Q_{15}(x) = x^8+x^7+x^5+x^4+x^3+x+1 = (x^4+x+1)\cdot(x^4+x^3+1)$, δηλαδή τα κυκλοτομικά πολυώνυμα δεν είναι εν γένει ανάγωγα πολυώνυμα.

2. Στο Παράδειγμα Α΄.3.35$_2$ είχαμε δει την ανάλυση του πολυωνύμου $x^{13}-1 \in \mathbb{Z}_3[x]$ ως εξής:

$$x^{13-1} = (x-1)\cdot(x^3+x^2+x+2)\cdot(x^3+x^2+2)\cdot(x^3+2x^2+2x+2)\cdot(x^3+2x+2).$$

Η ανάλυση του πολυωνύμου αυτού σε κυκλοτομικά πολυώνυμα δεν προσφέρει, καθότι $x^{13}-1 = Q_1(x)Q_{13}(x) = (x-1)\cdot(x^{12}+x^{11}+\cdots+x+1)$.

3. Στο Παράδειγμα Α΄.3.35$_3$ είχαμε δει την ανάλυση του πολυωνύμου $x^9-1 \in \mathbb{Z}_2[x]$ ως εξής:

$$x^9-1 = (x-1)\cdot(x^2+x+1)\cdot(x^6+x^3+1).$$

Η ανάλυση του πολυωνύμου αυτού σε κυκλοτομικά πολυώνυμα είναι $x^9-1 = Q_1(x)Q_3(x)Q_9(x) = (x-1)\cdot(x^2+x+1)\cdot(x^6+x^3+1)$, δηλαδή η προηγουμένη.

Από τα προηγούμενα βλέπουμε ότι, αν θέλουμε την παραγοντοποίηση του πολυωνύμου $x^n-1 \in \mathbb{F}[x]$, όπου $\mathbb{F}$ είναι ένα πεπερασμένο με q το πλήθος στοιχεία, με την βοήθεια των κυκλοτομικών πολυωνύμων, πρέπει να μπορούμε να αποφανθούμε πότε ένα κυκλοτομικό πολυώνυμο είναι ανάγωγο.

Πρόταση Α΄.3.39. *Έστω $\mathbb{F}$ ένα πεπερασμένο σώμα με q το πλήθος στοιχεία. Το κυκλοτομικό πολυώνυμο $Q_n(x) \in \mathbb{F}[x]$ αναλύεται σε $\varphi(n)/k$ το πλήθος ανάγωγους παράγοντες, καθένας βαθμού k, όπου k είναι ο μικρότερος θετικός ακέραιος, έτσι ώστε $n \mid q^k-1$ (δηλαδή η τάξη κάθε ανάγωγου παράγοντα είναι ίση με n).*

Επομένως, το $Q_n(x)$ είναι ανάγωγο, αν και μόνο αν $k = \varphi(n)$.

Απόδειξη. Άσκηση....

Παρατηρήστε ότι, από τον ορισμό, το κυκλοτομικό πολυώνυμο $Q_n(x)$ έχει βαθμό ίσον με $\varphi(n)$ και ρίζες τις πρωταρχικές n-οστες ρίζες της μονάδας.... ό.έ.δ.

Βιβλιογραφία

Hamming, R. *"Coding and Information Theory"*. Prentice-Hall, Englewood Cliffs 2^{nd} Edition, 1986.

Herstein, I. N. *"Abstract Algebra"*. New York: Macmillan, 1990.

Lidl, R. and Niederreiter H. . *"Introduction to finite fields and their applications"*. Cambridge University Prees, 2000.

McDonald, B. R. *"Finite Rings with Identity"*. New York: Marcel Dekker, 1947.

McEliece, R. J. *"Finite Fields for Computer Scientists and Engineers"*. Boston: Kluwer Academic Publishers, 1987.

Mullen, G. L. and Mummert C. *"Finite Fields and Applications"*, volume 41 of *Student Mathematical Library*. AMS, 2007.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Walker, J. L. *"Codes and Curves"*, volume 7 of *Student Mathematical Library*. AMS, 2000.

Σ. Ανδρεαδάκης. *Θεωρία Galois*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1992.

Σ. Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1993.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

Βιβλιογραφία

Η παρατιθέμενη Βιβλιογραφία δεν είναι πλήρης. Απλώς είναι ενδεικτική και αποσκοπεί ώστε ο ενδιαφερόμενος αναγνώστης να *απεγκλωβιστεί* από την προσήλωση σε ένα μόνο βιβλίο.

Βιβλιογραφία

Anderson, I. *"A first course in Combinatorial Mathematics"*. Oxford University Prees, 2000.

Berlekamp, E. R. *"Algebraic Coding Theory"*. Laguna Hills, CA: Aegean Park Press, 1984.

Hall, J.I. *Notes on Coding Theory*. (σε ηλεκτρονική μορφή). www.math.msu.edu/~jhall.

Hamming, R. *"Coding and Information Theory"*. Prentice-Hall, Englewood Cliffs 2^{nd} Edition, 1986.

Herstein, I. N. *"Abstract Algebra"*. New York: Macmillan, 1990.

Hill, R. *"A First Course in Coding Theory"*. Oxford University Press, Oxford, 1986.

Huffman, C. W. and Pless, V. . *"Fundamentals of Error-Correcting Codes"*. Cambridge University Press, 2003.

Justesen, J. and Hoholdt, T. *"A Course In Error-Correcting Codes"*. European Mathematical Society, 2004.

Lidl, R. and Niederreiter H. . *"Introduction to finite fields and their applications"*. Cambridge University Prees, 2000.

MacWilliams, F.J. and Sloane, N.J.A. *"The Theory of Error-correcting Codes"*. North-Holland, Amsterdam, 1977.

McDonald, B. R. *"Finite Rings with Identity"*. New York: Marcel Dekker, 1947.

McEliece, R. J. *"Finite Fields for Computer Scientists and Engineers"*. Boston: Kluwer Academic Publishers, 1987.

Mullen, G. L. and Mummert C. *"Finite Fields and Applications"*, volume 41 of *Student Mathematical Library*. AMS, 2007.

Niven, I. and Zuckerman, H.S. and Montgomery, H.L. *"An Introduction to the Theory of Numbers"*. John Wiley & Sons, Inc., New York, 5^{th} Edition, 1991.

Pless, V. *"Introduction to the Theory of Error-Correcting Codes"*. Wiley, New York, 1998.

Pretzel, O. *"Error-Correcting Codes and Finite Fields"*. Oxford University Press, Oxford, 1992.

Roman, S. *"Coding and Information Theory"*. Springer-Verlag, 1992.

Ron M. Roth. *"Introduction to Coding Theory"*. Cambridge University Press, 2006.

van Lint, J.H. *"Introduction to Coding Theory"*. Springer-Verlag, 1999.

vanLint, J.H. and Wilson, R.M. *"A course in Combinatorics"*. Cambridge University Prees , 2001.

Vermani, L. *"Elements of Algebraic Coding Theory"*. Chapman and Hall, London, 1996.

Walker, J. L. *"Codes and Curves"*, volume 7 of *Student Mathematical Library*. AMS, 2000.

Σ. Ανδρεαδάκης. *Θεωρία Galois*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1992.

Σ. Ανδρεαδάκης. *Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΥΜΜΕΤΡΙΑ, 1993.

Δ. Βάρσος. *Στοιχεία Αλγεβρικής Θεωρίας Κωδίκων*. Εκδόσεις Σοφία, 2005.

Δ. Βάρσος, Δ. Δεριζιώτης, Ι. Εμμανουήλ, Μ. Μαλιάκας και Ο. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις ΣΟΦΙΑ, 2013.

Δ. Πουλάκης. *Αλγεβρικοί Κώδικες*. Εκδόσεις ΖΗΤΗ, 2010.

Ευρετήριο