Σημειώσεις Αλγεβρικών Αλγορίθμων

Γιάννης Ζ. Εμίρης
Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών
emiris@di.uoa.gr

1 Νοεμβρίου 2011

Περιεχόμενα

Κεφάλαιο 1

Γενικό Διάγραμμα

Το κεφάλαιο παρουσιάζει συνοπτικά τις ενότητες «Αλγεβρικών αλγορίθμων», με έμφαση σε περιοχές του προσωπικού μας ενδιαφέροντος. Η έκταση των ενοτήτων αυτών ίσως ξεπερνά τα όρια ενός εξαμηνιαίου μαθήματος. Το κεφάλαιο καταλήγει με έναν κατάλογο αλγεβρικών λογισμικών.

1.1 Αναπαράσταση και πολυπλοκότητα

1. Σύγκριση αλγεβρικών αλγορίθμων απόλυτης ακρίβειας με προσεγγιστικές αριθμητικές μεθόδους και το αντίστοιχο υπολογιστικό κόστος.
2. Στοιχεία θεωρίας αλγορίθμων: υπολογιστικά μοντέλα, ασυμπτωτική πολυπλοκότητα.
3. Αναπαράσταση αριθμών: ακέραιοι απεριόριστης ακρίβειας, πραγματικοί floating point.
4. Αναπαράσταση πινάκων: πυκνή ή αραιή.
5. Αναπαράσταση πολυωνύμων μίας και πολλών μεταβλητών: πυκνή ή αραιή.

1.2 Αποτελεσματική ακριβής αριθμητική

1. Βασικές πράξεις μεταξύ ακεραίων και ρητών: πρόσθεση, πολλαπλασιασμός, διαίρεση με υπόλοιπο. Αντίστροφος μέσω επαναληπτικής μεθόδου του Νεύτωνα.
2. Βασικές πράξεις μεταξύ πολυωνύμων, συμπεριλαμβανομένου του αντιστρόφου $\mathrm{mod} x^{2n}$. Αντιστοιχία προβλημάτων και μεθόδων μεταξύ ακεραίων και πολυωνύμων.
3. Υπολογισμός μιας τιμής (μέθοδος Horner) και περισσοτέρων τιμών πολυωνύμου.
4. Υπολογισμός συντελεστών από τιμές (παρεμβολή). Επέκταση σε πολυώνυμα πολλών μεταβλητών και εκμετάλλευση αραιότητας.
5. Ταχύς Μετασχηματισμός Fourier (FFT). Εφαρμογή στον πολλαπλασιασμό ακεραίων. Επέκταση στα πολυώνυμα.
6. Κινέζικο θεώρημα στους ακεραίους. Απεριόριστη ακρίβεια μέσω της αριθμητικής των υπολοίπων. Επέκταση στα πολυώνυμα μίας μεταβλητής.

7. Βασικές πράξεις μεταξύ πινάκων και υπολογισμός της ορίζουσας. Πίνακες με ταχύ πολλαπλασιασμό με διάνυσμα και αλγόριθμοι " μαύρου κουτιού ".

8. Μέγιστος Κοινός Διαιρέτης (ΜΚΔ) στους ακεραίους: αλγόριθμος του Ευκλείδη και επέκτασή του. Εφαρμογή στα πολυώνυμα μιας μεταβλητής. Γενίκευση για τον υπολογισμό ρητής προσέγγισης Padé.

9. Παραγωντοποίηση στους ακεραίους, στα πολυώνυμα με συντελεστές σε πεπερασμένο σώμα και σε γενικά πολυώνυμα.

1.3 Πραγματικές ρίζες πολυωνύμου

1. Αντιπαράθεση με το αντίστοιχο πρόβλημα για μιγαδικές ρίζες και τις υπάρχουσες αριθμητικές μεθόδους (π.χ. επαναληπτική μέθοδος Newton). Αλγεβρικές επαναληπτικές μέθοδοι: p-αδική ανύψωση Hensel.

2. Ακολουθίες Sturm για μια μεταβλητή. Ομοιότητες με τον υπολογισμό του ΜΚΔ. Απομόνωση και προσέγγιση πραγματικών λύσεων.

3. Κανόνας Descartes, μέθοδος Vincent / Uspensky.

4. Γενίκευση Sturm σε πολυώνυμα πολλών μεταβλητών. Μέθοδος προσήμων Ben-or,Kozen,Reif. Κυλινδρική αλγεβρική υποδιαίρεση.

1.4 Επίλυση μη γραμμικών πολυωνυμικών συστημάτων

1. Αριθμός εξισώσεων ως προς τον αριθμό μεταβλητών. Από τα γραμμικά στα μη γραμμικά συστήματα.

2. Όρια στον αριθμό των κοινών ριζών: κλασικά όρια Bézout και αραιό όριο (Bernstein).

3. Βάσεις Groebner και αλγόριθμος του Buchberger. Αντιστοιχίες με τον Ευκλείδειο αλγόριθμο του ΜΚΔ πολυωνύμων μιας μεταβλητής και τη μέθοδο απαλειφής του Gauss για γραμμικά συστήματα.

4. Μέθοδος της επιλύουσας (ή απαλείφουσας) πολυωνύμων για την επίλυση συστημάτων. Κλασική και αραιή επιλύουσα. Αναγωγή σε ένα πρόβλημα γραμμικής άλγεβρας. Αντιστοιχίες με (α) τις μεθόδους Sylvester και Bézout για μια μεταβλητή και (β) τον κανόνα Cramer για γραμμικά συστήματα.

5. Δομημένοι πίνακες.

1.5 Εφαρμογές

1. Γεωμετρική μοντελοποίηση: Αλγεβρικοποίηση (implicitization) παραμετρικής έκφρασης μιας καμπύλης ή (υπερ)επιφάνειας. Τομή επιφανειών. Κωνικές τομές και μεταξύ τους κοινά σημεία. Offset καμπύλης.

2. Κινηματική σειριακών και παράλληλων ρομποτικών μηχανισμών: Κίνηση βραχίονα ρομπότ με 6 περιστροφικούς βαθμούς ελευθερίας (6R).

3. Επέκταση της κινηματικής των ρομπότ στον υπολογισμό των διατάξεων μορίου. Σταθερότητα μιας μοριακής διάταξης.

4. Θεωρία κωδίκων και Κρυπτογραφία (σύστημα RSA).

5. Επεξεργασία σήματος και εικόνας. Τεχνητή όραση: Υπολογισμός κίνησης αντικειμένου από σειρά εικόνων σταθερής κάμερας.

6. Υπολογιστική γεωμετρία και κατηγορήματα (predicates). Αυτόματη απόδειξη γεωμετρικών θεωρημάτων.

1.6 Λογισμικά

Αναφέρουμε ενδεικτικά ορισμένα λογισμικά σε C/C++.

1. Τα γενικά πακέτα που κυκλοφορούν, έχουν συνήθως εύχρηστο interface, αλλά είναι πληρωτέα: Τα πιο πλήρη είναι τα Maple (http://www.maplesoft.com), Mathematica. Υπάρχει επίσης το Reduce (http://ftp.rand.org/software_and_data/reduce), Axiom κλπ. Πληρωτέα πακέτα με μικρή δωρεάν έκδοση ή δωρεάν κατόπιν αίτησης είναι τα Mupad, Magma (linux).

2. Για αριθμητική ακριβείας και βασικές πράξεις: LiDIA (http://www-jb.cs.uni-sb.de/linktop/LiDIA), CORE (http://www.cs.nyu.edu/cs/faculty/yap), PARI,
SYNAPS (http://www-sop.inria.fr/galaad/software/synaps/) κλπ.

3. Γενικό αριθμητικό πακέτο: Matlab. Για την αριθμητική επίλυση μιας εξίσωσης, ίσως το καλύτερο λογισμικό οφείλεται στους Bini-Fiorentino που υλοποίησαν τον αλγόριθμο Aberth στο πακέτο Mpsolve, προσβάσιμο και μέσω της Synaps.

   Υπάρχουν διάφορες υλοποιήσεις αριθμητικών αλγορίθμων για την επίλυση αλγεβρικών συστημάτων, όπως αυτά που χρησιμοποιούν μεθόδους ομοτοπίας (PHCpack [Verschelde]), αριθμητική διατημάτων (Icos [Lebbah], Alias [Merlet], Intlab [Rump]), τοπολογικό βαθμό (Chabis [Βραχάτης]) κλπ.

4. Τα ισχυρότερα αλγεβρικά πακέτα που προσφέρουν επίλυση εξισώσεων είναι συνήθως δωρεάν. Τα παρακάτω υλοποιούν τις βάσεις Gröbner: Cocoa [Genova], FGb [Faugère, Paris], Macaulay (http://www.math.uiuc.edu/Macaulay2) [Cornell], Singular [Kaiserslautern].

   Για την επίλυση με μεθόδους πινάκων, όπως η απαλοίφουσα, υπάρχει η SYNAPS (http://www-sop.inria.fr/galaad/software/synaps/).

   Για την επίλυση στους πραγματικούς υπάρχει το RS του Rouillier, το οποίο διαθέτει πρόσβαση από το Maple και «συνεργάζεται» με το FGb σε μια κοινή πλατφόρμα που ονομάζεται Gb-RS. Υπάρχει επίσης το πακέτο SYNAPS::algebraic του Η. Τσιγαρίδα.

Κεφάλαιο 2

Θεωρητικό υπόβαθρο

2.1 Εισαγωγή

Οι αλγεβρικοί αλγόριθμοι αφορούν σε αλγεβρικά προβλήματα και, σε αντίθεση με αριθμητικές και αναλυτικές μεθόδους, χαρακτηρίζονται από απόλυτη ακρίβεια αποτελέσματος:

$$\det \begin{bmatrix} 1 & 2 \\ 2 & 3,999\ldots \end{bmatrix} = -0,000\ldots 1 < 0 < \det \begin{bmatrix} 1 & 2 \\ 2 & 4,000\ldots 01 \end{bmatrix}$$

με αντίτιμο το σχετικά υψηλό υπολογιστικό κόστος λόγω της πιθανής έκρηξης του μεγέθους των (ενδιάμεσων) τιμών. Παρακάτω συνοψίζεται μια σύγκριση των αλγεβρικών και των αριθμητικών μεθόδων.

Αλγεβρικοί αλγόριθμοι	- έναντι -	(προσεγγιστικών) αριθμητικών μεθόδων
απόλυτη ακρίβεια $\gg$		ακρίβεια αποτελέσματος (accuracy): περιορίζεται από το αριθμητικό σφάλμα
έκρηξη ενδιαμέσων τιμών		σταθερότητα (stability) αποτελέσματος ως προς το αριθμητικό σφάλμα
(intermediate swell)		Βαθμός ακρίβειας των υπολογισμών: μετράται από το πλήθος των χρησιμοποιούμενων ψηφίων (precision)
υψηλή υπολογιστική πολυπλοκότητα	$\gg$	συνήθως ικανοποιητική ταχύτητα
δυαδική (Boolean) πολυπλοκότητα		αριθμητική πολυπλοκότητα: όλες οι πράξεις έχουν μοναδιαίο (ενιαίο) κόστος
μέγεθος αποτελέσματος (κατώτερο όριο)		conditioning = = απόσταση από εκφυλισμένη κατάσταση (singularity)

Π.χ. υπολογισμός ορίζουσας πίνακα 2×2:

4πολλ/σμοί, 3 ΜΚΔ, 1 ΕΚΠ, 1πρόσθεση	2πολλ/σμοί, 1πρόσθεση

$$\det \begin{bmatrix} 2/3 & 4/5 \\ 4/3 & 389/250 \end{bmatrix} = \frac{2}{3}\cdot\frac{289}{250} - \frac{4}{3}\cdot\frac{4}{5} == \frac{11}{375} \qquad \det \begin{bmatrix} 0,666\ldots & 0,8 \\ 1,333\ldots & 1,556 \end{bmatrix} = 1,037333\cdots - 1,0666\ldots$$

Η περιοχή των αλγεβρικών αλγορίθμων ονομάζεται επίσης «άλγεβρα με υπολογιστή» (computer algebra), «υπολογιστική άλγεβρα» (computational algebra), αλλιώς «συμβολική επεξεργασία» (symbolic computation) διότι επεξεργάζεται σύμβολα: μεταβλητές x, y, πολυώνυμα κλπ. Ορισμένα τυπικά και σημαντικά παραδείγματα:

- πολλαπλασιασμός πολυωνύμων: $(x^2+3)*(x+286) \to x^3+286x^2+3x+858$.
- διαίρεση πολυωνύμων: $x^3+286x^2+3x+858/(x^2+3) \to x+286$.
- επίλυση πολυωνύμων (και αργότερα συστημάτων): $x^3+286x^2+3x+858 \to \{-286, -i\sqrt{3}, i\sqrt{3}\}$.
- ΜΚΔ πολυωνύμων: $x^3+286x^2+3x+858, 135x^2+37659x-286 \to x+286$.

2.2 Υπολογιστικά μοντέλα

Βάση είναι η RAM (Random Access Machine) όπου όλες οι παρακάτω λειτουργίες θεωρούνται πως εκτελούνται σε χρόνο ίσο με 1 ή κάποια σταθερά: είσοδος / έξοδος στοιχείου, πρόσβαση μνήμης, σύγκριση $(<, =, >)$, βασικές πράξεις (ίσως και $\sqrt{\cdot}, \ln, a^b, \mathrm{mod}, \mathrm{div}$). Κάθε στοιχείο καταλαμβάνει χώρο ίσο με 1 ή κάποια σταθερά. Επεκτεινόμαστε στην random RAM εάν προβλέπεται και παραγωγή τυχαίων τιμών.

Μας ενδιαφέρει η real RAM (ή arithmetic RAM) όπου κάθε στοιχείο $\in \mathbb{R}$ αναπαρίσταται με απεριόριστη ακρίβεια. Όμως αυτό είναι μη ρεαλιστικό!

Παράδειγμα 2.2.1 2 προσθέσεις $a+b, g+d$ ακεραίων $< 2^n$ ανάγονται σε μία: $(a*2^{n+1}+b)+(g*2^{n+1}+d)$. Ομοίως 2 πολλαπλ. ac, bd ανάγονται σε έναν: $(a*2^{n+1}+b)*(c*2^{n+1}+d) = ac^{4n+2}+(ad+bc)2^{n+1}+bd$. □

Για μια ακριβέστερη μελέτη πολυπλοκότητας, χρησιμοποιούμε την Boolean (δυαδική) RAM όπου σε κάθε $x \in \mathbb{R}$ αντιστοιχείται το μέγεθος/μήκος του x: είτε σε δυαδικά ψηφία bits (δυφία) στην δυαδική αναπαράσταση δηλ. $\lceil \log_2 x \rceil$ (logarithmic cost function) ψηφία, είτε σε λέξεις (words) σε μια ορισμένη αναπαράσταση.
Π.χ: $21 = 10101_2 \Rightarrow$ μέγεθος$(21) = 5$ bits < 1 bit $=$ μέγεθοσ(1).

Για $x \in \mathbb{R}$ το μέγεθος εξαρτάται από την ακρίβεια (precision) και την απόλυτη τιμή $|x|$. Για $x \in \mathbb{Z}$ (αντίστοιχα $\mathbb{Q}$) εξαρτάται από την απόλυτη τιμή $|x|$ (αριθμητή/παρονομαστή).

Θυμίζουμε σύντομα τους συμβολισμούς στην ανάλυση της ασυμπτωτικής συμπεριφοράς των αλγορίθμων.

$f(n) = O(F(n)) \Leftrightarrow \exists N, \exists c : \forall n \geq N : f(n) \leq cF(n)$. Π.χ.: $67 \ln n = O(\log_2 n), 562n^{34} = O(2^n), O(a+b) = O(\max\{a,b\})$.

$f(n) = o(F(n)) \Leftrightarrow \lim_{n\to\infty}(f(n)/F(n)) = 0 \Leftrightarrow \forall \epsilon \exists N, \forall n > N, f(n) < \epsilon F(n)$. Άρα θέτοντας $\epsilon = c$ βρίσκουμε $f(n) = O(F(n))$. Το αντίστροφο δεν ισχύει, δες π.χ. $13n^3 \lg n + 37n^{3.1} = O(n^{3.1})$.

$f(n) = \Omega(F(n)) \Leftrightarrow F(n) = O(f(n))$, $f(n) = \Theta(F(n)) \Leftrightarrow$ [$f(n) = O(F(n))$ & $f(n) = \Omega(F(n))$], $f(n) = O^*(F(n)) \Leftrightarrow$ [$\exists\, c : f(n) = O((\log F(n))^c F(n))$].

Χρησιμοποιούμε $O_A(\cdot)$ και $O_B(\cdot)$ που συμβολίζουν αντίστοιχα την αριθμητική και δυαδική πολυπλοκότητα.

2.3 Αναπαράσταση

Ξεκινάμε με την αναπαράσταση αριθμών. Ακέραιοι ($\mathbb{Z}$) απεριόριστης ακρίβειας (ομοίως οι ρητοί $\mathbb{Q}$): πολλαπλές λέξεις μνήμης σε λίστα (list) ή πίνακα (array): $2^{10} =$ [00000100][00000000].

Οι πραγματικοί αριθμοί $\mathbb{R}$ αναπαριστώνται / προσεγγίζονται ως αριθμοί κινητής υποδιαστολής (floating point), άρα όχι πάντα επακριβώς, ως εξής: $\pm m\, c^p$: εκθέτης $p \in [Pmin, Pmax)$, mantissa $m \in [0, 2^M)$. IEEE double: 64 bits = 1 (πρόσημο) + 53 (=M) + 10 (εκθέτης).

Συνεχίζουμε με την αναπαράσταση πινάκων. Πυκνή: 2-διάστατος πίνακας (array) M όπου $M[i,j] =$ στοιχείο σειράς i και στήλης j, ανήκει σε $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ή είναι πολυώνυμο. Συνήθως κατά γραμμές (row-major) δηλ. διάνυσμα σειρών με στοιχεία τις διευθύνσεις (pointers) των διανυσμάτων των στοιχείων. Π.χ. πρόσθεση πινάκων $n \times m$ απαιτεί nm προσθέσεις.

Αραιή: Διάνυσμα σειρών με στοιχεία διευθύνσεις (pointers) προς τις λίστες των μη μηδενικών στοιχείων, όπου κάθε στοιχείο ακολουθείται από τον αριθμό / δείκτη της στήλης. Π.χ. πρόσθεση πινάκων με a, b στοιχεία αντίστοιχα κοστίζει $O(n + a + b)$.

$$\begin{bmatrix} 7 & 0 & 5 & 0 \\ 0 & 7 & 0 & 5 \\ 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} \bullet \\ \circ \\ \bullet \\ \bullet \end{bmatrix} \rightarrow \begin{bmatrix} 7 \\ 1 \\ \circ \end{bmatrix} \rightarrow \begin{bmatrix} 5 \\ 3 \\ \otimes \end{bmatrix}$$

Τελειώνουμε με την αναπαράσταση πολυωνύμων. Με μία μεταβλητή $\mathbb{Z}[x]$ ή $\mathbb{C}[x]$: πυκνή ως πίνακας (array) των συντελεστών ή αραιή ως λίστα των μη μηδενικών όρων. Π.χ.: Το $-15x^4+3x^2-9$ αναπαρίσταται ως: (πυκνή) $[-15, 0, 3, 0, -9]$ και με βαθμό $= 4$, (αραιή) $[-15, 4] \rightarrow [3, 2] \rightarrow [-9, 0]$. Παρατήρησε επίσης το $x^{2000} - 1$.

Πολλές μεταβλητές $\mathbb{Z}[x_1, \ldots, x_n]$: Βασική επιλογή η ταξινόμηση των όρων βάσει του διανύσματος του εκθέτη δηλ. οι συντελεστές αγνοούνται. Εξετάζουμε ως παράδειγμα για τις 2 δυνατές ταξινομήσεις το πολυώνυμο $(x + y)^2 + x + y + 1$.

Επαγωγική: συνήθως αραιή. Θεωρούμε το πολυώνυμο ως προς μία μεταβλητή με συντελεστές πολυώνυμα στις υπόλοιπες μεταβλητές. Αυτοί οι συντελεστές με τη σειρά τους αποθηκεύονται επαγωγικά. Κάθε στοιχείο (record) περιέχει τον αριθμητικό συντελεστή, τον εκθέτη ως προς την τρέχουσα μεταβλητή κι ένα δείκτη (pointer) στον συντελεστή που είναι ο ίδιος ένα άλλο πολυώνυμο. Π.χ. με $x > y$, το παραπάνω πολυώνυμο γράφεται $x^2 + x(2y + 1) + (y^2 + y + 1)$ και φυλάσσεται ως:

$$\begin{bmatrix} 1 \\ 2 \\ \otimes\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 1 \\ \delta_3\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ \delta_7\ \otimes \end{bmatrix} \qquad \delta_3 \rightarrow \begin{bmatrix} 2 \\ 1 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ \otimes \end{bmatrix} \qquad \delta_7 \rightarrow \begin{bmatrix} 1 \\ 2 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 1 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ \otimes \end{bmatrix}$$

Κατανεμημένη: μία λίστα (άρα αραιή αναπαράσταση) όρων διατεταγμένων ανάλογα με τη διάταξη των διανυσμάτων του κάθε εκθέτη.

Λεξικογραφική διάταξη (όπως ο τηλεφωνικός κατάλογος). Έστω $x_1 > x_2 > \cdots > x_n$ τότε για κάθε 2 διανύσματα, $(a_1, a_2, \ldots a_n) > (b_1, b_2, \ldots, b_n)$ αν και μόνο αν $a_k > b_k$ και $a_i = b_i$ για κάθε $i < k$. Π.χ. με $x > y : x^2 + 2xy + x + y^2 + y + 1$. Κάθε όρος δίνεται από το διάνυσμα εκθέτη και τον αριθμητικό συντελεστή:

$$\begin{bmatrix} 2 \\ 0 \\ 1 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 1 \\ 2 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \\ 1 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 2 \\ 1 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \\ 1 \\ \delta \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \\ \otimes \end{bmatrix}$$

Διάταξη συνολικού βαθμού κι έπειτα λεξικογραφική: $x^2 + 2xy + y^2 + x + y + 1$.

Κεφάλαιο 3

Αποτελεσματική ακριβής αριθμητική

3.1 Βασικές πράξεις ακεραίων

Ξεκινάμε με ακέραιους μήκους n δυαδικών ψηφίων, ή δυφίων, βλ. [AHU74, Akr89, vzGG99].

Η πρόσθεση και η αφαίρεση ακεραίων με $\leq n$ ψηφία καταλήγει σε ένα αποτέλεσμα με $\leq n+1$ ψηφία, ενώ απαιτεί $\leq n+1$ στοιχειώδεις δυαδικές πράξεις, άρα έχει κόστος $\Theta_B(n)$.

Η πράξη του πολλαπλασιασμού δύο ακεραίων, καθένας με $\leq n$ ψηφία, έχει ως αποτέλεσμα έναν ακέραιο με $\leq 2n$ ψηφία. Ο Σχολικός αλγόριθμος έχει δυαδική πολυπλοκότητα $O_B(n^2)$. Υπάρχει αλγόριθμος Διαίρει και Βασίλευε [KO63] που αποδίδεται στον Karatsuba:

Θεώρημα 3.1.1 (Karatsuba-Ofman) *Ο αλγόριθμος Διαίρει και Βασίλευε (Divide and Conquer) για Πολλαπλασιασμό ακεραίων μήκους n έχει δυαδική πολυπλοκότητα $O_B(n^{\lg 3}) = O_B(n^{1.585\ldots})$.*

Απόδειξη. «Διαιρούμε» τους δεδομένους ακεραίους σε: $a = a_0 + 2^{n/2}a_1, b = b_0 + 2^{n/2}b_1$. Τότε,

$$ab = a_0b_0 + 2^{n/2}(a_0b_1 + b_0a_1) + 2^n a_1b_1,$$

όπου $(a_0b_1 + b_0a_1) = (a_0 + a_1)(b_0 + b_1) - a_0b_0 - a_1b_1$. Έστω $M(n)$ το κόστος του πολλαπλασιασμού και $A(n)$ αυτό της πρόσθεσης. $M(n) = 3M(n/2) + 4A(n/2) + 2A(n) = 3M(n/2) + O(n) = O(n^{\lg 3})$. ΟΕΔ

Θεώρημα 3.1.2 *Βάσει του Ταχέως Μετασχηματισμού Fourier, ο Πολλαπλασιασμός ακεραίων μήκους n έχει δυαδική πολυπλοκότητα $O_B(n \log n \log\log n)$.*

Απόδειξη. Δες πολλαπλασιασμό πολυωνύμων και τον αλγόριθμο FFT, ενότητα 3.5. ΟΕΔ

Διαίρεση (με υπόλοιπο): Δεδομένων των ακεραίων a, b με μεγέθη $2n$ και n δυαδικών ψηφίων αντίστοιχα, υπολογίστε ακέραιους q (πηλίκο) και r (υπόλοιπο) με μεγέθη $\leq n+1$ και $\leq n$ αντίστοιχα, τέτοιους ώστε

$$a = bq + r \qquad \text{όπου} \qquad 0 \leq r < |b|.$$

Γράφουμε $q = a \text{ quo } b, r = a \bmod b$. Ο σχολικός αλγόριθμος για διαίρεση με υπόλοιπο κοστίζει $O_B(n^2)$ εάν οι δεδομένοι ακέραιοι έχουν μήκος n δυφία.

Η πράξη mod (modulus) απεικονίζει έναν ακέραιο a στον πεπερασμένο δακτύλιο $\mathbb{Z}_b = \{0, 1, 2, \ldots, b-1\}$ που ορίζεται από τον (θετικό) ακέραιο b. Αν b πρώτος τότε $\mathbb{Z}_b$ πέρα από δακτύλιος ($+$ με αντίστροφο, $\times$ επιμερισμένος ως προς $+$) είναι και σώμα ($+, \times$ με αντίστροφο).
Π.χ. $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}, 1+4 = 5 \equiv 0 \pmod 5, 2+3 = 5 \equiv 0, 1 \times 1 = 1, 2 \times 3 = 6 \equiv 1, 4 \times 4 = 16 \equiv 1.$

Έστω $D(n)$ η πολυπλοκότητα της διαίρεσης (με υπόλοιπο). $R(n) = O(D(n))$. $D(n) = O(M(n) + R(n)) \Leftarrow a/b = a(1/b)$.

Έστω $R(n)$ η πολυπλοκότητα για αντίστροφο (ο πλήρης ορισμός έπεται), $S(n)$ για τετραγωνισμό ακέραιου n ψηφίων. $S(n) = \Theta(M(n)) \Leftarrow ab = \frac{1}{2}((a+b)^2 - a^2 - b^2)$. $S(n) = O(R(n)) \Leftarrow a^2 = \frac{1}{\frac{1}{a} - \frac{1}{a+1}} - a$.
Άρα, γράφουμε απλά $M = \Theta(S) = O(R) = O(D),\ D = O(M + R) = O(R)$ επομένως $M = \Theta(S) = O(R),\ R = \Theta(D)$. Θα αποδείξουμε παρακάτω πως $R = O(M)$, καταλήγοντας έτσι στο εξής θεώρημα:

Θεώρημα 3.1.3 *Οι δυαδικές πολυπλοκότητες πολλαπλασιασμού, διαίρεσης με υπόλοιπο, αντίστροφου και τετραγωνισμού $M(n), D(n), R(n), S(n)$ συνδέονται ασυμπτωτικά με σταθερές.*

Απομένει να μελετήσουμε τον υπολογισμό του αντιστρόφου ώστε να δείξουμε $R = O(M)$. Ο αντίστροφος του a ορίζεται κατά σύμβαση (ώστε να είναι ακέραιος) ως τα n σημαντικότερα δυαδικά ψηφία στον ρητό $2^{2n-1}/a$, μετατοπισμένα δεξιά κατά $2n$ δυφία. Εάν $a = 2^{n-1}$, χρησιμοποιούμε τα $n+1$ σημαντικότερα ψηφία. Εδώ υποθέτουμε πως η μετάθεση κατά $2n-1$ ψηφία γίνεται χωρίς επιπλέον κόστος. Άρα αρκεί να υπολογιστεί το ακέραιο μέρος του $2^{2n-1}/a$, στην γενική περίπτωση.
Π.χ. $a = [11], 1/a = [0, 0101\ldots], 2^3/a = [10, 1\ldots]$ άρα αρκεί να υπολογίσω τον ακέραιο [10]. $a = [100], 1/a = [0, 01], 2^5/a = [1000]$.

Απόδειξη. Ο Αλγόριθμος αντιστρόφου υπολογίζει ακολουθία προσεγγίσεων $t_i \to t =$ προσέγγιση του $1/a$, όπου $t = t_i + (1/a)(1 - t_i a)$ και προσεγγιστικά

$$t_{i+1} = t_i + t_i(1 - t_i a) = 2t_i - t_i^2 a.$$

Η ιδέα είναι πως αυτή η προσέγγιση υπολογίζεται επαναληπτικά με πολλαπλασιασμούς, εφαρμόζοντας την επανάληψη του Νεύτωνα, όπως και για τον αντίστροφο πολυωνύμου μιας μεταβλητής (ενότητα 3.2). Ποια είναι η σύγκλιση;

$$t_i a = 1 - s \Rightarrow t_{i+1} a = 2t_i a - t_i^2 a^2 = 2(1-s) - (1-s)^2 = 1 - s^2.$$

Αν $s \leq 1/2$, το πλήθος των σωστών δυαδικών ψηφίων διπλασιάζεται σε κάθε επανάληψη. Δηλ. έχοντας υπολογίσει το $t_i \bmod 2^{2^i}$, ο αλγόριθμος υπολογίζει το $t_{i+1} \bmod 2^{2^{i+1}}$. Αυτή είναι ουσιαστικά μια αλγεβρική θεώρηση της Νευτώνειας επανάληψης (η οποία κάποτε αναφέρεται και ως ανύψωση (lifting) Hensel). Άρα

$$R(n) \leq R(n/2) + M(n/2) + M(n) + cn.$$

Επομένως $R(n/2) \leq R(n/4) + M(n/4) + M(n/2) + cn/2$ και γενικά $R(n/2^{k-1}) \leq R(n/2^k) + M(n/2^k) + M(n/2^{k-1}) + cn/2^{k-1}$. Για $k = \lg n \Rightarrow R(n) \leq O(1) + M(n) + 2M(n/2) + \cdots + 2M(2) + cn(1 + 1/2 + \cdots + 1/2^{k-1}) \leq O(1) + O(M(n))(1 + 1/2 + \cdots + 1/2^{k-1}) + O(n) \leq O(M(n))$.

Εναλλακτικά, ο Αλγόριθμος [AHU74, sec.8.1] αναφέρεται στον $2^{2n-1}/a$ και καταλήγει στην ίδια ανάλυση. ΟΕΔ

Π.χ. $a = [11]$, έστω $t_0 = [0, 01]$ τότε $t_1 = [0, 0101], t_2 = [0, 01010101]$ κοκ. Παρόμοια προσεγγίζουμε: $2^3/a$ με $t_0 = [10, 1], t_1 = [10, 10101]$ κοκ.

3.2 Βασικές πράξεις μεταξύ πολυωνύμων μίας μεταβλητής

Βιβλιογραφία: [AHU74, sel.278-289]. Έστω πολυώνυμα $p_1(x), p_2(x)$ μίας μεταβλητής x με ακέραιους συντελεστές (ή πραγματικούς στη real RAM). Ο (μέγιστος) βαθμός τους (degree) συμβολίζεται με d_1, d_2, αντίστοιχα, και ο αριθμός των όρων τους με t_1, t_2. Έστω $d = \max\{d_1, d_2\}$.

Το **άθροισμα** έχει βαθμό $\leq d$ και $\leq t_1 + t_2$ όρους. Υπολογίζεται με αριθμητική πολυπλοκότητα $\Theta_A(d)$.

Το **γινόμενο** έχει βαθμό $d_1 + d_2$ και $\leq t_1 t_2$ όρους. Αλγόριθμοι και αριθμητικές πολυπλοκότητες αντίστοιχοι με αυτούς για πολλαπλασιασμό ακεραίων:

$$O_A(d_1 d_2), O_A(d^{\lg 3}), O_A(d \log^2 d), O_A(d \log d),$$

χρησιμοποιώντας, αντίστοιχα, τον σχολικό αλγόριθμο, Διαίρει και βασίλευε, γενική αποτίμηση και παρεμβολή ή, τέλος, αποτίμηση και παρεμβολή με FFT. Η πολυπλοκότητα βάσει του FFT είναι πιο μικρή από ό,τι στους ακεραίους, διότι δεν υπάρχει το πρόβλημα του κρατούμενου (carry). Ανάλογα, σε αραιή αναπαράσταση οι πολυπλοκότητες είναι $O_A(t_1 t_2)$ και $O_A(t^{\lg 3})$.

Αντιστοιχία προβλημάτων και μεθόδων μεταξύ ακεραίων και πολυωνύμων: Κάθε δυαδικός ακέραιος $[c_{n-1}\ c_{n-2}\ \ldots\ c_0]$ αντιστοιχεί σε ένα και μοναδικό «δυαδικό» πολυώνυμο $c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0$.

Άσκηση 3.2.1 Αποδείξτε πως η πολυπλοκότητα πολλαπλασιασμού με τον αλγόριθμο Διαίρει και βασίλευε είναι $O_A(d^{\lg 3})$.

Η **διαίρεση με υπόλοιπο** ορίζεται από $p_1(x) = p_2(x)q(x) + r(x) : \deg(r(x)) < \deg(p_2(x))$. Το πηλίκο $q(x) = p_1(x) \operatorname{quo} p_2(x)$ έχει βαθμό $d_1 - d_2$ και $\leq t_1 - t_2 + 1$. Τα q, r είναι μοναδικά εφόσον οι συντελεστές των πολυωνύμων είτε βρίσκονται σε σώμα, είτε βρίσκονται σε αντιμεταθετικό δακτύλιο που περιέχει μονάδα και το p_2 είναι μονικό (monic) δηλ. Μοναδιαίου Μεγιστοβάθμιου Συντελεστή.

Το **αντίστροφο** ορίζεται κατά σύμβαση ως $x^{2n} \operatorname{quo} p(x)$, όπου το quo εκφράζει τον υπολογισμό του πηλίκου πολυωνύμων. Υποθέτουμε πως το p_2 είναι μονικό, δηλ. $p_2(0) = 1$. Έστω $A(f)$ το Ανάστροφο πολυώνυμο ενός πολυωνύμου $f(x)$ βαθμού k, όπου $A(f) := x^k f(1/x)$. Εξ ορισμού, $A(p_1) = A(q)A(p_2) + x^{d_1-d_2+1}A(r) \equiv A(q)A(p_2) \bmod x^{d_1-d_2+1} \Rightarrow A(q) \equiv A(p_1)A(p_2)^{-1}$. Θα δείξουμε κατασκευαστικά πως το $A(p_2)^{-1} \bmod x^{d_1-d_2+1}$ υπάρχει και είναι καλώς ορισμένο, οπότε αρκεί να το υπολογίσουμε.

Το γενικό πρόβλημα είναι ο υπολογισμός $g \in D[x] : \ fg \equiv 1 \bmod x^k$ όπου $f \in D[x],\ f(0) = 1$. Ο επαναληπτικός αλγόριθμος του Νεύτωνα ανάγει το πρόβλημα σε πολλαπλασιασμούς και προσθαφαιρέσεις, όπως και στην περίπτωση του υπολογισμού του αντιστρόφου ακεραίου στο $\mathbb{Z}$ (θεώρημα 3.1.3): Επιλύει την εξίσωση $\phi(g) = 1/g - f \Rightarrow \phi' = -1/g^2$. Η επανάληψη χρησιμοποιεί την εξίσωση της εφαπτομένης $\phi'(g_i) = (y - \phi(g_i))/(x - g_i)$ στο g_i για να υπολογίσει τη νέα τιμή της μεταβλητής q ως εξής:

$$g_{i+1} = g_i - \phi(g_i)/\phi'(g_i) = 2g_i - fg_i^2, \quad i \geq 0.$$

Λήμμα 3.2.2 *Με τους παραπάνω συμβολισμούς, εάν η αρχική προσέγγιση είναι $g_0 = 1$ και υπολογίζω το g_{i+1} ως $2g_i - fg_i^2 \bmod x^{2^{i+1}}$, τότε $fg_i \equiv 1 \bmod x^{2^i}$.*

Απόδειξη. Η επαγωγική βάση $fg_0 \equiv 1 \bmod x$ ισχύει εξ υποθέσεως. Το βήμα είναι $1 - fg_{i+1} \equiv 1 - f(2g_i - fg_i^2) \bmod x^{2^{i+1}}$. Το δεύτερο μέλος γράφεται $(1 - fg_i)^2 \equiv 0 \bmod x^{2^{i+1}}$ διότι $1 - fg_i \equiv 0 \bmod x^{2^i}$ από την επαγωγική υπόθεση. ΟΕΔ

Θεώρημα 3.2.3 *Οι αριθμητικές πολυπλοκότητες πολλαπλασιασμού, τετραγωνισμού, διαίρεσης με υπόλοιπο και αντίστροφου συνδέονται με σταθερές.*

Εξετάζουμε τώρα τον **υπολογισμό μιας τιμής** δεδομένου πολυωνύμου, βλ. [BP94], [EP99, pp.1-15].

Υπολογισμός μίας τιμής με τον κανόνα του Horner [Νεύτων]: $p(a) = (\cdots(c_n a + c_{n-1})a + \cdots) + c_0$: n προσθέσεις, n πολλαπλασιασμούς: βέλτιστη.

Ισοδύναμα $p(a) = r(x) = p(x) \bmod (x-a)$ διότι $p(x) = q(x)(x-a) + r(x), \deg(r(x)) = 0$ δηλ. $r(x) = r(a)$. Άρα η διαίρεση με υπόλοιπο, όταν ο διαιρέτης είναι γραμμικός, κοστίζει $O(n)$.

Πρόβλημα 3.2.4 *Με δεδομένα k σημεία $x_0, \ldots, x_{k-1}$ και τους συντελεστές του πολυωνύμου $p(x)$, βαθμού n, υπολόγισε k τιμές $p(x_0), \ldots, p(x_{k-1})$.*

Απλές λύσεις: Ο Horner δίνει $O_A(kn)$. Πολλαπλασιασμός πίνακα με διάνυσμα δίνει επίσης $O_A(kn)$, αλλά η παρακάτω πρόταση βελτιώνει αυτή την πολυπλοκότητα. Με την πρόταση αυτή ουσιαστικά μπορούμε να εκμεταλλευτούμε την ειδική δομή του παρακάτω πίνακα. Πρόκειται για τη δομή Vandermonde.

Παράδειγμα 3.2.5 Ο υπολογισμός της τιμής του $p(x)$ στα σημεία x_0, x_1, x_2 γράφεται με χρήση πινάκων ως εξής:

$$p(x) = c_2x^2 + c_1x + c_0 \Rightarrow \begin{bmatrix} 1 & x_0 & x_0^2 \\ 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} p(x_0) \\ p(x_1) \\ p(x_2) \end{bmatrix}$$

□

Πρόταση 3.2.6 *Υπάρχει αλγόριθμος για το πρόβλημα 3.2.4, τύπου Διαίρει και βασίλευε, με συνολική πολυπλοκότητα $O_A(n \lg^2 n)$, για $k = \Theta(n)$.*

Απόδειξη. Γενική Ιδιότητα: Για $a, b, c \geq 0, (a \bmod (bc)) \bmod b = a \bmod b$.
Απόδειξη: $a \bmod bc = k \Rightarrow a = jbc + k, a \bmod b = m \Rightarrow a = ib + m$. Άρα $k = ib + m - jbc \Rightarrow k \bmod b = m$.

Χρησιμοποιούμε την παρακάτω ταυτότητα, και γενικεύσεις της ταυτότητας αυτής, η οποία είναι συνέπεια της παραπάνω ιδιότητας:

$$p(x) \bmod (x - x_i) = [p(x) \bmod \prod_{j \in J}(x - x_j)] \bmod (x - x_i), \qquad i \in J \subset \mathbb{N}.$$

Θα δούμε πώς μπορούμε να υπολογίσουμε όλα τα γινόμενα $\prod_j (x - x_j)$ γρήγορα με τη μέθοδο fan-in στο στάδιο της σύνθεσης. Για ευκολία στους υπολογισμούς υποθέτουμε $n = k$.

Στάδιο σύνθεσης (fan-in): Ο υπολογισμός όλων των $\prod_j (x - x_j)$ που χρειαζόμαστε στο στάδιο υποδιαίρεσης ξεκινά με τα $x - x_j$ για $i = 0, \ldots, n-1$ και πρώτα υπολογίζουμε $n/2$ γινόμενα δευτέρου βαθμού $(x - x_{2i})(x - x_{2i+1})$ για $i = 0, 1, \ldots, n/2 - 1$. Έπειτα $n/4$ γινόμενα 4ου βαθμού $(x - x_{4i})(x - x_{4i+1})(x - x_{4i+2})(x - x_{4i+3})$ για $i = 0, 1, \ldots, n/4 - 1$, κοκ. Ουσιαστικά κατασκευάζουμε δυαδικό δένδρο με φύλλα τα $x - x_j$, κόμβους τα διάφορα πολυώνυμα, και ρίζα το $\prod_{0 \leq i < n} x - x_j$. Το κόστος για τον υπολογισμό των $n/2^j$ πολυωνύμων βαθμού 2^j είναι

$$O_A((n/2^j)M(2^{j-1})) = O_A(nj), \quad j = 1, \ldots, \lg n,$$

όπου $M(t) = O(t \log t)$ εκφράζει το κόστος πολλαπλασιασμού πολυωνύμων βαθμού t μέσω FFT. Συνολική πολυπλοκότητα $= O(n(1 + 2 + \cdots + \lg n)) = O(n \lg^2 n)$. Παρακάτω φαίνεται σχηματικά το δένδρο υπολογισμού, όπου $k = \lg n - j$.

$$q = p \bmod \prod_{i=0}^{n-1}(x - x_i)$$

$$p \bmod \prod_{i=0}^{n/2-1}(x - x_i) \qquad\qquad p \bmod \prod_{i=n/2}^{n-1}(x - x_i)$$

$$\text{επίπεδο } k,\ \text{κόμβος } m \in [0, 2^k): \quad \cdots \quad p \bmod \prod_{i=mn/2^k}^{(m+1)n/2^k-1} \quad \cdots$$

$$p \bmod (x - x_0) \quad p \bmod (x - x_1) \qquad \ldots \qquad p \bmod (x - x_{n-2}) \quad p \bmod (x - x_{n-1}$$

Στάδιο Υποδιαίρεσης (fan-out): Ο υπολογισμός του $q(x) = p(x) \bmod \prod_{i=0}^{n-1}(x - x_i)$ οδηγεί στον υπολογισμό του πολυωνύμου $p(x) \bmod \prod_{i=0}^{n/2-1}(x - x_i)$ ως $q(x) \bmod \prod_{i=0}^{n/2-1}(x - x_i)$ και $p(x) \bmod \prod_{i=n/2}^{n-1}(x - x_i) = q(x) \bmod \prod_{i=n/2}^{n-1}(x - x_i)$. Άρα το κόστος είναι της διαίρεσης με υπόλοιπο (mod) του p και δύο φορές του $q(x)$, δηλ. συνολικά $O(n \log n)$, μέσω FFT. Έτσι έχουμε δύο πολυώνυμα βαθμού $n/2 - 1$. Στο επόμενο στάδιο γίνονται 4 πράξεις mod με τέτοια πολυώνυμα, άρα συνολικού κόστους $4(n-2)/2 \cdot O(\log n)$.

Στο στάδιο k, υπολογίζουμε 2^k πολυώνυμα ως υπόλοιπα διαίρεσης με διαιρέτη το γινόμενο των $(x - x_i)$, με $i = mn/2^k, \ldots, (m+1)n/2^k - 1$, όπου $m = 0, \ldots, 2^k - 1$, όπως στο παραπάνω σχήμα. Άρα ο διαιρέτης είναι βαθμού $n/2^k$ και το υπόλοιπο της διαίρεσης είναι βαθμού $n/2^k - 1$ όπου $k = 0, 1, \ldots, \lg n$. Επομένως το συνολικό κόστος ανά επίπεδο στο δένδρο είναι $2^k n/2^k \cdot O(\lg n)$.

Συνολικά κατασκευάζουμε ένα δυαδικό δένδρο με κόμβους που αντιστοιχούν στα πολυώνυμα $q(x), \ldots$ (η ρίζα αντιστοιχεί στο $q(x)$) και φύλλα που αντιστοιχούν στον υπολογισμό μίας τιμής πολυωνύμου βαθμού=1. Πολυπλοκότητα θεωρώντας πως τα πολυώνυμα-διαιρέτες έχουν υπολογιστεί εκ των προτέρων: $T(n) = 2T(n/2) + 2O(n \lg n) = 2nO(\lg n) + 4(n/2)O(\lg n) + \cdots + 2^k(n/2^{k-1})O(\lg n) < 2nkO(\lg n)$ άρα συνολικά, για $k = \lg n, T(n) = O(n \lg^2 n)$. ΟΕΔ

Αν δεν χρησιμοποιήσουμε FFT για τον πολλαπλασιασμό πολυωνύμων, αλλά έναν αλγόριθμο με πολυπλοκότητα M, τότε η πολυπλοκότητα του fan-in, αλλά και του fan-out, είναι $O_A(M \log n)$.

Το πρόβλημα αποτίμησης επεκτείνεται και στην αποτίμηση των παραγώγων πολυωνύμου. Μια σχετική πρόταση που θα χρειαστούμε παρακάτω είναι η εξής.

Πρόταση 3.2.7 Linnainmaa [76], Baur-Strassen [TCS'83], βλ. [BP94, thm.2.1.3]. *Στο μοντέλο των Straight-Line Programs, η πολυπλοκότητα του υπολογισμού της τιμής μιας ρητής συνάρτησης πολλών μεταβλητών $x_1, \ldots, x_k$ σε ένα σημείο, φράσσει ασυμπτωτικά το κόστος υπολογισμού της τιμής στο σημείο αυτό, όλων των παραγώγων πρώτης τάξης (ως προς $x_1, \ldots, x_k$) της συνάρτησης.*

3.2.1 Παρεμβολή

Πρόβλημα 3.2.8 *Παρεμβολή (interpolation) είναι το πρόβλημα του υπολογισμού των $n+1$ συντελεστών του πολυωνύμου $p(x)$ από $n+1$ τιμές $r_i = p(x_i), i = 0, \ldots, n$ για δεδομένα διαφορετικά σημεία x_i, δηλ. το αντίστροφο του προβλήματος υπολογισμού τιμών, όπου θεωρείται γνωστός ο βαθμός του πολυωνύμου $= n$.*

Βιβλιογραφία: [EP99, pp.1-15] Στην γλώσσα των πινάκων, επίλυση ενός γραμμικού συστήματος Vandermonde, με δεδομένο το διάνυσμα γινομένου $[p(x_0), \ldots, p(x_n)]$.

Πρόταση 3.2.9 *Υπάρχει αλγόριθμος με πολυπλοκότητα $O_A(n \lg^2 n)$ για το πρόβλημα 3.2.8.*

Ο τύπος του Lagrange: Έστω $L(x) = \prod_{i=0,\dots,n}(x - x_i), L'(x)$ η παράγωγος ως προς x είναι $'L(x) = \sum_{i=0}^{n} \prod_{j \neq i}(x - x_j)$. Άρα, για κάθε x_k ισχύει $L'(x_k) = \prod_{j \neq k}(x_k - x_j)$. Επίσης, ορίζουμε

$$L_i(x) = \prod_{j=0,\dots,n, j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Από τα x_i, r_i υπολογίζουμε το πολυώνυμο

$$p(x) = L(x) \sum_{i=0}^{n} \frac{r_i}{L'(x_i)(x - x_i)} = \sum_{i=0}^{n} \frac{r_i}{L_i'(x_i)} \prod_{j \neq i}(x - x_j) = \sum_{i=0}^{n} r_i L_i(x).$$

Η κατασκευή αυτή δηλώνει πως το $p(x)$ ικανοποιεί τα δεδομένα $p(x_i) = r_i$. Επιπλέον, είναι το μοναδικό πολυώνυμο βαθμού n με αυτή την ιδιότητα: Αν υπάρχει δεύτερο τέτοιο πολυώνυμο τότε η διαφορά τους έχει βαθμό $\leq n$ και $n + 1$ ρίζες, άρα πρόκειται για το μηδενικό πολυώνυμο. Η παραπάνω συζήτηση αποδεικνύει το εξής:

Λήμμα 3.2.10 *Το $p(x)$ είναι το μοναδικό πολυώνυμο βαθμού n, το οποίο ικανοποιεί $p(x_i) = r_i, i = 0, \dots, n$, άρα είναι το ζητούμενο πολυώνυμο στο πρόβλημα 3.2.8.*

Απόδειξη. Απομένει να δείξουμε πως ο παραπάνω υπολογισμός γίνεται με πολυπλοκότητα $O_A(n \lg^2 n)$. Υπολογίζουμε το $L(x)$ όπως στο στάδιο συνδυασμού (fan-in) παραπάνω, έπειτα το $L'(x)$ και τέλος τις τιμές $L'(x_i)$ για $i = 0, \dots, n$ σε $O_A(n \lg^2 n)$ σύμφωνα με την παραπάνω πολυπλοκότητα.

Έπειτα, υπολογίζουμε το άθροισμα των ρητών εκφράσεων στον αρχικό τύπο για το $p(x)$ όπως στο στάδιο συνδυασμού (fan-in). Για $k = 1$, δηλ. στα φύλλα του δένδρου, ξεκινώ με τη ρητή έκφραση

$$\frac{r_0(x - x_1)/L'(x_0) + r_1(x - x_0)/L'(x_1)}{(x - x_1)(x - x_0)}.$$

Στο επίπεδο k υπάρχουν $n/2^k$ τέτοιες πράξεις για $k = 1, \dots, \lg n$. Κάθε άθροισμα ρητών εκφράσεων βαθμού 2^k απαιτεί 3 πολλαπλασιασμούς, μια πρόσθεση πολυωνύμων βαθμού το πολύ 2^{k-1}:

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}.$$

Άρα σε κάθε επίπεδο του δένδρου το συνολικό κόστος είναι $O(n/2^k)M(2^{k-1})$ και συνολικά ο υπολογισμός του αθροίσματος κοστίζει $O_A(n \lg^2 n)$.

Ο τελικός πολλαπλασιασμός με το $L(x)$ δεν είναι παρά η απλοποίηση με τον παρονομαστή του τελικού αθροίσματος που έχει υπολογιστεί στην ρίζα του δένδρου. Επομένως δεν εκτελείται διαίρεση, απλώς ο αλγόριθμος επιστρέφει τον αριθμητή. ΟΕΔ

Τα $L_j(x)$ αποτελούν μια βάση ως προς την οποία το $p(x)$ έχει συντελεστές τα r_j. Η μετάβαση από την συνήθη βάση δυνάμεων $(1, x, x^2, \dots)$ σε αυτή τη βάση εκφράζεται από έναν πίνακα Vandermonde. Η νέα αυτή βάση έχει ενδιαφέρουσες ιδιότητες αριθμητικής σταθερότητας σε γεωμετρικές και σχεδιαστικές εφαρμογές.

Παράδειγμα 3.2.11

$$p(x) = \det \begin{bmatrix} x+3 & 1 & 0 \\ 1 & x & 1 \\ 1 & x & 2 \end{bmatrix}$$

με τιμές $p(0) = -1, p(1) = 3, p(2) = 9$. $L(x) = x^3 - 3x^2 + 2x, L'(x) = 3x^2 - 6x + 2, L'(0) = 2, L'(1) = -1, L'(2) = 2$. $p(x) = L(x)[-1/(2x) + 3/(-x+1) + 9/(2x-4)] = x^2 + 3x - 1$. □

Παρακάτω (ενότητα 3.3) εξετάζεται ένα αντίστοιχο πρόβλημα «παρεμβολής» ακεραίων από τις προβολές τους σε πεπερασμένα σώματα (Κινέζικο υπόλοιπο). Οι μέθοδοι επίλυσης στα δύο προβλήματα είναι ουσιαστικά οι ίδιες. Συγκεκριμένα, η παρεμβολή Newton που παρουσιάζεται στην 3.3 μπορεί να χρησιμοποιηθεί και στην παρεμβολή πολυωνύμων μίας μεταβλητής.

3.3 Κινέζικο θεώρημα

Βιβλιογραφία: [DST88, pp.218-21], [AHU74, pp.289-300], [EP99, pp.1-15].

Η ενότητα παρέχει μια θεωρητική θεμελίωση της παρεμβολής όπως εξετάστηκε παραπάνω για πολυώνυμα στο $\mathbb{Q}[x]$ και όπως, ισοδύναμα, εφαρμόζεται και για ακεραίους. Θα δούμε πώς η παρεμβολή κατά Lagrange δίνει μια κατασκευαστική λύση στο Θεώρημα του Κινέζικου υπολοίπου (Chinese remainder theorem) και, εναλλακτικά, πώς η παρεμβολή κατά Newton δίνει μια άλλη, αυξητική λύση.

Κίνητρο / πρόβλημα: Έκρηξη ενδιάμεσων τιμών στον υπολογισμό ΜΚΔ ακεραίων, πολυωνύμων, ή στην επίλυση γραμμικών συστημάτων. Για παράδειγμα, αν οι συντελεστές γραμμικού συστήματος $n \times n$ έχουν μήκος L, οι ρίζες έχουν μήκος nL, αλλά υπάρχουν (αφελείς) αλγόριθμοι που χρησιμοποιούν αριθμούς μήκους $2^n L$. Γενικά, η προσέγγιση χρησιμοποιείται όπου είναι χρήσιμη η παρεμβολή πολυωνύμου από τις τιμές του ή, γενικότερα, από τις «προβολές» του. Θα δούμε την αντίστοιχη έννοια «προβολής» και στους ακεραίους, αλλά το θεώρημα γενικεύεται και σε δακτυλίους.

Θεώρημα 3.3.1 *(Κινέζικου υπολοίπου) Έστω ακέραιοι $p_i \geq 2$ και $m_i \in \mathbb{Z}_{p_i} = \{0, 1, \ldots, p_i - 1\}$ για $i = 1, \ldots, k$, όπου οι p_i είναι πρώτοι μεταξύ τους (relatively prime) ανά δύο δηλ. $i \neq j \Rightarrow ΜΚΔ(p_i, p_j) = 1$. Τότε υπάρχει μοναδικός ακέραιος $a \in \{0, 1, \ldots, \prod_{i=1}^{k} p_i - 1\}$ τέτοιος ώστε $a \bmod p_i = m_i$ για $i = 1, \ldots, k$.*

Απόδειξη. Η ύπαρξη του a αποδεικνύεται κατασκευαστικά παρακάτω μέσω της παρεμβολής κατά Lagrange ή Newton. Για τη μοναδικότητα, έστω $a' \neq a$ με τις ίδιες ιδιότητες. Ορίζουμε $d = a - a' \neq 0$ για το οποίο

$$d \equiv 0 \pmod{p_i}, \forall i \Rightarrow d \equiv 0 \pmod{\prod_{i=1}^{k} p_i},$$

που όμως είναι άτοπο από τον ορισμό του d. ΟΕΔ

Άρα κάθε θετικός ακέραιος ορίζεται πλήρως από τα υπόλοιπα της διαίρεσης με k πρώτους (μεταξύ τους) όταν το γινόμενο των πρώτων είναι μεγαλύτερο από τον ακέραιο. Ισοδύναμα, ένας ακέραιος με πρόσημο ορίζεται πλήρως από τους k πρώτους όταν βρίσκεται στο διάστημα $\{-\lfloor \frac{1}{2} \prod_{i=1}^{k} p_i \rfloor, \ldots, 0, \ldots, \lceil \frac{1}{2} \prod_{i=1}^{k} p_i \rceil - 1\}$.

Άρα, η αριθμητική στο $\mathbb{Z}$ εκτελείται με απόλυτη ακρίβεια χρησιμοποιώντας κυρίως ακέραιους πεπερασμένου μήκους (μικρότερους από τους p_i) και απεριόριστου μήκους μόνο για την αλγοριθμική εκτέλεση του Κινέζικου θεωρήματος, ως εξής:

1. Προβολή των δεδομένων σε επαρκή αριθμό πεπερασμένων σωμάτων.
2. Υπολογισμό της επιθυμούμενης ποσότητας σε κάθε πεπερασμένο σώμα (field).
3. Εφαρμογή του Κινέζικου θεωρήματος για τον υπολογισμό της ακέραιας ποσότητας.

Αντίστοιχο θεώρημα ισχύει στο $\mathbb{Q}[x]$ με τις εξής αντιστοιχίες: $p_i \to p_i(x)$ πρώτα μεταξύ τους ανά δύο δηλ. κάθε $p_i(x), p_j(x)$ έχουν μέγιστο κοινό διαιρέτη=1, $m_i \to m_i(x)$ πολυώνυμο βαθμού $<$ βαθμός $(p_i(x))$, $a \to a(x)$ πολυώνυμο βαθμού $<$ βαθμός $(\prod_{i=1}^{k} p_i(x))$.

Τελικά, η αριθμητική εκτελείται με απόλυτη ακρίβεια κατ'επέκταση και στο $\mathbb{Q}, \mathbb{Q}[x]$ και κάθε Ευκλείδεια περιοχή (βλ. ορισμό 4.1.3) χρησιμοποιώντας κυρίως στοιχεία μικρού «μεγέθους» όπως στο $\mathbb{Z}$ παραπάνω. Το θεώρημα μάλιστα γενικεύεται και σε αντιμεταθετικούς δακτυλίους με μονάδα.

Λήμμα 3.3.2 *Έστω $a, p \in \mathbb{N}$. Κάθε στοιχείο $a \in \mathbb{Z}_p$, τέτοιο ώστε $ΜΚΔ(a, p) = 1$, έχει αντίστροφο στον πεπερασμένο δακτύλιο $\mathbb{Z}_p$.*

Το λήμμα είναι τετριμμένο για κάθε πρώτο p, οπότε το $\mathbb{Z}_p$ είναι σώμα. Αλλιώς, δείτε την άσκηση 3.3.7.

Αλγόριθμος Lagrange: Στα πολυώνυμα, όταν τα $p_i(x)$ είναι γραμμικά, ο υπολογισμός των $m_i(x)$ και $a(x)$ είναι απλά υπολογισμός τιμών και εκτέλεση παρεμβολής αντίστοιχα, οπότε βρίσκουμε τον τύπο της ενότητας 3.2.1. Στους ακέραιους ο αντίστοιχος τύπος είναι:

$$a = \sum_{i=1}^{k} \left[\left(\frac{m_i}{\prod_{j \neq i} p_j} \bmod p_i \right) \prod_{j \neq i} p_j \right] \bmod \prod_{j=1}^{k} p_j.$$

Ο παρονομαστής αντιστρέφεται $\bmod p_i$ χάρη στο λήμμα 3.3.2. Έχοντας υπολογίσει εκ των προτέρων τις τιμές που είναι ανεξάρτητες του a και θεωρώντας τους p_i σταθερού μήκους, το κόστος είναι $O_B(k \log^2 k)$.

Αλγόριθμος Newton, στους ακέραιους: αυξητικός δηλ. σταδιακά βελτιώνει την προσέγγιση υπολογίζοντας ακέραιους που ικανοποιούν μια ακόμη σχέση $a \bmod p_i = m_i$. Έστω $a_i = a \bmod \prod_{j=1}^{i} p_j$ οπότε $a_0 = 0, a_1 = m_1, a = a_k$ και s_i τέτοια ώστε $s_i \prod_{j=1}^{i-1} p_j \bmod p_i \equiv 1$. Τα s_i είναι καλώς ορισμένα χάρη στο λήμμα 3.3.2.

$$a_i = a_{i-1} + [(m_i - a_{i-1}) s_i \bmod p_i] \prod_{j=1}^{i-1} p_j$$

Απόδειξη ορθότητας:
(1) $a_i \bmod p_i \equiv a_{i-1} + m_i - a_{i-1} \bmod p_i \equiv m_i$.
(2) $a_i \bmod \prod_{j=1}^{i-1} p_j = a_{i-1} \bmod \prod_{j=1}^{i-1} p_j$.
(3) Η παράσταση στην αγκύλη [.] είναι μικρότερη από $p_i \Rightarrow [.] \prod_{j=1}^{i-1} p_j \leq (p_i - 1) \prod_{j=1}^{i-1} p_j$. Επομένως

$$a_{i-1} < \prod_{j=1}^{i-1} p_j \Rightarrow a_i < \prod_{j=1}^{i-1} p_j + p_i \prod_{j=1}^{i-1} p_j - \prod_{j=1}^{i-1} p_j = \prod_{j=1}^{i} p_j.$$

Άρα η υπολογιζόμενη τιμή λύνει το πρόβλημα και λόγω του θεωρήματος είναι η μοναδική. Η μέθοδος Newton υπολογίζει σε κάθε στάδιο έναν αριθμό «ανεξάρτητο» από τους προηγούμενους, όπως δηλ. τα ψηφία σε μια δεκαδική (ή δυαδική) αναπαράσταση και έχει κόστος που φράσσεται από το εξής:

$$M(k) + M(k-1) + \cdots + M(1) \leq \log k \log\log k (k + \cdots + 1) = O_B(k^2 \log k \log\log k).$$

Παράδειγμα 3.3.3 Δίνονται $m_1 = a \bmod 5 = 3, m_2 = a \bmod 3 = 1, m_3 = a \bmod 2 = 0$. Με μέθοδο Lagrange υπολογίζουμε: $(1/6) \bmod 5 = 1, (1/10) \bmod 3 = 1$ άρα $a = (3/6 \bmod 5) * 6 + (1/10 \bmod 3) * 10 + (0/15 \bmod 2) * 15 = (3 * 1 \bmod 5) * 6 + (1 * 1 \bmod 3) * 10 + 0 = 28$.

Με μέθοδο Newton υπολογίζουμε: $s_1 * 1 \bmod 5 = 1 \Rightarrow s_1 = 1, s_2 * 5 \bmod 3 = 1 \Rightarrow s_2 = 2, s_3 * 15 \bmod 2 = 1 \Rightarrow s_3 = 1$. Άρα: $a_1 = 0 + (3s_1 \bmod 5) * 1 = 3 (= m_1), a_2 = 3 + [(1-3)s_2 \bmod 3] * 5 = 13, a_3 = 13 + [(0-13)s_3 \bmod 2] * 15 = 28 = a$. □

Είναι άμεση η προσαρμογή της μεθόδου Newton στο $\mathbb{Q}[x]$, με $a_0(x) = 0, a_1(x) = m_1(x)$ και, αν $a_i(x)$ τα ενδιάμεσα πολυώνυμα, τότε έχουμε:

$$a_i(x) = a_{i-1}(x) + \left[\frac{m_i(x) - a_{i-1}(x)}{\prod_{j=1}^{i-1} p_j(x)} \bmod p_i(x) \right] \cdot \prod_{j=1}^{i-1} p_j(x).$$

Παράδειγμα 3.3.4 (συνέχεια αυτού της 3.2.1): Με γραμμικά $p_i(x) = x - x_i$ και τιμές m_i, δίνονται $x_i = 0, 1, 2, m_i = -1, 3, 9$. Άρα

$$\begin{array}{rcl}
a_1(x) & = & -1, \\
a_2(x) & = & (-1) + [(3-(-1))/x \bmod (x-1)]x = -1 + [4 \bmod (x-1)]x = 4x - 1, \\
 & & \text{διότι } (1/x) \bmod (x-1) = 1, \\
a_3(x) & = & (4x-1) + [9 - (4x-1)/x(x-1) \bmod (x-2)]x(x-1) \\
 & = & (4x-1) + [(-2x+5) \bmod (x-2)]x(x-1) \\
 & & \text{διότι } 1/(x(x-1)) \bmod (x-2) = \frac{1}{2}, \text{ δηλ. } x(x-1) \bmod (x-2) = x^2 - x \bmod (x-2) = 2, \\
a_3(x) & = & = (4x-1) + x(x-1) = x^2 + 3x - 1, \\
 & & \text{διότι } (-2x+5) \bmod (x-2) = 1.
\end{array}$$

Για την αντιστροφή του πολυωνύμου $f(x) = x^2 - x$ στον πεπερασμένο δακτύλιο $\bmod p_i = x-2$ μπορούμε να λύσουμε ένα γραμμικό σύστημα: Γνωρίζουμε (από την σχέση Bézout και την επέκταση του Ευκλείδειου αλγόριθμου) τους βαθμούς των $s(x) = s$ (βαθμός$= 0 < \deg p_i(x)$) και του πηλίκου $q = ax + b$ (βαθμός$= 1 < \deg f(x) = 2$) και θέτουμε: $s(x^2 - x) = (ax + b)(x - 2) + 1$, το οποίο δίνει το ισοδύναμο γραμμικό σύστημα: $s = a, -s = -2a + b, -2b + 1 = 0$, συνεπώς $b = a = s = 1/2$.

Αυτή η μέθοδος είναι γενική. Όταν το $p_i(x)$ είναι γραμμικό, αρκεί να χρησιμοποιήσουμε το γεγονός πως η πράξη mod ισοδυναμεί με αποτίμηση. □

Γενικά, για την αντιστροφή πολυωνύμου $f(x)$ σε πεπερασμένο δακτύλιο $\bmod p_i(x)$ υπολογίζουμε την σχέση Bézout στην επέκταση του Ευκλείδειου αλγόριθμου (βλ. το επόμενο κεφάλαιο) με ορίσματα τα πολυώνυμα $f(x), p_i(x) \in \mathbb{Q}[x]$, που είναι πρώτα μεταξύ τους, οπότε προκύπτει η σχέση

$$s(x)f(x) - q(x)p_i(x) = \gcd(f, p_i) = 1, \text{ όπου } \deg s < \deg p_i, \deg q < \deg f.$$

3.3.1 Ασκήσεις

Άσκηση 3.3.5 Υπολογίστε την ορίζουσα του παρακάτω πίνακα με εφαρμογή του Κινέζικου θεωρήματος και του φράγματος Hadamard στην τιμή της:

$$\begin{bmatrix} 2 & 5 & -1 \\ 0 & 3 & 7 \\ -2 & 1 & -3 \end{bmatrix}.$$

Άσκηση 3.3.6 Υπολογίστε το γινόμενο των $f(x) = 2x - 3$ και $g(x) = x^2 - x + 5$ με αποτίμηση και εφαρμογή του Κινέζικου θεωρήματος.

Άσκηση 3.3.7 Δώστε μια κατασκευαστική απόδειξη του λήμματος 3.3.2 στην περίπτωση που ο p δεν είναι πρώτος.

Άσκηση 3.3.8 Δείξτε πώς η μέθοδος Newton μπορεί να εκτελεστεί με πιθανοκρατικό κριτήριο τερματισμού για να επιταχυνθεί [BEPP99].

3.4 Πολυώνυμα σε πολλές μεταβλητές

Έστω (n) το πλήθος των μεταβλητών. Βιβλιογραφία: [BP94, pp.62-65], [EP99, pp.1-15], [Zip93].

Άθροισμα πολυωνύμων (αραιή αναπαράσταση) με t_1 και t_2 όρους αντίστοιχα $= \Theta(t_1 + t_2)$.

Πολλαπλασιασμός. Έστω $N = \prod_{i=1}^{n} D_i, D_i = 2d_i + 1, d_i$ φράσσει από πάνω τον βαθμό των πολυωνύμων ως προς $x_i, D = \max_i\{D_i\}$.

- Μέθοδος [Karatsuba-Ofman] ανά μεταβλητή, σε $O_A(D^{n \lg 3})$.
- Μετασχηματισμός Kronecker σε μια μεταβλητή τότε κόστος $= O_A(N \lg N \lg\lg N) = O(D^n n \lg D(\lg n + \lg\lg n))$:
$$x_1 = y, x_{k+1} = y^{D_1 \cdots D_k}, k = 1, \ldots, n-1.$$

Υπολογισμός τιμών/παρεμβολής: υπολογίζουμε $2n$ τιμές των δεδομένων πολυωνύμων, άρα τα $2n$ γινόμενα τιμών αποτελούν τιμές του γινομένου πολυωνύμου. Από αυτές, με παρεμβολή, βρίσκουμε τους συντελεστές αυτού του πολυωνύμου με συνολικό κόστος $O_A(N \lg N \lg\lg D)$.

Για αραιά πολυώνυμα με $t \ll D^n$ όρους και συντελεστές σε άπειρα σώματα $O_A(t \lg^2 t \lg\lg t)$.

Υπολογισμός τιμών (σε πλέγμα $d_1 \times d_1 \times \cdots \times d_n$) και παρεμβολή (όπου $d = \max\{d_i\}$): Με βάση τον FFT, αριθμητικές πολυπλοκότητες $O_A^*(d^n)$ και $O_A^*(nd^n)$ αντίστοιχα. Για αραιά πολυώνυμα με πλήθος όρων $= t \ll T =$ ανώτερο όριο:

- κάθε υπολογισμός κοστίζει $O_A^*(T \log t)$,
- Με πιθανολογικό (probabilistic) αλγόριθμο (τυχαιότητας, randomized Monte Carlo), παρεμβολή $= O_A^*(nd^2t)$ [Zippel], εφόσον ο βαθμός ανά μεταβλητή d είναι γνωστός. Η παραπάνω πολυπλοκότητα στηρίζεται στην χρήση δομημένων πινάκων, ενώ υπάρχει και ντετερμινιστική έκδοση του αλγορίθμου με μεγαλύτερη, αλλά πάλι πολυωνυμική, πολυπλοκότητα.
- Σε άπειρα (ή αρκετά μεγάλα) σώματα, παρεμβολή $= O_A^*(ndT)$ [Ben-Or, Tiwari'88], εφόσον το φράγμα T είναι γνωστό. Χρησιμοποιεί τον αλγόριθμο Berlekamp-Massey για την επίλυση γραμμικής αναδρομικής ακολουθίας, ενώ η παραπάνω πολυπλοκότητα στηρίζεται στην χρήση δομημένων πινάκων.

3.5 Ταχύς Μετασχηματισμός Fourier

Πρόβλημα 3.5.1 *Διακριτού Μετασχηματισμού Fourier (ειδική περίπτωση υπολογισμού πολλών τιμών πολυωνύμου): Με δεδομένο πολυώνυμο $p(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0$ υπολογίζουμε τις τιμές του σε όλες τις n-οστές ρίζες της μονάδας στους μιγαδικούς.*

Η επίλυση γίνεται με τον Ταχύ Μετασχηματισμό (FFT, Fast Fourier Transform). Δες επίσης: [AHU74, pp.252-274], [EP99, pp.1-15]. Για σχετικά αριθμητικά προβλήματα: [BP94].

Μια σημαντική ευκολία είναι να υποθέσουμε πως το n είναι άρτιος. Λόγω της αναδρομής, τελικά θα χρειαστεί να είναι δύναμη του 2. Οι n ρίζες είναι

$$\{1, \omega = e^{2\pi i/n}, \omega^2 = e^{4\pi i/n}, \ldots, \omega^{n-1} = e^{2\pi i(n-1)/n}\}.$$

Για την υποδιαίρεση του προβλήματος γράφουμε

$$p(x) = (c_0 + c_2x^2 + \cdots + c_{n-2}x^{n-2}) + x(c_1 + c_3x^2 + \cdots + c_{n-1}x^{n-2}) = q(x^2) + xs(x^2)$$

και θέτουμε $y = x^2$, όπου τα $q(y), s(y)$ είναι βαθμού $(n-2)/2$.

Εκμεταλλευόμαστε τις ιδιότητες των ριζών του 1 για τον ταχύτερο υπολογισμό των τιμών: Όταν $x = \omega^j$ για $j = 0, \ldots, n-1$ τότε το $y = \omega^{2j}$ παίρνει μόνο $n/2$ διαφορετικές τιμές. Δηλαδή οι αναδρομικοί υπολογισμοί των $q(\omega^{2j}), s(\omega^{2j})$ αρκούν για να υπολογιστούν τα $p(\omega^j), p(\omega^{n/2+j})$. Επιπλέον $\omega^j = -\omega^{j+n/2}$, το οποίο μειώνει στο ήμισυ τους πολλαπλασιασμούς $\times s(y)$, ανάγοντας τις μισές προσθέσεις $q(y) + \ldots$ σε αφαιρέσεις γνωστών ποσοτήτων $q(y) - \ldots$. Έτσι ορίζεται ένας γράφος αναδρομικών κλήσεων για τις τιμές του $p(x)$, γνωστός και ως «πεταλούδα».

Άρα το πρόβλημα υπολογισμού n τιμών πολυωνύμου βαθμού $n-1$ ανάγεται σε δύο προβλήματα $n/2$ τιμών πολυωνύμων βαθμού $(n-2)/2$ (διαίρει+βασίλευε). Η επίλυση του αρχικού προβλήματος από τα δύο υποπροβλήματα κοστίζει $n/2$ πολλαπλασιασμούς και n προσθαφαιρέσεις επομένως η συνολική πολυπλοκότητα ισούται με

$$T(n) = 1,5n + 2T(n/2) = 1,5kn + 2^kT(n/2^k) = 1,5n\lg n + O(n) = O_A(n\lg n).$$

Παράδειγμα 3.5.2 $p(x) = 3x^3 + 2x^2 - x + 5, n = 4$, ρίζες του 1 είναι $\{1, \omega = i, \omega^2 = -1, \omega^3 = -\omega\}$. Γράφουμε

$$p(x) = (5 + 2x^2) + x(-1 + 3x^2) = q(y) + xs(y).$$

Με δύο πολλαπλασιασμούς και 4 προσθαφαιρέσεις το πρόβλημα ανάγεται στον υπολογισμό των τιμών των $q(y), s(y)$ στα σημεία $1, \omega^2 = -1$. Αυτό απαιτεί δύο πολλαπλασιασμούς $(2*1, 3*1)$ και 4 προσθαφαιρέσεις $(5+2, 5-2, -1+3, -1-3)$, εκμεταλλευόμενοι επαγωγικά τις ιδιότητες των ριζών της μονάδας. Το σύνολο των πράξεων είναι 4 πολλαπλασιασμοί και 8 προσθαφαιρέσεις συν 4 πράξεις για τον επαγωγικό υπολογισμό των $q(y), s(y)$. Το σύνολο πράγματι φράσσεται από $1,5n\lg n + n = 12 + 4$. □

Πρόβλημα 3.5.3 *Το αντίστροφο πρόβλημα (παρεμβολή): Υπολογισμός των συντελεστών πολυωνύμου βαθμού $n-1$ από τις τιμές του στις n-οστές ρίζες της μονάδας.*

Επίλυση με τον αλγόριθμο IFFT (Inverse Fast Fourier Transform). Θυμηθείτε την αναπαράσταση του προβλήματος με πίνακες Vandermonde. Έστω Ω ο πίνακας $n \times n$ με στοιχεία $\Omega_{ij} = [\omega^{ij}/\sqrt{n}]$ για

$i,j = 0,\ldots,n-1$. Το πρόβλημα του μετασχηματισμού Fourier είναι ο υπολογισμός του διανύσματος-στήλη p^T:

$$\sqrt{n}\left[\frac{\omega^{ij}}{\sqrt{n}}\right]_{i,j=0,\ldots,n-1}\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1}\end{bmatrix} = \left[\omega^{ij}\right]_{i,j=0,\ldots,n-1}\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1}\end{bmatrix} = \begin{bmatrix} p(\omega^0) \\ \vdots \\ p(\omega^{n-1})\end{bmatrix} = p^T.$$

Αντίστροφο πρόβλημα είναι λύση για διάνυσμα-στήλη c του παραπάνω συστήματος, με δεδομένο το p. Άρα $c = (1/\sqrt{n})\Omega^{-1}[p(\omega^0),\ldots,p(\omega^{n-1})]^T$ και δεδομένου ότι $\Omega^{-1} = [\omega^{-ij}/\sqrt{n}]$ και ω^{-1} είναι μια n–οστή ρίζα του 1, το c υπολογίζεται μέσω του μετασχηματισμού Fourier (FFT) σαν τον υπολογισμό τιμών του πολυωνύμου με συντελεστές $p(\omega^j)$ στις ρίζες του 1.

Πολλαπλασιασμός πολυωνύμων $p(x)q(x)$ σε $O_A(n\lg n)$ μέσω υπολογισμού τιμών και παρεμβολής (μέθοδος Toom):

1. Υπολογισμός τιμών μέσω FFT ($p(x)$ στα a_i για $i = 1,\ldots,2n$),
2. FFT (q στα a_i για $i = 1,\ldots,2n$),
3. $p(a_i) * q(a_i) \rightarrow$ τιμές $(pq)(a_i)$ για $i = 1,\ldots,2n$,
4. τέλος παρεμβολή μέσω IFFT ($(pq)(a_i)$ για $i = 1,\ldots,2n$) $\rightarrow$ συντελεστές $(pq)(x)$.

3.6 Πίνακες

Βιβλιογραφία: [DST88, pp.86-7], [AHU74, pp.226-35]. Θεωρούμε πυκνούς ορθογώνιους πίνακες $n \times m$: Η πρόσθεση και η αφαίρεση τέτοιων πινάκων εκτελούνται σε $O_A(nm)$.

Θεωρούμε τετράγωνους πίνακες $n \times n$: πολλαπλασιασμός $= \Omega_A(n^2)$.

1. Σχολικός αλγόριθμος $= O_A(n^3)$.
2. Διαίρει+βασίλευε [Strassen'69] $O_A(n^{\lg 7}) = O_A(n^{2.81})$.
3. [Coppersmith-Winograd'90] $O_A(n^{2.376})$.

Ο φημισμένος αλγόριθμος Διαίρει+βασίλευε [Strassen'69] κατέρριψε το κυβικό άνω φράγμα. Για να οριστεί, αρκεί το παράδειγμα πινάκων 2×2 που πολλαπλασιάζονται με 7 πολλαπλασιασμούς και «πολλά» αθροίσματα. Οι δεδομένοι πίνακες έχουν στοιχεία a_{ij}, b_{ij} για $i,j = 1,2$ και ο πίνακας-γινόμενο έχει στοιχεία c_{ij}. Έστω

$$m_2 = (a_{11}+a_{22})(b_{11}+b_{22}), m_3 = (a_{11}+a_{12})b_{22}, m_4 = a_{22}(b_{21}-b_{11}), m_5 = a_{11}(b_{12}-b_{22}), m_7 = (a_{21}+a_{22})b_{11}.$$

Τότε: $\begin{array}{ll} c_{11} = (a_{12}-a_{22})(b_{21}+b_{22}) + m2 - m3 + m4 & c_{12} = m_3 + m_5 \\ c_{21} = m_4 + m_7 & c_{22} = m_2 + m_5 - m_7 - (a_{11}-a_{21})(b_{11}+b_{12}) \end{array}$.

Λήμμα 3.6.1 *Η αριθμητική πολυπλοκότητα της αντιστροφής τετράγωνου πίνακα φράσσεται από αυτήν του υπολογισμού ορίζουσας.*

Απόδειξη. Χρησιμοποιούμε τον τύπο του αντίστροφου $A^{-1} = \frac{1}{\det A}A^a$, όπου ο πίνακας A^a έχει ως στοιχείο στην θέση (i,j) την ελάσσονα ορίζουσα (i,j) του A. Ο υπολογισμός όλων των ελασσόνων οριζουσών γίνεται με συνολική πολυπλοκότητα ίση με αυτή της ορίζουσας, χάρη στο θεώρημα 3.2.7. Το τελευταίο εφαρμόζεται και στην περίπτωση του μοντέλου real RAM εφόσον ο αλγόριθμος είναι σχετικά απλός. ΟΕΔ

Για τετράγωνους πίνακες $n \times n$ με σταθερά στοιχεία, οι εξής υπολογισμοί έχουν αριθμητικές πολυπλοκότητες που συνδέονται με σταθερές: Πολλαπλασιασμός, αντιστροφή, ορίζουσα, επίλυση $Mx = b$, παραγοντοποίηση σε κάτω/άνω τριγωνικούς $M = LU$, παραγοντοποίηση με αναδιάταξη (permutation) γραμμών $M = LUP$, όπου b διάνυσμα διάστασης $= n, L$ και U πίνακας $n \times n$ τριγωνικός κάτω και άνω αντίστοιχα, P πίνακας αναδιάταξης $n \times n$ δηλ. κάθε σειρά/στήλη περιέχει μόνο ένα μη μηδενικό στοιχείο που ισούται με 1.

Οι εξής υπολογισμοί έχουν αριθμητικές πολυπλοκότητες που φράσσονται από αυτήν του πολλαπλασιασμού πινάκων: Υπολογισμός πυρήνα, δηλ. των διανυσμάτων $\{x : Mx = 0\}$, υπολογισμός τάξης (rank), δηλ. πλήθους γραμμικά ανεξάρτητων γραμμών/στηλών.

Ορισμός 3.6.2 *Χαρακτηριστικό πολυώνυμο $n \times n$ πίνακα M είναι το πολυώνυμο* $\det(M - \lambda I)$, *όπου I ο μοναδιαίος πίνακας $n \times n$. Η μεταβλητή είναι λ και ο βαθμός $= n$. Οι ρίζες του χαρακτηριστικού πολυωνύμου λέγονται* ιδιοτιμές *(eigenvalues) του M. Στη διανυσματική εξίσωση $(M - \lambda I)x = 0$ οι ρίζες του λ είναι οι ιδιοτιμές, ενώ τα διανύσματα $x \neq 0$ διάστασης $= n$ λέγονται* ιδιοδιανύσματα.

Θεώρημα 3.6.3 (Cayley-Hamilton) *Έστω $\chi(\lambda) = \det(A - \lambda I)$ το χαρακτηριστικό πολυώνυμο πίνακα A, τότε $\chi(A) = 0$.*

Πρόταση 3.6.4 *Ιδιότητες:*
(1) Υπάρχουν $\leq n$ ανεξάρτητα ιδιοδιανύσματα.
(2) Για ιδιοδιανύσματα x, y, το διάνυσμα kx για σταθερά $k \neq 0$ καθώς και το διάνυσμα $x + y$ είναι επίσης ιδιοδιανύσματα με την ίδια ιδιοτιμή, έτσι τα ιδιοδιανύσματα που αντιστοιχούν στην ιδιοτιμή λ σχηματίζουν ένα γραμμικό υπόχωρο που καλείται ιδιόχωρος του λ.
(3) Για διαφορετικές ιδιοτιμές, τα αντίστοιχα ιδιοδιανύσματα είναι γραμμικώς ανεξάρτητα.

Πολυπλοκότητα χαρακτηριστικού πολυωνύμου $<$ πολλαπλασιασμού $* \log^2 n$. Πολυπλοκότητα ιδιοδιανυσμάτων/ιδιοτιμών $\leq 25n^3$, με αριθμητική προσέγγιση μόνο.

Περνάμε τώρα στην ορίζουσα πινάκων με συμβολικά στοιχεία (ή ακέραιους). Για τον υπολογισμό της, υπάρχει η μέθοδος του Bareiss [Bar68], η οποία αποφεύγει τη δημιουργία κλασμάτων (αντίστοιχα ρητών) [Akr89, ch.5]:
1. Προσαρμοσμένη απαλοιφή Gauss: πολλαπλ/ζουμε την γραμμή $j+1$ με a_{jj} και θεωρούμε την γραμμή j πολλαπλασιασμένη με $a_{(j+1)j}$.
2. Αφαιρούμε τη νέα γραμμή j από τη νέα γραμμή $j+1$. Μετά την αφαίρεση των γραμμών δημιουργούμε 0 στις θέσεις $(i,j), i > j$.
3. Επαναλαμβάνοντας τα βήματα 1, 2 στην γραμμή $j+2$ δημιουργούμε 0 στις θέσεις $(i, j+1), i > j+1$.
4. Παρατηρούμε πως τα μη μηδενικά στοιχεία της γραμμής $j+2$ διαιρούνται από το a_{jj}.

Κατ'επέκταση, τα μη μηδενικά στοιχεία της γραμμής $j+3$ διαιρούνται από την ορίζουσα $\begin{vmatrix} a_{j,j} & a_{j,j+1} \\ a_{j+1,j} & a_{j+1,j+1} \end{vmatrix}$.

Ένας πίνακας $[a_{ij}]_{ij}$ μετατρέπεται ως εξής:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots \\ 0 & a_{11}a_{22} - a_{12}a_{21} & a_{11}a_{23} - a_{13}a_{21} \\ 0 & \vdots & \\ 0 & a_{11}a_{i2} - a_{12}a_{i1} & a_{11}a_{i3} - a_{13}a_{i1} \end{bmatrix} \rightarrow \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots \\ 0 & a_{11}a_{22} - a_{12}a_{21} & \cdots & \begin{vmatrix} a_{11} & a_{2j} \\ a_{1j} & a_{21} \end{vmatrix} \\ 0 & 0 & a_{11}[1,2,3] & a_{11}[1,2,4] \end{bmatrix}$$

όπου $[1,2,j] = \det[a_{ik} : i = 1,2,3, k = 1,2,j]$.

Μελετάμε τώρα τη Δυαδική Πολυπλοκότητα. Για $n \times n$ πίνακα $A = [a_{ij}]_{ij}$, έστω a_i τα διανύσματα σε κάθε γραμμή (ή στήλη). Για την τιμή της ορίζουσας, το φράγμα Hadamard είναι το βέλτιστο γενικό φράγμα:

$$|\det A| \leq \prod_{i=1}^{n} \|a_i\|_2 \leq n^{n/2} \max\{|a_{ij}|\}^n,$$

Με το Κινέζικο θεώρημα πετυχαίνουμε κόστος $O_B^*(n^3 n \log^2 a + n^2 \log a) = O_B^*(n^4 \log^2 a)$, όπου a το απόλυτα μεγαλύτερο στοιχείο του A. Διαπιστώνουμε πως ο κυρίαρχος όρος οφείλεται στις αποτιμήσεις της ορίζουσας σε πεπερασμένα πεδία: απαιτούνται $O^*(n \log a)$ αποτιμήσεις από το φράγμα Hadamard, καθεμία κόστους $O_B^*(n^3 \log a)$ με τον απλό αλγόριθμο.

Η Μέθοδος Bareiss, αγνοώντας λογαριθμικούς παράγοντες, έχει κόστος $\sum_{i=1}^{n} n^2 i \log a = O_B^*(n^4 \log a)$. Σχετικά πρόσφατα, η πολυπλοκότητα αυτή βελτιώθηκε από τους Kaltofen-Villard [KV01, KV05].

Άσκηση 3.6.5 Συγκρίνετε την αριθμητική και δυαδική πολυπλοκότητα διαφορετικών μεθόδων υπολογισμού ορίζουσας πίνακα $m \times m$ του οποίου τα στοιχεία είναι πολυώνυμα σε μία μεταβλητή, βαθμού d και συντελεστές μήκους L. Συγκρίνετε τουλάχιστον δύο μεθόδους: την απευθείας ανάπτυξη της ορίζουσας και την παρεμβολή του πολυωνύμου της ορίζουσας.

3.6.1 Δομημένοι πίνακες

Η ενότητα μελετά δομημένους (structured) πίνακες, δηλ. πίνακες που ορίζονται από ένα πλήθος στοιχείων γραμμικό ως προς την διάστασή τους. Βιβλιογραφία: [BP94, EP99].

Έχουμε ήδη δει τους πίνακες Vandermonde που ορίζονται από μια στήλη τους, καθώς οι υπόλοιπες περιέχουν δυνάμεις τους. Μάλιστα είδαμε πως ο πολλαπλασιασμός ένος τέτοιου πίνακα με διάνυσμα ισοδυναμεί με την αποτίμηση πολυωνύμου μιας μεταβλητής βαθμού d σε $d+1$ σημεία, ενώ η επίλυση αντίστοιχου γραμμικού συστήματος ισοδυναμεί με την παρεμβολή των συντελεστών του πολυωνύμου. Αμφότερες πράξεις γίνονται σε $O_A(d \log^2 d)$, δηλ. περίπου μια τάξη μεγέθους ταχύτερα από τις αντίστοιχες πράξεις σε γενικούς πίνακες. Αυτός είναι και η συνηθέστερη συμπεριφορά, σε χοντρικές γραμμές, για την πολυπλοκότητα δομημένων πινάκων.

Ορισμός 3.6.6 *Ενας πίνακας $n \times m$ καλείται Toeplitz εάν τα στοιχεία στην θέση $(a+i, b+i)$, $i > 0$ όπου ορίζονται, ισούνται με αυτό στην θέση (a,b), δηλ. ο πίνακας έχει σταθερές διαγωνίους. Συνεπώς αρκούν $n+m-1$ στοιχεία για να οριστεί ο πίνακας (π.χ. τα στοιχεία στην πρώτη στήλη, πρώτη γραμμή).*

Έστω ένας πίνακας $n \times m$ με k υποπίνακες $k_i \times m$, όπου $\sum_i k_i = n$ και κάθε υποπίνακας ορίζεται από k_i συνεχόμενες γραμμές και όλες τις στήλες του αρχικού πίνακα. Εάν όλοι οι υποπίνακες είναι Toeplitz, ο συνολικός πίνακας καλείται Toeplitz κατά ομάδες (γραμμών) (block Toeplitz).

Ιδιότητες πίνακα Toeplitz (απλού και κατά ομάδες):

- Ο πολλαπλασιασμός ενός ορθογώνιου κάτω τριγωνικού πίνακα Toeplitz με ένα διάνυσμα εκφράζει τον πολλαπλασιασμό πολυωνύμων, όπου οι συντελεστές των πολυωνύμων βρίσκονται αντίστοιχα στην πρώτη στήλη του πίνακα και στα στοιχεία του διανύσματος. Ομοίως για τον πολλαπλασιασμό διανύσματος από αριστερά με έναν ορθογώνιο άνω τριγωνικό πίνακα Toeplitz.

- Όταν ο πίνακας είναι Toeplitz κατά ομάδες γραμμών, ο πολλαπλασιασμός διανύσματος από αριστερά εκφράζει το άθροισμα γινομένων πολυωνύμων.
- Η αντιμετάθεση στηλών (και γραμμών εφόσον δεν παραβιάζεται η ομαδοποίηση) δίνει ένα νέο πίνακα Toeplitz κατά ομάδες γραμμών, με τις ίδιες ιδιότητες.

Η πολυπλοκότητα των βασικών πράξεων σε τέτοιους πίνακες μειώνεται κατά μια τάξη μεγέθους περίπου, μέσω του FFT.

Άσκηση 3.6.7 Επεκτείνετε την παραπάνω συζήτηση στις αντίστοιχες πράξεις πολυωνύμων πολλών μεταβλητών. Εξετάστε και «αραιά» πολυώνυμα που ορίζονται από τους μη-μηδενικούς όρους τους.

Κεφάλαιο 4

Ευκλείδειος αλγόριθμος και εφαρμογές

4.1 Αλγεβρικό υπόβαθρο

Μελετάμε ορισμένες κατηγορίες δακτυλίων, χρήσιμες στη συνέχεια.

Ορισμός 4.1.1 Ακέραια περιοχή *(integral domain)* *λέγεται κάθε αντιμεταθετικός δακτύλιος με μονάδα* 1, *όπου δεν υπάρχει διαιρέτης του 0, δηλ.* $ab = 0 \Rightarrow a = 0 \vee b = 0$.

Ορισμός 4.1.2 *Μια ακέραια περιοχή* D *καλείται περιοχή μοναδικής παραγοντοποίησης (unique factorization domain, UFD) ανν κάθε στοιχείο επιδέχεται «μοναδικής» παραγοντοποίησης. Πιο τυπικά,*
(α) κάθε $a \in D - \{0, 1\}$ *παραγοντοποιείται ως* $a = c_1 \cdots c_n$, *όπου τα* c_i *ανάγωγα,*
(β) αν υπάρχει κι άλλη παραγοντοποίηση $a = d_1 \cdots d_m$, *τότε* $m = n$ *και υπάρχει μια 1-1 αντιστοίχιση των* c_i, d_i *τέτοια ώστε* $c_i | d_i$, $d_i | c_i$.

Ορισμός 4.1.3 Ευκλείδειος δακτύλιος *(Euclidean ring)* *λέγεται κάθε αντιμεταθετικός δακτύλιος* D *όπου ορίζεται μια συνάρτηση « διαβάθμισης »* $\phi : D \to \mathbb{N}$, *τ.ώ.* $ab \neq 0 \Rightarrow \phi(ab) \leq \phi(a)$ *και ορίζεται η διαίρεση* $a = bq + r$ *με υπόλοιπο* r, *όπου* $r = 0$ *ή* $\phi(r) < \phi(b)$.

Ένας Ευκλείδειος δακτύλιος που είναι και ακέραια περιοχή λέγεται Ευκλείδεια περιοχή (Euclidean domain).

Παράδειγμα 4.1.4 Ο δακτύλιος $\mathbb{Z}_s$, για $s = pq \in \mathbb{Z}$ όχι πρώτο, περιέχει τα p, q που είναι διαιρέτες του 0, άρα δεν είναι ακέραια περιοχή.

Το $\mathbb{Z}$ είναι Ευκλείδεια περιοχή με συνάρτηση διαβάθμισης την απόλυτο τιμή. Έστω σώμα K. Το K είναι Ευκλείδεια περιοχή με συνάρτηση διαβάθμισης $K \mapsto 1$. Επίσης το $K[x]$ είναι Ευκλείδεια περιοχή με συνάρτηση διαβάθμισης τον βαθμό πολυωνύμου, π.χ. $\mathbb{Q}[x]$ αλλά όχι το $\mathbb{Z}[x]$. □

Αποδεικνύεται ότι κάθε Ευκλείδεια περιοχή είναι UFD.

Στην ιεραρχία δακτυλίων εμφανίζεται και η εξής περιοχή:

Ορισμός 4.1.5 *Περιοχή κύριων ιδεωδών (principal ideal domain, PID) ορίζεται ως ένας δακτύλιος όπου όλα τα ιδεώδη είναι κύρια, δηλ. παράγονται από ένα στοιχείο.*

Κάθε Ευκλείδεια περιοχή είναι PID και κάθε PID είναι UFD, οπότε μια ιεραρχία δακτυλίων είναι:

- Σώμα (field),
- Ευκλείδεια περιοχή,
- Περιοχή κύριων ιδεωδών (PID),
- Περιοχή μοναδικής παραγοντοποίησης (UFD),
- Ακέραια περιοχή,
- Αντιμεταθετικός δακτύλιος.

Μια παράλληλη, αλλά λιγότερο πλούσια ιεραρχία περιγράφεται ως εξής: Δακτύλιος με διαίρεση (division ring) λέγεται κάθε δακτύλιος όπου ορίζεται η διαίρεση. Αν ισχύει και η αντιμεταθετικότητα στην διαίρεση, τότε πρόκειται για σώμα. Παράδειγμα δακτύλιου με διαίρεση που δεν είναι σώμα αποτελεί το σύνολο των quaternions. Ένας δακτύλιος με διαίρεση που είναι και ακέραια περιοχή θα είναι και Ευκλείδεια περιοχή.

4.2 Μέγιστος Κοινός Διαιρέτης

Μελετάμε με το πρόβλημα του Μέγιστου Κοινού Διαιρέτη (ΜΚΔ) ακεραίων και πολυωνύμων μιας μεταβλητής. Βιβλιογραφία: [DST88, pp.68-70], [AHU74, pp.300-13].

Ορισμός 4.2.1 *Ο* μέγιστος κοινός διαιρέτης *ΜΚΔ*(a, b) *σε μια Ευκλείδειο περιοχή είναι το μέγιστο στοιχείο της που διαιρεί τα* a *και* b*. Στους ακέραιους πρόκειται για το μέγιστο θετικό, στα πολυώνυμα μίας μεταβλητής, αυτό με μέγιστο βαθμό. Το* ελάχιστο κοινό πολλαπλάσιο *ΕΚΠ*(a, b) *είναι το μικρότερο στοιχείο που διαιρεί τα* a, b*.*

Μια θεμελιώδης ιδιότητα είναι πως ΕΚΠ(a, b) ΜΚΔ$(a, b) = ab$.

Ο Αλγόριθμος του Ευκλείδη είναι ο αρχαιότερος αλγόριθμος σε χρήση σήμερα, και μάλιστα ο αρχαιότερος που δίνει και τρόπο επαλήθευσης του αποτελέσματος μέσω της επέκτασής του. Δεδομένων των ακεραίων a, b θέτουμε $c_0 = a, c_1 = b$. Για $i = 2, 3, \ldots$ εκτελούμε τις διαιρέσεις με υπόλοιπο: $c_{i-2} = c_{i-1}q_i + c_i$, όπου ο επόμενος ακέραιος στην ακολουθία c_i ορίζεται ως το υπόλοιπο της διαίρεσης. Η ακολουθία τερματίζεται όταν $c_k = 0$ οπότε και ο ΜΚΔ$(a, b) = c_{k-1}$. Η απόδειξη της ορθότητας στηρίζεται στην ιδιότητα

$$\text{ΜΚΔ}(c_{i-2}, c_{i-1}) = \text{ΜΚΔ}(c_{i-1}, c_i).$$

Παρατηρήστε πως η ιδιότητα αυτή θα μπορούσε να χρησιμοποιηθεί ως επαγωγικός ορισμός της συνάρτησης ΜΚΔ, εφόσον ορίσουμε την επαγωγική βάση. Αποτελεί φυσικά και έναν αλγόριθμο.

Περνάμε τώρα στην επέκταση του Ευκλείδειου αλγόριθμου για τον υπολογισμό του ΜΚΔ ως γραμμικού συνδυασμού των αρχικών ακέραιων. Ορίζουμε $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$. Σύμφωνα με την σχέση $c_i = c_{i-2} - c_{i-1}q_i$, ορίζουμε επαγωγικά

$$s_i = s_{i-2} - s_{i-1}q_i, t_i = t_{i-2} - t_{i-1}q_i \Rightarrow \text{ΜΚΔ}(a, b) = as_{k-1} + bt_{k-1},$$

το οποίο είναι μια εφαρμογή της γενικότερης σχέσης $c_i = c_0 s_i + c_1 t_i$. Η τελευταία αποδεικνύεται επαγωγικά. Οι s_{k-1}, t_{k-1} λέγονται συντελεστές Bézout [vzGG99, sec.3.2]. Στο λήμμα 4.2.3 θα φράξουμε το μέγεθος των συντελεστών Bézout.

Παράδειγμα 4.2.2 $\text{ΜΚΔ}(612, 187) = 17 = 612 \cdot 4 + 187 \cdot (-13)$.

i	c_i	q_i	s_i	t_i	
0	612		1	0	
1	187		0	1	$612 = 3 * 187 + 51$
2	51	3	1	-3	$187 = 3 * 51 + 34$
3	34	3	-3	10	$51 = 1 * 34 + 17$
4	17	1	4	-13	$34 = 2 * 17 + 0$
5	0	2			

□

Λήμμα 4.2.3 *Για τους s_i, t_i που ορίστηκαν παραπάνω, ισχύει πως* $\deg s_i = \deg c_1 - \deg c_{i-1}$ *και* $\deg t_i = \deg c_0 - \deg c_{i-1}$.

Απόδειξη. Η απόδειξη της πρώτης σχέσης περνά από τις σχέσεις $\deg s_i = \sum_{j=3}^{i} \deg q_j > \deg s_{i-1}$. Για μια λεπτομερή απόδειξη, δείτε [vzGG99, Λήμ.3.10]. ΟΕΔ

Παράδειγμα 4.2.4 $p_0 = x^3 + 2x - 3, p_1 = 3x^2 + 2$, $\text{ΜΚΔ}(p_0, p_1) = 1$. Εφαρμόζουμε τον Ευκλείδειο αλγόριθμο στα πολυώνυμα με ρητούς συντελεστές $\mathbb{Q}[x]$.

i	p_i	q_i	s_i	t_i
0	$x^3 + 2x - 3$		1	0
1	$3x^2 + 2$		0	1
2	$\frac{4}{3}x - 3$	$\frac{1}{3}x$	1	$-\frac{x}{3}$
3	275/16	$(9/4)x + (81/16)$	$-(9/4)x - (81/16)$	$(3/4)x^2 + (27/16)x + 1$
4	0	$(64/825)x - (48/275)$		

□

Η πολυπλοκότητα του βασικού αλγορίθμου στο $\mathbb{Z}$, συμπεριλαμβανομένου του υπολογισμού s_i, t_i για ένα συγκεκριμένο i, είναι

$$O_B(M(n) \log n) = O_B(n \log^2 n \log\log n)$$

με τη μέθοδο Διαίρει+βασίλευε, όπου n = μέγιστο μήκος των a, b και $M(n)$ =πολυπλοκότητα πολλαπλασιασμού ακεραίων μήκους n. Η μέθοδος βασίζεται στο ΜΚΔ πολυωνύμων μιας μεταβλητής που συζητείται ευθύς αμέσως. Για τον υπολογισμό όλων των s_i, t_i το κόστος είναι $O_B(n^2)$. Είναι ενδιαφέρον πως δεν υπάρχουν ισχυρά κάτω φράγματα. Τα καλύτερα φαίνεται να είναι $\Omega(\log n)$ υπολογισμοί υπολοίπων [vanDerDries-Moschovakis].

Οι αλγόριθμοι του Ευκλείδη επεκτείνονται άμεσα σε πολυώνυμα μιας μεταβλητής στο $\mathbb{Q}[x]$ [vzGG99, ch.11], [BP94, sec.1.5]. Εδώ η συνάρτηση διαβάθμισης είναι ο βαθμός του πολυωνύμου. Ο αλγόριθμος Διαίρει+βασίλευε σε κάθε φάση του μειώνει στο ήμισυ τον βαθμό του υπολοίπου. Αυτή η φάση έχει ασυμπτωτική πολυπλοκότητα $M(n)$, δηλ. ίση με το κόστος πολλαπλασιασμού και n ο μέγιστος βαθμός των $a(x), b(x)$. Το συνολικό κόστος είναι

$$O_A(M(n) \log n) = O_A(n \log^2 n).$$

Για τον υπολογισμό όλων των s_i, t_i το κόστος είναι $O_A(n^2)$.

Το κυριότερο πρόβλημα εδώ είναι η εκθετική αύξηση του μεγέθους των (ενδιάμεσων) συντελεστών στον Ευκλείδειο αλγόριθμο. Γι' αυτό έχουν μελετηθεί μέθοδοι που γενικεύουν τη βασική σχέση, βασισμένες στην ψευδο-διαίρεση: Έστω $\sigma(p)$ ο μεγιστοβάθμιος συντελεστής του πολυωνύμου p.

Ορισμός 4.2.5 *Στην* ψευδο-διαίρεση $\alpha p(x) = q(x)s(x)+r(x)$, *όπου* $p(x), s(x) \in \mathbb{Z}[x]$ *με* $\deg(p(x)) \geq \deg(s(x)) > \deg(r(x))$, *έχουμε* $\alpha = \sigma(s)^{\delta} \in \mathbb{Z}$, *όπου* $\delta = \deg(p(x)) - \deg(s(x)) + 1$, *ώστε το* ψευδο-πηλίκο $q(x) \in \mathbb{Z}[x]$, *συνεπώς και το* ψευδο-υπόλοιπο $r(x) \in \mathbb{Z}[x]$. *Τα* $q(x), r(x)$ *είναι μοναδικά.*

Έστω $p_0(x) = a(x), p_1(x) = b(x)$ και για $i \geq 2 : \alpha_i p_{i-2}(x) = p_{i-1}(x)q_i(x) + \beta_i p_i(x)$ όπου α_i και β_i σταθερές. Για τον πλήρη ορισμό τους δες βιβλιογραφία. Συνοπτικά:

- $\alpha_i = \beta_i = 1$ στον *Ευκλείδειο* αλγόριθμο: δίνει το ελάχιστο β_i αλλά το μέγιστο μέγεθος συντελεστών, δηλ. εκθετικό στην χειρότερη περίπτωση [Zip93].
- $\beta_i p_i(x) =$ ψευδο-υπόλοιπο στην παραπάνω ψευδο-διαίρεση όπου το β_i είναι ο ΜΚΔ των συντελεστών του ψευδο-υπολοίπου (άρα υπολογίζεται ως ένα ΜΚΔ ακεραίων), δηλ. το $p_i(x)$ είναι ένα *πρωτογενές (primitive)* πολυώνυμο: μέγιστο β_i, ελάχιστο μέγεθος πολυωνυμικών συντελεστών, αλλά υψηλό υπολογιστικό κόστος. Αυτός ο αλγόριθμος εφαρμόζεται επαγωγικά και με πολλές μεταβλητές $\mathbb{Z}[x_1, \ldots, x_n]$.
- Το β_i δίνεται σε συνάρτηση των α_j, β_j για $j < i$ ενώ τα πολυώνυμα δίνονται από κάποια υπο-απαλοίφουσα (subresultant) (δες ενότητα 4.3 και κεφ. 6). Συγκεκριμένα, $\alpha_i = c^{d_{i-2}-d_{i-1}+1}$, όπου c ο μεγιστοβάθμιος συντελεστής του $p_{i-1}(x)$ και $\deg p_i = d_i$. Η θεωρία των Habicht, Collins, Brown αποδεικνύει πως το β_i διαιρεί το ψευδο-υπόλοιπο των $p_{i-2}(x), p_{i-1}(x)$. Επιτυγχάνονται ενδιάμεσες τιμές β_i και ενδιάμεσο μέγεθος συντελεστών των p_i σε σχέση με τις άλλες μεθόδους. Συγκεκριμένα, οι συντελεστές των p_i έχουν μήκος $O_B^*(nL)$, όπου L το μέγεθος των συντελεστών στα δεδομένα πολυώνυμα. Η μέθοδος αυτή πετυχαίνει βέλτιστη δυαδική πολυπλοκότητα $O_B^*(n^3L)$ για τον υπολογισμό *ολόκληρης* της ακολουθίας [Lombardi-Roy-ElDin, Reischert].

4.3 Απαλοίφουσα δύο πολυωνύμων

Έστω $p_1 = a_{d_1}x^{d_1} + \cdots + a_0$ και $p_2 = b_{d_2}x^{d_2} + \cdots + b_0$ σε δακτύλιο $D[x]$, όπου D μια Ευκλείδεια περιοχή. Θα μελετήσουμε την απαλοίφουσα των πολυωνύμων, που δίνει μια συνθήκη επιλυσιμότητας του συστήματος των δύο πολυωνύμων. Παρατηρήστε πως, για τυχαίους συντελεστές, $n+1$ πολυώνυμα σε n μεταβλητές δεν έχουν κοινές ρίζες (εδώ $n = 1$).

Ορισμός 4.3.1 *Η απαλοίφουσα* $R(p_1, p_2)$ *των πολυωνύμων ανήκει στο* D *και μηδενίζεται αν τα πολυώνυμα έχουν τουλάχιστον μια κοινή ρίζα στην αλγεβρική θήκη του* D.

Ορίζουμε τον πίνακα Sylvester S με στήλες που αντιστοιχούν στα μονώνυμα με δυνάμεις $[0, 1, \ldots, d_1 + d_2 - 1]$. Υπάρχουν 2 ομάδες γραμμών και περιέχουν πολλαπλάσια των p_1 και p_2 επί τις εξής δυνάμεις του x: $B_1 = [0, 1, \ldots, d_2 - 1]$ και $B_2 = [0, 1, \ldots, d_1 - 1]$ αντίστοιχα.

$$R(p_1, p_2) = \begin{vmatrix} a_0 & a_1 & \cdots & a_{d_1} & 0 & \cdots & & 0 \\ 0 & a_0 & a_1 & \cdots & a_{d_1} & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & \\ 0 & & & a_0 & a_1 & \cdots & & a_{d_1} \\ b_0 & b_1 & \cdots & & b_{d_2} & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & & b_{d_2} & 0 & 0 \\ \vdots & & \ddots & & & \ddots & & \\ 0 & & & b_0 & b_1 & \cdots & & b_{d_2} \end{vmatrix}.$$

Θεώρημα 4.3.2 [Syl53] *Υποθέτουμε ότι a_{d_1} και b_{d_2} είναι μη μηδενικό δηλ.* $\deg p_i = d_i, i = 1, 2$. *Τότε* $\det S = 0$ *αν και μόνο αν τα p_1 και p_2 έχουν κοινή ρίζα.*

Απόδειξη. Έστω κοινή ρίζα α. Τότε το μη μηδενικό διάνυσμα $[1, \alpha, \alpha^2, \ldots, \alpha^{d_1+d_2-1}]$ βρίσκεται στον πυρήνα του S διότι το γινόμενο του S επί το διάνυσμα περιέχει τις τιμές των πολλαπλασίων των p_1, p_2 στο α. Άρα ο S είναι μη αντιστρέψιμος.

Αντίστροφα: $\det S = 0 \Rightarrow$ υπάρχει μη μηδενικό διάνυσμα w τέτοιο ώστε $wS = 0$. Θεωρούμε πως το w αντιπροσωπεύει 2 πολυώνυμα q_1, q_2 με συντελεστές που αντιστοιχούν στα B_1 και B_2. Τότε το wS εκφράζει το πολυώνυμο $p_1q_1 + p_2q_2 = 0 \Rightarrow p_1q_1 = -p_2q_2$. Εφόσον αυτό το πολυώνυμο είναι βαθμού $< d_1 + d_2$, το ελάχιστο κοινό πολλαπλάσιο (ΕΚΠ) των p_1, p_2 είναι βαθμού $< d_1 + d_2$. Όμως, γενικά, $\deg \gcd(p_1, p_2) = d_1 + d_2 - \deg(\text{ΕΚΠ})$, άρα $\deg[\gcd(p_1, p_2)] > 0$ δηλ. δεν είναι σταθερός, άρα υπάρχει κοινή (μιγαδική) ρίζα. ΟΕΔ

Πόρισμα 4.3.3 *Υπό τις παραπάνω προϋποθέσεις, η απαλοίφουσα $R(p_1, p_2)$ του συστήματος ισούται με* $\det S$. *Συνεπώς, ο βαθμός της απαλοίφουσας ως προς τους συντελεστές των p_1, p_2 ισούται με d_2 και d_1 αντίστοιχα. Τέλος,* $R(p_1, p_2) = 0 \Leftrightarrow \deg \gcd(p_1, p_2) \geq 1$.

Ο πίνακας Sylvester περιέχει 2 υποπίνακες Toeplitz (με όλες τις στήλες) άρα είναι Toeplitz κατά ομάδες γραμμών. Ο πίνακας Toeplitz (κατά ομάδες) ορίζεται στην ενότητα 3.6.1.

Η απαλοίφουσα υπολογίζεται και ως ορίζουσα του πίνακα Bézout [1779]. Υποθέτουμε $d_1 \geq d_2$ και, χρησιμοποιώντας μια νέα μεταβλητή y, ορίζουμε πολυώνυμο στις μεταβλητές x, y:

$$\Delta(x, y) \;=\; \frac{1}{x - y} \begin{vmatrix} p_1(x) & p_1(y) \\ p_2(x) & p_2(y) \end{vmatrix} \;=\; \sum_{i=0}^{d_1-1} \theta_i(x) y^i.$$

Η διαίρεση ορίζεται διότι για $x = y$ η ορίζουσα μηδενίζεται. Το πολυώνυμο $\Delta(x, y)$ είναι συνολικού βαθμού $d_0 + d_1 - 1$, συμμετρικό ως προς x, y και βαθμού $d_1 - 1$ ανά μεταβλητή, όπου τα $\theta_i(x)$ πολυώνυμα σε μια μεταβλητή. Κατασκευάζουμε τώρα τον πίνακα της απαλοίφουσας:

$$\begin{array}{r} \\ \theta_0 \\ \vdots \\ \theta_{d_2-1} \\ p_2(x) \\ \vdots \\ x^{d_1-d_2-1}\, p_2(x) \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \cdots & \cdots & x^{d_1-1} \end{array} \\ \left[\begin{array}{cccc} & & & \\ & & & \\ & & & \\ & & M & \\ & & & \\ & & & \\ & & & \end{array}\right] \end{array}$$

Θεώρημα 4.3.4 *Η ορίζουσα του παραπάνω πίνακα M ισούται με την απαλοίφουσα $R(p_1, p_2)$.*

Απόδειξη. Έστω α κοινή ρίζα των p_i τότε $\Delta(\alpha, y) = 0$ και όλα τα $\theta_i(\alpha)$ μηδενίζονται. Συνεπώς υπάρχει διάνυσμα $(1, \alpha, \ldots, \alpha^{d_1-1}) \neq 0$ στον πυρήνα του M, άρα $\det M = 0$, επομένως $R \mid \det M$.

Θυμηθείτε το πόρισμα 4.3.3. Το $\Delta(x, y)$, και συνεπώς τα θ_i, είναι όλα γραμμικά ως προς τους συντελεστές κάθε p_i. Άρα ο βαθμός της ορίζουσας $\det M$ ως προς τους συντελεστές των p_1, p_2 είναι d_2, d_1 αντίστοιχα, άρα η ορίζουσα δεν περιέχει παρασιτικό παράγοντα επιπλέον της απαλοίφουσας. ΟΕΔ

Η ορίζουσα του S δεν αλλάζει αν προσθέσουμε την j-οστή στήλη της, πολλαπλασιασμένη με x^{j-1} για $j = 2, \ldots, d_1 + d_2$, στην πρώτη στήλη. Όμως ο πίνακας έχει αλλάξει καθόσον η πρώτη στήλη περιέχει τα πολυώνυμα $p_1(x), \ldots, x^{d_2-1}p_1(x), p_2(x), \ldots, x^{d_1-1}p_2(x)$. Αν αναπτύξουμε την ορίζουσα ως προς την πρώτη στήλη, συνάγεται η εξής ιδιότητα: $R(p_1, p_2) = p_1(x)t(x)+p_2(x)s(x)$, όπου $\deg t < d_2, \deg s < d_1$.

Επεκτείνουμε τώρα την συζήτηση στις *υπο-απαλοίφουσες* (subresultants) δυο πολυωνύμων μιας μεταβλητής, βλ. [Mis93, ch.7], [Yap00] ή [Zip93, sec.93]. Θεωρήστε την i-οστή ορίζουσα

$$R_i(p_1, p_2) = \begin{vmatrix} p_1(x) & a_{i+1} & \cdots & a_{d_1} & & \\ \vdots & & & & \ddots & \\ x^{d_2-i-1}p_1(x) & & & \cdots & & a_{d_1} \\ p_2(x) & b_{i+1} & \cdots & b_{d_2} & & \\ \vdots & & & & \ddots & \\ x^{d_1-i-1}p_2(x) & & & \cdots & & b_{d_2} \end{vmatrix}.$$

Ο πίνακας προκύπτει από τον S αν αφαιρέσουμε τις τελευταίες i γραμμές που περιέχουν συντελεστές του p_1, τις τελευταίες i γραμμές (που περιέχουν συντελεστές του p_2), τις τελευταίες i στήλες (οι οποίες πλέον περιέχουν μόνο μηδενικά) και, τέλος, τις i αριστερότερες στήλες που βρίσκονται δεξιά της πρώτης. Ο πίνακας είναι προφανώς τετράγωνος, με διάσταση $d_1 + d_2 - 2i$.

Ορισμός 4.3.5 *Η μηδενική υπο-απαλοίφουσα R_0 είναι η απαλοίφουσα $R(p_1, p_2) = \det S$. Για $0 < i \leq \min\{d_1, d_2\}$, η i-οστή υπο-απαλοίφουσα είναι η ορίζουσα R_i. Για $i = \min\{d_1, d_2\}$, η υπο-απαλοίφουσα R_i είναι η ορίζουσα του πίνακα που περιέχει μόνο συντελεστές του p_2 όπου η πρώτη γραμμή είναι $[p_2, 0, \ldots, 0]$. Για $\min\{d_1, d_2\} < i < \max\{d_1, d_2\}$ ορίζουμε $R_i = 0$.*

Λήμμα 4.3.6 *Οι συντελεστές της υπο-απαλοίφουσας R_i έχουν δυαδικό μήκος $O^*((d_1 + d_2)L)$, αν το L φράσσει το δυαδικό μήκος των συντελεστών των $p_i(x)$.*

Ο βαθμός της $R_0 = R$ ως προς x είναι μηδέν. Αν $i = d_2 < d_1$, ο αντίστοιχος πίνακας είναι κάτω τριγωνικός και $R_{d_2}(x) = p_2(x)a_{d_2}^{d_1-d_2-1}$, άρα $\deg R_{d_2}(x) = d_2$.

Θεώρημα 4.3.7 *Ο βαθμός της υπο-απαλοίφουσας είναι $\deg R_i(x) \leq i$ για $i = 0, \ldots, \min\{d_1, d_2\}$.*

Η βασική ιδιότητα των υπο-απαλοιφουσών είναι η παρακάτω ισοδυναμία.

Θεώρημα 4.3.8 *Εφόσον τα $p_1, p_2 \in K[x]$ για K μια περιοχή μοναδικής παραγοντοποίησης (unique factorization domain) με μονάδα, τα p_1, p_2 έχουν ένα κοινό διαιρέτη βαθμού $k \Leftrightarrow R_i = 0$, $\forall i < k$ και $R_k \neq 0$.*

4.4 Ρητή παρεμβολή κατά Padé

Η υπόλοιπη ενότητα εφαρμόζει τον Ευκλείδειο αλγόριθμο στο πρόβλημα της ρητής παρεμβολής ή προσέγγισης κατά Padé.

Ορισμός 4.4.1 *Έστω πολυώνυμο $f \in F[x]$ βαθμού $\leq N - 1$. Η ρητή παρεμβολή ή προσέγγιση κατά* Padé *$(k, N - k)$ του πολυωνύμου f συνίσταται στην εύρεση πολυωνύμων $r, t \in F[x]$, βαθμών $\leq k - 1$ και $\leq N - k$ αντίστοιχα, όπου $t(0) \neq 0$, τέτοια ώστε*

$$r \equiv tf \bmod x^N.$$

Σε πολλές εφαρμογές το f είναι απλώς οι πρώτοι N όροι μιας σειράς Taylor μιας οποιασδήποτε αναλυτικής συνάρτησης. Δηλ. ορίζεται πλήρως από τις τιμές της συνάρτησης και των $N-1$ πρώτων παραγώγων της στο 0, γιαυτό και μιλάμε για "παρεμβολή". Το γενικότερο πρόβλημα, όπου δίνονται οι τιμές μιας αναλυτικής συνάρτησης σε N οποιαδήποτε σημεία x_i καλείται προσέγγιση Hermite. Τότε $p_0 = \prod_{i=1}^{N}(x-x_i)$. Αν τα x_i είναι όλα διαφορετικά, τότε ονομάζεται προσέγγιση Cauchy.

Το πρόβλημα λύνεται με την επέκταση του Ευκλείδειου αλγόριθμου. Ορίζουμε το j ως το πρώτο βήμα (δηλ. ελάχιστο j) όπου $\deg p_j < k$, δηλ. $\deg p_{j-1} \geq k$. Αν διαλέξω $p_0 = x^N$, τότε $\deg t_j = \deg p_0 - \deg p_{j-1} \leq N-k$. Επίσης $p_1 t_j \equiv p_j \bmod p_0$, οπότε αρκεί να διαλέξω $p_1 = f$ και τα p_j, t_j είναι σχεδόν λύση της προσέγγιση Padé.

Για μια πλήρη λύση απαιτείται $t(0) \neq 0$ ώστε το πολυώνυμο $t(x)$ να είναι αντιστρέψιμο $\bmod x^N$. Αν $\text{ΜΚΔ}(p_j, t_j) = 1 \Rightarrow \text{ΜΚΔ}(p_0, t_j) = 1$ διότι $p_j = p_0 s_j + p_1 t_j$. Όμως $\text{ΜΚΔ}(x^N, t_j) = 1 \Rightarrow t_j(0) \neq 0$, δηλ. έχουμε πλήρη λύση αν $\text{ΜΚΔ}(p_j, t_j) = 1$. Αντίστροφα, όταν υπάρχει πλήρης λύση τότε $\text{ΜΚΔ}(p_j, t_j) = 1$. Διότι αλλιώς, $\text{ΜΚΔ}(p_j, t_j) \neq 1 \Rightarrow \text{ΜΚΔ}(x^N, t_j) \neq 1 \Rightarrow x | t_j(x)$. Δείξαμε λοιπόν πως έχουμε πλήρη λύση ανν $\text{ΜΚΔ}(p_j, t_j) = 1$.

Παράδειγμα 4.4.2 Προσέγγιση Padé$(2,2)$, του $f = 1 + 2x + 3x^2 + 4x^3 \in \mathbb{Z}_5[x]$, δηλ. $N = 4, k = 2$. Για απλοποίηση των πράξεων θέτω $p_1 = -f \equiv x^3 + 2x^2 + 3x + 4$.

i	p_i	q_i	s_i	t_i
0	x^4		1	0
1	$x^3 + 2x^2 + 3x + 4$	$x + 3$	0	1
2	$x^2 + 2x + 3$	x	1	$4x + 2$
3	4	$4x^2 + 3x + 2$	$4x$	$x^2 + 3x + 1$
4	0		$4x^3 + 3x^2 + 2x + 1$	x^4

Για $j = 3$, $p_3/t_3 \equiv -1/(x-1)^2$ λύνει το αρχικό πρόβλημα διότι αυτό είναι το ελάχιστο j όπου $\deg p_j < 2$. Σημειώστε πως $t_3 \equiv (x-1)^2$.

Επιπλέον, για $j = 1$, $p_1/t_1 \equiv f$ λύνει την προσέγγιση Padé$(4,0)$ δηλ. επιτυγχάνει απλώς μια παρεμβολή πολυωνύμου, όπου όμως το δεδομένο σημείο είναι πολλαπλό (κι όχι διαφορετικά σημεία).

Για $j = 4$ δεν παρέχει λύση σε κανένα πρόβλημα Padé διότι $x | t_4$ και όντως θα είχαμε $0/(4x^4)$. □

Η Πολυπλοκότητα για την αναγνώριση κι εύρεση λύσης Padé είναι $O_A(N \log^2 N)$. Σε χρόνο $O_A(N^2)$ βρίσκουμε για ποια k, N το αντίστοιχο πρόβλημα Padé$(k, N-k)$ έχει λύση και ποια είναι αυτή. Ας σημειωθεί πως ένας αλγόριθμος που λύνει την προσέγγιση Padé μπορεί να λύσει το πρόβλημα του ΜΚΔ [BP94, sec.1.5].

4.5 Γραμμικώς αναδρομικές ακολουθίες

Ξεκινάμε με γραμμικώς αναδρομικές ακολουθίες και καταλήγουμε στον αλγόριθμο των Berlekamp-Massey. Στην συνέχεια εξετάζουμε μια βασική εφαρμογή, η οποία αφορά στους δομημένους και αραιούς πίνακες.

Ορισμός 4.5.1 [vzGG99, sec.12.3] *Έστω ένας διανυσματικός χώρος V επί κάποιου σώματος F. Η ακολουθία $a = (a_0, a_1, a_2, \dots)$, με στοιχεία $a_i \in V$, καλείται* γραμμικώς αναδρομική *(linearly recursive) αν υπάρχει $N \in \mathbb{N}$ και*

$$\exists \chi = \sum_{j=0}^{N} c_j x^j \in F[x],\ \deg \chi(x) = N \ :\ \sum_{j=0}^{N} c_j a_{j+i} = 0,\ \forall\ i \in \mathbb{N}.$$

Το $\chi(x)$ καλείται χαρακτηριστικό ή γεννήτωρ (characteristic, generating, annihilating) πολυώνυμο της a. Το ελάχιστο (minimal) πολυώνυμο $\mu_a(x)$ της ακολουθίας είναι το χαρακτηριστικό πολυώνυμο ελάχιστου βαθμού.

Παράδειγμα 4.5.2 1. Για την $a = (0, 0, \dots)$ με $V = F$, κάθε πολυώνυμο είναι χαρακτηριστικό.

2. Για την Fibonacci με $V = F = \mathbb{Q}$, $a = (0, 1, 1, 2, 3, 5, \dots)$ δηλ. $a_{i+2} = a_{i+1} + a_i$, με χαρακτηριστικό πολυώνυμο $\chi(x) = x^2 - x - 1$. Αυτό είναι και ελάχιστο, διότι δεν παραγωγίζεται.

3. Για κάποιον τετράγωνο πίνακα $A \in V = F^{N\times N}$, έστω η ακολουθία $a_i = A^i$. Τότε, το χαρακτηριστικό πολυώνυμο του πίνακα $\chi_A = \det(A - xI)$ είναι και χαρακτηριστικό της ακολουθίας, σύμφωνα με το θεώρημα Cayley-Hamilton. Αντίστοιχα, το *ελάχιστο πολυώνυμο* του πίνακα είναι και ελάχιστο της ακολουθίας, όπου το πρώτο ορίζεται ως το πολυώνυμο με κύριο συντελεστή 1 και απλές ρίζες τις ιδιοτιμές του A.

4. Έστω $b \in V = F^N$, πίνακας $A \in F^{N\times N}$ και η ακολουθία Krylov $a_i = A^i b$: οποιοδήποτε χαρακτηριστικό πολυώνυμο της (A^i) είναι και χαρακτηριστικό πολυώνυμο της $(a_i = A^i b)$. Επίσης, $\mu_{A^i b} | \mu_{A^i}$.

5. Αν επιπλέον έχουμε διάνυσμα $u \in F^N$, τότε οποιοδήποτε χαρακτηριστικό πολυώνυμο της $(A^i b)$ είναι και χαρακτηριστικό πολυώνυμο της $(u^T A^i b)$. Επίσης, $\mu_{u^T A^i b} | \mu_{A^i b}$.

□

Θα συμβολίζουμε με $f \otimes a$ μια νέα ακολουθία με i-στό στοιχείο το $\sum_{j=0}^{N} f_j a_{j+i}$. Τότε ένα πολυώνυμο $f \neq 0$ είναι χαρακτηριστικό της ακολουθίας a ανν $f \otimes a = 0 \Leftrightarrow \mu_a(x) | f(x)$. Για την απόδειξη του τελευταίου με αναγωγή σε άτοπο, θεωρήστε το υπόλοιπο της διαίρεσης, που είναι ένα νέο χαρακτηριστικό πολυώνυμο βαθμού μικρότερου από αυτόν του $\mu_a(x)$.

Στους πίνακες, $\mu(x) | \chi(x)$ ενώ ισούνται αν και μόνο αν όλες οι ιδιοτιμές έχουν πολλαπλότητα $= 1$.

Λήμμα 4.5.3 *Έστω $h = \sum_i a_i x^i$ η γεννήτρια συνάρτηση μιας ακολουθίας, ένα πολυώνυμο $f \in F[x]$, $\deg f = d$, και $r := A(f) = x^d f(1/x)$ το ανάστροφό του. Τότε*

$$f \otimes a = 0 \Leftrightarrow rh \in F[x] \ : \ \deg(rh) < d \Leftrightarrow \exists g \in F[x], \deg(g) < d \ : \ h = g/r.$$

Επίσης, $f = \mu_a \Rightarrow d = \max\{1 + \deg g, \deg r\}$ και $\text{ΜΚΔ}(g, r) = 1$.

Απόδειξη. $f \otimes a = 0 \Leftrightarrow f_0 a_i + \dots + f_d a_{d+i} = 0$, όπου το τελευταίο άθροισμα εκφράζει τον συντελεστή του x^{d+i} στο rh για κάθε $i \geq 0$. Άρα $rh = g \in F[x]$.

Για το δεύτερο σκέλος, $[\deg r \leq d \ \& \ \deg g < d] \Rightarrow d \geq \max\{\cdot\}$. Όμως, $d > \max\{\cdot\} \Rightarrow \deg r < d \Rightarrow f_0 = 0 \Rightarrow x | f(x) \Rightarrow (f/x)(x)$ είναι χαρακτηριστικό πολυώνυμο της a, άρα το $f(x)$ δεν είναι ελάχιστο, το οποίο είναι αντίθετο της υπόθεσης.

Για το τελευταίο σκέλος, έστω $u := \text{ΜΚΔ}(g, r)$ και θα δείξουμε πως πρόκειται για το σταθερό πολυώνυμο. Εισάγουμε πολυώνυμο $f' := f/A(u)$ βαθμού $\deg f' = d - \deg u$, όπου $r/u = A(f')$. Τώρα, $(r/u)h = g/u$ είναι πολυώνυμο (διότι $u|g$) βαθμού $< d - \deg u$. Άρα το πολυώνυμο f' ικανοποιεί τις αρχικές υποθέσεις (στην θέση του f) και με βάση το πρώτο σκέλος είναι χαρακτηριστικό. Αφού το f είναι ελάχιστο, έχουμε $d - \deg u \geq d \Rightarrow \deg u = 0$. ΟΕΔ

Με δεδομένους $2N$ όρους μιας ακολουθίας κι ενός άνω φράγματος N στον βαθμό του ελάχιστου πολυωνύμου, είναι τώρα εύκολο να υπολογίσουμε το ελάχιστο πολυώνυμο από το παραπάνω λήμμα: Έστω

$h := a_{2N-1}x^{2N-1} + \cdots + a_0$. Η προσέγγιση Padé$(N, N)$ του h δίνει $g, t \in F[x],\ \deg g < N, \deg t \leq N$ τέτοια ώστε $h \equiv g/t \bmod x^{2N}$ και $t(0) \neq 0$. Θέτοντας $d := \max\{1 + \deg g, \deg t\}$, ο αλγόριθμος επιστρέφει το ανάστροφο του t ως προς d, δηλ. το $x^d t(1/x)$.

Παράδειγμα 4.5.4 Συνέχεια του παραδείγματος 4.4.2. Το δεδομένο πολυώνυμο f αντιστοιχεί στην ακολουθία $(1, 2, 3, 4, \dots) \subset \mathbb{Z}_5$. Η απάντηση $f \equiv -1/(x-1)^2 \bmod x^4$ οδηγεί στο $d := \max\{1, 2\} = 2$ άρα $\mu(x) = A_2((x-1)^2) = x^2 + 3x + 1$ που όντως είναι χαρακτηριστικό (κι ελάχιστο) της ακολουθίας $(1, 2, 3, 4, 0, 1, 2, \dots)$. □

Η υπόλοιπη ενότητα εφαρμόζει τα παραπάνω σε δομημένους κι αραιούς πίνακες που διαθέτουν ταχύ πολλαπλασιασμό με διάνυσμα με βάση την προσέγγιση του Wiedemann, δες [vzGG99]. Η ιδέα είναι πως το ελάχιστο πολυώνυμο $\mu_{A^i b}$ της ακολουθίας Krylov υπολογίζεται σε χρόνο $O_A(N)\Delta(N) + O_A(N \log^2 N) = O_A(N)\Delta(N)$, όπου $\Delta(N)$ η αριθμητική πολυπλοκότητα πολλαπλασιασμού πίνακα επί διάνυσμα και ο πρώτος προσθετέος αφορά στον υπολογισμό $2N$ όρων της ακολουθίας, ενώ ο δεύτερος στην εφαρμογή της επέκτασης του Ευκλείδειου αλγόριθμου για την προσέγγιση Padé. Για τυχαίο διάνυσμα b, $mu_{A^i b} = \mu_A$.

Έστω πίνακας A. Αν διαλέξω τυχαίο τριγωνικό πίνακα B με μη-μηδενική ορίζουσα, τότε με μεγάλη πιθανότητα το χαρακτηριστικό κι ελάχιστο πολυώνυμο του AB ταυτίζονται. Από το πολυώνυμο αυτό υπολογίζω την ορίζουσα του AB και συνεπώς την ορίζουσα του A, σε χρόνο $O_A(N)\Delta(N)$.

Για αυθαίρετους πίνακες αυτή η πολυπλοκότητα είναι $O(N^3)$, αλλά για αραιούς και δομημένους πίνακες είναι πολύ μικρότερη: Αν υπάρχουν k μη-μηδενικά στοιχεία ανά γραμμή, τότε $\Delta(N) = O_A(Nk)$, το οποίο συχνά είναι στο $o(N^2)$ άρα κι η ορίζουσα στο $o(N^3)$. Για πίνακες Vandermonde, Toeplitz κλπ, έχουμε $\Delta(N)$ στο $O_A(N \log^2 N), O_A(N \log N)$ αντίστοιχα.

Πέρα απ' την ορίζουσα, πολλά άλλα προβλήματα γραμμικής άλγεβρας ανάγονται σε πολλαπλασιασμούς πίνακα επί διάνυσμα με βάση τα παραπάνω. Το αρχικό παράδειγμα του Wiedemann ήταν η επίλυση του συστήματος $Ax = b \in F^N$, μέσω του υπολογισμού του ελάχιστου πολυωνύμου μ της ακολουθίας $A^i b$, για αντιστρέψιμο πίνακα A. Έστω νέο πολυώνυμο $T(x) := -[\mu(x) - \mu_0]/(x\mu_0)$. Η λύση του συστήματος είναι το διάνυσμα $T(A)b$.

4.6 Στοιχεία θεωρίας αριθμών

Λήμμα 4.6.1 *Αν $a, b, p \in \mathbb{Z},\ p$ πρώτος τότε $(a+b)^p \equiv a^p + b^p \bmod p$.*

Απόδειξη. $p \mid \binom{p}{i}$ για όλα τα $i = 1, \dots, p-1$ και $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}$. ΟΕΔ

Μια άμεση συνέπεια είναι πως $(a+b)^{p^k} \equiv a^{p^k} + b^{p^k} \bmod p$, για $i \in \mathbb{N}$, το οποίο αποδεικνύεται επαγωγικά ως προς k.

Λήμμα 4.6.2 *Αν $a, m \in R$, όπου R μια Ευκλείδεια περιοχή, τότε το a είναι αντιστρέψιμο* mod$m$ *αν ο ΜΚΔ είναι $(a, m) = 1$.*

Απόδειξη. Η αντιστρεψιμότητα σημαίνει πως $\exists\ s \in \mathbb{Z} : as \equiv 1 \bmod m \Leftrightarrow \exists\ s, t \in \mathbb{Z} : as + tm = 1 \Leftrightarrow (a, m) = 1$. ΟΕΔ

Θεώρημα 4.6.3 (Μικρό θεώρημα Fermat) *Αν $a, p \in \mathbb{Z},\ p$ πρώτος τότε $a^p \equiv a \bmod p$. Αν επιπλέον $p \not| a$ τότε $a^{p-1} \equiv 1 \bmod p$.*

Απόδειξη. Χρησιμοποιώ επαγωγή στο $a \in \mathbb{Z}_p = \{0, \ldots, p-1\}$. Η βάση $a = 0$ είναι προφανής. Για το βήμα, $a^p = [(a-1)+1]^p \equiv (a-1)^p + 1^p \bmod p$, από το λήμμα 4.6.1. Από την επαγωγική υπόθεση, $a^p \equiv (a-1) + 1 = a \bmod p$.

Η δεύτερη πρόταση είναι άμεση συνέπεια της πρώτης κατόπιν εφαρμογής του λήμματος 4.6.2. ΟΕΔ

Θεώρημα 4.6.4 [Agrawal-Kayal-Saxena'02] *Αν $a, p \in \mathbb{Z}$, $(a,p) = 1$, τότε ο p είναι πρώτος αν και μόνο αν $(x-a)^p \equiv x^p - a \bmod p$.*

Απόδειξη. Αν ο p είναι πρώτος τότε $p \mid \binom{p}{i}$, $i = 1, \ldots, p \Rightarrow (x-a)^p \equiv x^p - a^p \bmod p$ και το αποτέλεσμα προκύπτει από το μικρό θεώρημα του Fermat.

Αντίστροφα, έστω πως υπάρχει πρώτος $q \mid p$ και μάλιστα έστω k η μεγαλύτερη δύναμή του τ.ώ. $q^k \mid p$. Τότε $q^k \not| \binom{p}{q}$, επίσης $(q^k, a^{p-q}) = 1$ διότι αλλιώς το $q|a \Rightarrow (a,p) > 1$. Συνεπώς ο όρος $\binom{p}{q} x^q a^{p-q}$ στο ανάπτυγμα του $(x-a)^p$ δε μηδενίζεται, ενώ δεν εμφανίζεται στο δεξιό μέλος, άρα η εξίσωση πολυωνύμων δεν ισχύει. ΟΕΔ

Το πόρισμα που συνάγεται είναι πως αν ο p είναι πρώτος τότε $(x-a)^p \equiv x^p - a \bmod (x^r - 1) \bmod p$, για κάθε ακέραιο $r < p$.

Πρόταση 4.6.5 [Chebychev] *Το σύνολο των πρώτων αριθμών που είναι μικρότεροι ή ίσοι με το $2k$, για κάποιο $k \in \mathbb{N}$, έχουν γινόμενο $\geq 2^k$.*

Μπορούμε τώρα να δώσουμε την γενική μορφή του πολυωνυμικού αλγορίθμου 4.6 των Agrawal-Kayal-Saxena'02 για αναγνώριση πρώτων αριθμών, όπως διαμορφώθηκε σε συνεργασία με τον Lenstra.

Algorithm 1 Αναγνώριση πρώτων αριθμών με πολυωνυμική πολυπλοκότητα

Η είσοδος είναι ακέραιος $n > 0$.
Η έξοδος θα είναι η απάντηση " Πρώτος " ή " Όχι πρώτος ".
Τα βήματα του αλγορίθμου είναι τα εξής.

1: Ελέγχουμε αν υπάρχει $t \in \mathbb{Z}, k \in \{1, \ldots, \lceil \lg n \rceil\}$ τ.ώ. $t^k = n$, δηλ. αν το n είναι τέλεια δύναμη. Αν ναι, τότε ο αλγόριθμος επιστρέφει " Όχι πρώτος " και τερματίζει.
2: Έστω $N := 2n(n-1)(n^2-1)\cdots(n^{4\lceil \lg n \rceil^2} - 1)$ και r ο ελάχιστος πρώτος που δεν διαιρεί το N. Παρατηρώ πως υπάρχει $k = O(\lg^5 n)$: $N \leq 2^k$. Από την πρόταση 4.6.5 συνάγεται πως οι πρώτοι που είναι $\leq 2k$ έχουν γινόμενο $> N$. Άρα υπάρχει τουλάχιστον ένας που δεν διαιρεί το N συνεπώς $r = O(\lg^5 n)$.
3: Αν ο n είναι πρώτος $< r$ ο αλγόριθμος επιστρέφει " Πρώτος ", ενώ αν υπάρχει πρώτος $< r$ που διαιρεί το n τότε επιστρέφει " Όχι πρώτος ".
4: Για κάθε $b \in \{1, \ldots, r\}$, ελέγχω αν $(x+b)^n \equiv x^n + b \bmod n \bmod (x^r - 1)$. Αν υπάρχει b όπου δεν ισχύει η ταυτότητα πολυωνύμων, τότε ο αλγόριθμος επιστρέφει " Όχι πρώτος ".
5: Αν φτάσουμε σ' αυτό το στάδιο, ο n είναι δύναμη πρώτου κι αφού δεν είναι τέλεια δύναμη (από το 1ο στάδιο) τότε ο αλγόριθμος επιστρέφει " Πρώτος ".

Η ορθότητα του αλγορίθμου αποδεικνύεται εύκολα, εκτός από το τελευταίο βήμα, όπου πρέπει να εφαρμοστεί η παρακάτω πρόταση 4.6.8. Αυτή ήταν και η τεχνική με την οποία μειώθηκε η πολυπλοκότητα σε $O(\log^6 n)$, από το αρχικό φράγμα των Agrawal-Kayal-Saxena.

Ας αναφερθούμε συνοπτικά στην πολυπλοκότητα για να διαπιστώσουμε πως είναι πολυωνυμικού κόστους, και ειδικότερα στο $O(\log^6 n)$. Το κόστος του 2ου βήματος 2 είναι στο $O_B(\lg^5 n)$. Το 3ο βήμα απαιτεί r

ελέγχους πολυωνυμικού κόστους. Στο 4ο βήμα, γίνονται r έλεγχοι $\bmod (x^r - 1)$, δηλαδή πολυωνυμικού κόστους. Η ολοκλήρωση της απόδειξης της πολυωνυμικής πολυπλοκότητας αφήνεται ως άσκηση.

Για την απόδειξη της πρότασης 4.6.8 απαιτούνται ορισμένα πιο προχωρημένα εργαλεία της υπολογιστικής θεωρίας αριθμών. Το βασικότερο είναι η συνάρτηση Euler. Στον δακτύλιο $\mathbb{Z}_m$, για οποιονδήποτε ακέραιο m, το πλήθος των στοιχείων $\{a \ : \ (a,m) = 1\} \subset \mathbb{Z}_m$ συμβολίζεται $\phi(m)$ και καλείται συνάρτηση του Euler (totient function).

Άσκηση 4.6.6 1. Αν p πρώτος $\Rightarrow \phi(p) = p - 1$ και $\phi(p^k) = p^k - p^{k-1}$.

2. Αν $n_1, \ldots, n_k \in \mathbb{N}^*$, $(n_i, n_j) = 1 \ \forall i \neq j \Rightarrow \phi(n_1 \cdots n_k) = \phi(n_1) \cdots \phi(n_k)$.

3. Έστω οι πρώτοι $p_1, \ldots, p_k$ διαιρέτες του $n \in NN^*$, τότε $\phi(n) = n(1 - 1/p_1) \cdots \phi(1 - 1/p_k)$.

Πρόταση 4.6.7 [Euler] $n \in \mathbb{N}^*, a \in \mathbb{Z}, (a,n) = 1 \Rightarrow n | a^{\phi(n)} - 1$.

Πρόταση 4.6.8 [Agrawal-Kayal-Saxena-Lenstra'02] *Έστω* $(n,r) = 1$, $(n, b - b') = 1 \ \forall b \neq b' \in S \subset \mathbb{Z}$ *και* $((x+b)^n \equiv x^n + b \bmod n \bmod (x^r - 1) \ \forall b \in S$. *Θέτουμε* $v := \min\{k : n^k \equiv 1 \bmod r\}$. *Αν,*

$$d | \phi(r)/v \Rightarrow \binom{|S| + \phi(r) - 1}{|S|} \geq n^{2d\lfloor\sqrt{\phi(r)}/d\rfloor},$$

τότε το n *είναι δύναμη πρώτου.*

Κεφάλαιο 5

Επίλυση στους πραγματικούς

Το κεφάλαιο αυτό πραγματεύεται την εύρεση όλων των πραγματικών λύσεων μιας πολυωνυμικής εξίσωσης ή συστήματος εξισώσεων. Το πρόβλημα αυτό συναντά πλειάδα εφαρμογών σε τομείς όπως η υπολογιστική γεωμετρία, ο σχεδιασμός με υπολογιστή, η ρομποτική κοκ.

Σημειώνουμε τη μεγάλη αριθμητική αστάθεια (μεγαλύτερη από τις μιγαδικές ρίζες) των πραγματικών ριζών σε συνάρτηση μιας μεταβολής στους συντελεστές. Π.χ. το πολυώνυμο του Wilkinson $p(x) = (x+1)(x+2)\cdots(x+20) = x^{20} + 210x^{19} + \cdots + 20!$ έχει 20 πραγματικές ρίζες ενώ το $p(x) + 2^{-32}x^{19}$ έχει μόνο 10 πραγματικές ρίζες και οι υπόλοιπες μιγαδικές έχουν φανταστικό μέρος απόλυτης τιμής > 0.8. Σήμερα μόνο με αλγεβρικές μεθόδους (δηλ. συμβολική επεξεργασία) μπορεί να λυθεί ικανοποιητικά αυτό το πρόβλημα.

Το βασικό πρόβλημα που εξετάζεται στο κεφάλαιο είναι η απομόνωση όλων των πραγματικών ριζών μιας εξίσωσης σε διαστήματα με ρητά άκρα, έτσι ώστε κάθε διάστημα να περιέχει μια ρίζα και όλες οι ρίζες να βρίσκονται σε κάποιο διάστημα. Τα διαστήματα αυτά καλούνται « διαστήματα απομόνωσης ». Υπάρχουν οι εξής κατηγορίες αλγορίθμων ακριβείας για το πρόβλημα αυτό:

- Οι αλγόριθμοι υποδιαίρεσης, που υποδιαιρούν ένα αρχικό διάστημα σε μικρότερα, έως ότου αυτά περιέχουν μία ή καμία ρίζα. Οι αλγόριθμοι αυτοί διακρίνονται από τον τρόπο που μετρούν ρίζες σε ένα διαστήμα και πρόκειται κυρίως για τις μεθόδους Sturm και Descartes. Θα μελετηθούν στην ενότητα 5.2 και 5.3.
- Ο αλγόριθμος των συνεχών κλασμάτων (continued fractions) που στηρίζεται στην προσέγγιση των πραγματικών αριθμών από ένα συνεχές κλάσμα με ακέραιους συντελεστές [Akr89, Tsi06]. Π.χ.

$$\frac{2}{3} = 0 + \frac{1}{1+\frac{1}{2}}, \qquad \sqrt{2} = 1.41421\cdots = 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{2+\cdots}}}.$$

- Τέλος, υπάρχουν μέθοδοι που βασίζονται στην αριθμητική διαστημάτων [Moo66, Mer00], Rump.

5.1 Πραγματικά σώματα

Γενική βιβλιογραφία: [DST88, pp.105-11], [BPR03, Mis93] [Yap00, lect.VII].

Ξεκινάμε με στοιχεία από την θεωρία πραγματικών σωμάτων [Mis93]. Μας ενδιαφέρει να μελετήσουμε σώματα που συμπεριφέρονται όπως οι πραγματικοί, δηλ. στα οποία ορίζονται οι ανισώσεις και διαστήματα, σε αντίθεση με τους μιγαδικούς αριθμούς.

Ορισμός 5.1.1 *Ένα σώμα (field) K καλείται* διατεταγμένο *όταν περιέχει ένα υποσύνολο θετικών αριθμών R, κλειστό ως προς τις 2 πράξεις $(*, +)$, τέτοιο ώστε για κάθε στοιχείο $x \in K, x \neq 0$, είτε $x \in R$ είτε $-x \in R$.*

Π.χ. $\mathbb{R}, \mathbb{Q}, \mathbb{R}(\epsilon), \mathbb{Q}(\epsilon)$ και $\mathbb{Q}(\sqrt[3]{2}) \equiv \mathbb{Q}[x]/\langle x^3 - 2\rangle$. Αντίθετα, το $\mathbb{C}$ δεν είναι διατεταγμένο. Σημειώστε πως το $0 < \epsilon \ll 1$ είναι ένας απειροελάχιστος (infinitesimal) θετικός δηλ. μπορούμε να θεωρήσουμε πως $\epsilon \to 0^+$. Το $1/\epsilon$, που ανήκει στο $\mathbb{R}(\epsilon)$, τείνει στο άπειρο. Θυμίζουμε πως ένας δακτύλιος $K(x)$ περιέχει όλες τις ρητές εκφράσεις ως προς x με συντελεστές στο K, δηλ. όλα τα κλάσματα με αριθμητή στο $K[x]$ και παρονομαστή στο $K[x] \setminus \{0\}$.

Τα διατεταγμένα σώματα είναι αναγκαστικά άπειρα και μας παρέχουν την δυνατότητα να μελετήσουμε ανισότητες και διαστήματα. Δηλ. $a > b \Leftrightarrow a - b \in R$. Επίσης, $a > b \Rightarrow a + c > b + c, \forall c$, ενώ $a > b \Rightarrow ac > bc$, $\forall c \in R$.

Η βασική έννοια ορίζεται ευθύς αμέσως και μελετά σώματα που, χωρίς να είναι απαραίτητα αλγεβρικά κλειστά, είναι κλειστά ως προς την ύπαρξη των πραγματικών ριζών.

Ορισμός 5.1.2 *Ένα σώμα K καλείται* κλειστό πραγματικό *όταν είναι διατεταγμένο, κάθε θετικός έχει μια θετική τετραγωνική ρίζα, και κάθε εξίσωση περιττού βαθμού στο $K[x]$ έχει μια ρίζα στο K.*

Π.χ. $\mathbb{R}, \mathbb{R}(\epsilon), \mathbb{R}(\epsilon_1, \epsilon_2)$, αλλά όχι το $\mathbb{Q}$ ούτε η αλγεβρική θήκη $\overline{\mathbb{Q}}$, ούτε το $\mathbb{Q}(\sqrt[3]{2})$. Θυμηθείτε πως το $\overline{\mathbb{Q}}$ περιέχει όλες τις ρίζες πολυωνύμων στο $\mathbb{Q}[x]$.

Από τους ορισμούς προκύπτει πως για κάθε $p(x) \in K[x]$, όπου το K κλειστό πραγματικό, που είναι μη-παραγοντοποιήσιμο (ανάγωγο) και μονικό (με μοναδιαίο μεγιστοβάθμιο συντελεστή) έπεται πως $\deg p \in \{1, 2\}$. Ειδικότερα, ένα δευτεροβάθμιο πολυώνυμο είναι ανάγωγο ανν η διακρίνουσα είναι αρνητική.

Λήμμα 5.1.3 *Το K είναι κλειστό πραγματικό ανν είναι διατεταγμένο και το $K(\sqrt{-1})$ είναι αλγεβρικά κλειστό.*

Απόδειξη. Άσκηση. ΟΕΔ

Θεώρημα 5.1.4 (Μέσης τιμής, Bolzano) *Έστω K ένα κλειστό πραγματικό σώμα, $p \in K[x]$, $a < b \in K$ και $p(a)p(b) < 0$. Τότε υπάρχει $c \in (a, b) : p(c) = 0$.*

Ένα πολυώνυμο $p(x)$ είναι *χωρίς τετράγωνα* εάν δεν έχει πολλαπλές ρίζες δηλ. εάν η παραγοντοποίησή του σε γραμμικά πολυώνυμα ($\in \mathbb{C}[x]$ ή, γενικότερα, ως προς την αλγεβρική θήκη του σώματος των συντελεστών) δεν περιλαμβάνει κανέναν παράγοντα υψωμένο σε δύναμη. Κάθε παράγων υψωμένος σε δύναμη $k > 1$ στο $p(x)$ εμφανίζεται στην δύναμη $k-1$ στην παράγωγο $p'(x)$. Για κάθε $p(x)$, το πολυώνυμο $p(x)/\gcd(p(x), p'(x))$ είναι χωρίς τετράγωνα και με το ίδιο σύνολο ριζών όπως το $p(x)$.

Έστω μια ακολουθία τιμών $(t_1, \ldots, t_k)$. Ορίζουμε ως το *πλήθος μεταβολών προσήμου* το πλήθος μεταβολών στην ακολουθία μη-μηδενικών προσήμων. Π.χ. πλήθος μεταβολών της $[-, +, +, -] = 2$, πλήθος μεταβολών της $[+, 0, +, -] = 1$.

Άσκηση 5.1.5 Δείξτε με αντιπαράδειγμα πως δεν ισχύει πάντα το αντίστροφο στο Θεώρημα Μέσης τιμής.

5.2 Ακολουθίες Sturm

Έστω $a \in \mathbb{R} \cup \{-\infty, +\infty\}$ και μια ακολουθία πολυωνύμων $(p_1, \dots, p_k)$. Ορίζουμε ως το *πλήθος μεταβολών προσήμου* της ακολουθίας στο σημείο a, και το συμβολίζουμε $V(a)$, το πλήθος μεταβολών προσήμου στην ακολουθία των τιμών $[p_1(a), \dots, p_k(a)]$, όπου $p(\pm\infty) = \lim_{x\to\pm\infty} p(x)$.

Στην συνέχεια μελετάμε ακολουθίες πολυωνύμων πάνω σε πραγματικά διαστήματα.

Ορισμός 5.2.1 *Μια* ακολουθία Sturm *ενός πολυωνύμου $p \in K[x]$ στο $[a,b] \subset K \cup \{-\infty, +\infty\}$, όπου K κλειστό πραγματικό, είναι μια ακολουθία $(p_1, p_2, \dots, p_k)$ με $p_1 = p$ εάν:*

1. $p(a)p(b) \neq 0$,
2. $\forall c \in [a,b], p_k(c) \neq 0$,
3. $\forall c \in [a,b] : p_j(c) = 0 \Rightarrow p_{j-1}(c)p_{j+1}(c) < 0$,
4. $\forall c \in [a,b] : p_1(c) = 0 \Rightarrow$ *υπάρχουν διαστήματα* $[c_1, c), (c, c_2]$ *τέτοια ώστε:* $u_1 \in [c_1, c) \Rightarrow p_1(u_1)p_2(u_1) < 0$ *και* $u_2 \in (c, c_2] \Rightarrow p_1(u_2)p_2(u_2) > 0$.

Η πρώτη συνθήκη δεν είναι ιδιαίτερα σημαντική και με λίγη προσοχή αναιρείται. Η δεύτερη και η 4η περιγράφουν την συμπεριφορά της ακολουθίας στην αρχή και το τέλος της. Η 3η συνθήκη περιγράφει την συμπεριφορά των ενδιάμεσων πολυωνύμων και, εφαρμοσμένη για $j = 2$, σημαίνει πως δεν υπάρχουν κοινές ρίζες των $p = p_1, p_2$ στο $[a,b]$.

Το επόμενο θεώρημα δείχνει πως ο παραπάνω ορισμός δεν είναι κενός, δηλ. υπάρχει τουλάχιστον μια ακολουθία Sturm. Το θεώρημα ορίζει έτσι την απλή / κανονική ακολουθία Sturm.

Θεώρημα 5.2.2 (Ύπαρξη ακολουθίας Sturm) *Έστω μια ακολουθία $(p_1, p_2, \dots, p_k)$ με $p_1 = p \in K[x]$ ένα πολυώνυμο χωρίς τετράγωνα και K κλειστό πραγματικό, $p_2 = p'$ (παράγωγος) και*

$$p_i = -(p_{i-2} \bmod p_{i-1}), \quad i = 3, \dots, k,$$

όπου k ο ελάχιστος ακέραιος για τον οποίο $p_{k-1} \bmod p_k = 0$. Η ακολουθία (p_i) είναι ακολουθία Sturm σε διάστημα $[a,b]$ όπου $p(a)p(b) \neq 0$ και καλείται απλή / κανονική ακολουθία Sturm.

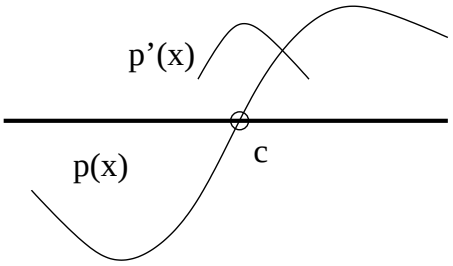
Απόδειξη. (1) Κατ' επιλογή τα a, b δεν είναι ρίζες του p.

(2) $\text{ΜΚΔ}(p, p') =$ μη μηδενική σταθερά διότι το p δεν έχει τετράγωνα. Το p_k είναι πολλαπλάσιο του $\text{ΜΚΔ}(p, p')$ επί μια μη μηδενική σταθερά άρα $p_k =$ σταθερά.

(3) $\exists q_i \in K[x] : p_{i-1} = p_i q_i - p_{i+1} \Rightarrow p_{i-1}(c) = 0 - p_{i+1}(c)$. Εάν $p_{i-1}(c) = 0$ ή $p_{i+1}(c) = 0$ τότε $\forall j > i-2, p_j(c) = 0$: άτοπο για $j = k$.

(4) Για c τέτοιο ώστε $p(c) = 0$ έχουμε $p'(c) \neq 0$ (διότι p χωρίς τετράγωνα) άρα υπάρχει διάστημα (c_1, c_2) που περιέχει το c όπου το p' έχει σταθερό πρόσημο ενώ το p αλλάζει πρόσημο στο c, δεδομένου ότι πρόκειται για απλή ρίζα. Το σχήμα 5.1 δείχνει την περίπτωση όπου $p'(c) > 0$ και $p(u_1) < 0 < p(u_2)$. Αντίστοιχο σκεπτικό ισχύει όταν $p'(c) < 0$, οπότε θα είχαμε $p(u_1) > 0 > p(u_2)$. ΟΕΔ

Πόρισμα 5.2.3 *Κάθε ακολουθία $(p_i) = (p, p', \dots)$ όπου $a_i p_i = b_i p_{i-2} + p_{i-1} q_{i+1}$ για $a_i, b_i \in K$, $a_i b_i < 0$, όπου το $p(x) \in K[x]$ είναι χωρίς τετράγωνα και το K κλειστό πραγματικό, είναι ακολουθία Sturm στο $[a,b]$ όπου $p(a)p(b) \neq 0$.*



Σχήμα 5.1: Μια περίπτωση συμπεριφοράς των p, p'.

Απόδειξη. Όπως παραπάνω: άσκηση. ΟΕΔ

Λήμμα 5.2.4 *Μία ακολουθία προσήμων $(\sigma, \tau, -\sigma)$ έχει μία αλλαγή προσήμου για κάθε $\sigma, \tau \in \{+, -\}$.*

Είμαστε τώρα έτοιμοι να διατυπώσουμε το βασικό θεώρημα της ενότητας, που θα μας επιτρέψει να μετράμε τις διαφορετικές πραγματικές ρίζες ενός πολυωνύμου σε ένα διάστημα, χωρίς όμως να υπολογίζουμε τις πολλαπλότητές τους.

Θεώρημα 5.2.5 (Sturm) *Έστω μια ακολουθία Sturm $(p_i) = (p_1, \ldots, p_k)$ στο $[a, b] \subset K \cup \{-\infty, +\infty\}$, όπου $p = p_1 \in K[x]$ και K κλειστό πραγματικό. Έστω $V(c)$ το πλήθος μεταβολών προσήμου της $(p_i(c))$, για $c \in K \cup \{-\infty, +\infty\}$, όπου ως τιμή πολυωνύμου στο $\pm\infty$ εκλαμβάνεται το όριό του. Τότε το πλήθος των διαφορετικών πραγματικών ριζών του $p_1(x)$ στο $[a, b]$ ισούται με $V(a) - V(b)$.*

Απόδειξη. Έστω $a_1 < \cdots < a_m$ οι ρίζες $\in (a, b)$ ΌΛΩΝ των πολυωνύμων στην (p_i). Θα αποδείξουμε επαγωγικά πως $V(a) - V(c_i) =$ πλήθος πραγματικών ριζών στο (a, c_i) για τυχαίο $c_i \in (a_i, a_{i+1})$ σε κάθε $i = 0, \ldots, m$, όπου $a_0 = a, a_{m+1} = b$.

Η βάση της επαγωγής για $c_0 \in (a_0, a_1)$: δεν υπάρχει καμία ρίζα άρα, από το θεώρημα μέση τιμής του Bolzano, δεν υπάρχει καμία αλλαγή προσήμου, δηλ. $V(a) - V(c_0) = 0$. Ακόμη κι αν $\exists i \in (1, k) : p_i(a) = 0$, η ισότητα ισχύει διότι $p_{i-1}(a)p_{i+1}(a) < 0$. Επομένως οι ακολουθίες προσήμου είναι $[\cdots, \sigma, 0, -\sigma, \cdots]$ και $[\cdots, \sigma, \tau, -\sigma, \cdots]$, δηλ. έχουν κι οι δύο μία μεταβολή προσήμου, για $\sigma, \tau \in \{+, -\}$.

Επαγωγικό βήμα: Υποθέτοντας $V(a) - V(c_i) =$πλήθος ριζών $\in (a, c_i)$ θα το αποδείξουμε για c_{i+1} όπου $c_i < a_{i+1} < c_{i+1} < a_{i+2}$. Διακρίνουμε 2 περιπτώσεις ανάλογα με το αν $p(a_{i+1}) \neq 0$ ή $p(a_{i+1}) = 0$.

1. Αφού $p(a_{i+1}) \neq 0$, τότε $p_j(a_{i+1}) = 0,\ j \in (1, k)$. Χάριν της ιδιότητας (3) των ακολουθιών Sturm, $p_{j+1}(a_{i+1})p_{j-1}(a_{i+1}) < 0$, συνεπώς έχουμε τις ακολουθίες προσήμων

$$\begin{aligned} [p_{j-1}(c_i), p_j(c_i), p_{j+1}(c_i)] &= [\sigma, \tau_0, -\sigma], \\ [p_{j-1}(a_{i+1}), p_j(a_{i+1}), p_{j+1}(a_{i+1})] &= [\sigma, 0, -\sigma], \\ [p_{j-1}(c_{i+1}), p_j(c_{i+1}), p_{j+1}(c_{i+1})] &= [\sigma, \tau_1, -\sigma], \end{aligned}$$

   για $\sigma, \tau_0, \tau_1 \in \{+, -\}$. Σύμφωνα με το λήμμα 5.2.4, υπάρχει μια αλλαγή προσήμου σε καθεμιά από τις 3 ακολουθίες. Άρα, αν μόνο το p_j μηδενίζεται στο c_i, έχουμε $V(c_{i+1}) = V(c_i)$. Αν υπάρχει κι άλλο πολυώνυμο που μηδενίζεται στο a_{i+1} το ίδιο επιχείρημα δείχνει πως τελικά $V(c_{i+1}) = V(c_i)$.

2. $p(a_{i+1}) = 0 \Rightarrow$ χάριν της ιδιότητας (4) των ακολουθιών Sturm τα p_1, p_2 έχουν διαφορετικό πρόσημο στο c_i και ίδιο στο c_{i+1}. Έχουμε $p_2(a_{i+1}) \neq 0$, άρα το p_2 δεν αλλάζει πρόσημο στο ανοιχτό διάστημα

(c_i, c_{i+1}), λόγω Bolzano. Από την συνθήκη (4), οι ακολουθίες προσήμων των $(p, p_2, \dots)$ στα c_i και c_{i+1} είναι, αντίστοιχα:

$$[-\sigma, \sigma, s], \quad [\sigma, \sigma, s'],$$

όπου $\sigma \in \{+, -\}$ και s, s' υπακολουθίες προσήμων τέτοιες ώστε $V(\sigma, s) = V(\sigma, s')$, όπως αποδείξαμε για την 1η περίπτωση παραπάνω. Σημειώστε πως αν $p_j(a_{i+1}) = 0$ για $j > 2$ τότε $s \neq s'$, όπως στην 1η περίπτωση: όμως και πάλι $V(\sigma, s) = V(\sigma, s')$. Συνεπώς, $V(c_{i+1}) = V(c_i) - 1$.

ΟΕΔ

Η απόδειξη του επαγωγικού βήματος απλοποιείται για απλές ακολουθίες διότι για κάθε $i < j < k$, υπάρχουν $s(x), t(x)$: $p_k(x) = s(x)p_i(x) + t(x)p_j(x)$, όπως στον Ευκλείδειο αλγόριθμο του ΜΚΔ (το οποίο αφήνεται σαν άσκηση στον αναγνώστη). Άρα $p_i(a) = p_j(a) = 0 \Rightarrow p_k(a) = 0$, το οποίο είναι άτοπο. Άρα δεν υπάρχουν δύο πολυώνυμα που μηδενίζονται στο a.

Θεώρημα 5.2.6 *Το θεώρημα 5.2.5 ισχύει για την ακολουθία $(p, p', p_3, \dots, p_k)$ όπου $p_i = -(p_{i-2} \bmod p_{i-1})$, $i \geq 3$, $p_k = \gcd(p, p')$ και το $p(x)$ μπορεί να έχει πολλαπλές ρίζες στο διάστημα $[a, b]$, όπου $p(a)p(b) \neq 0$.*

Απόδειξη. Άσκηση. ΟΕΔ

Το παρακάτω θεώρημα είναι ιστορικά προγενέστερο, καθότι οι Budan, Fourier δεν χρησιμοποιούσαν ακολουθίες υπολοίπων, αλλά παραγώγων.

Θεώρημα 5.2.7 (Budan-Fourier) *Έστω η ακολουθία $(p = p_0, p_1, \dots, p_d)$, με $p \in K[x]$, το οποίο δύναται να έχει πολλαπλές ρίζες, όπου $p_i = p^{(i)}$ η i-οστή παράγωγος και διάστημα $[a, b]$ τ.ώ. $p(a)p(b) \neq 0$. Αποδείξτε πως $V(a) - V(b)$ ισούται με το άθροισμα του πλήθους των διαφορετικών πραγματικών ριζών του $p(x)$ στο $[a, b]$ συν κάποιον άρτιο φυσικό αριθμό.*

Απόδειξη. Ακολουθούμε την απόδειξη του θεωρήματος του Sturm. Παρατηρείστε πως η ακολουθία ικανοποιεί τις συνθήκες (1) και (2) μιας ακολουθίας Sturm.

Αποδεικνύουμε πως ισχύει η συνθήκη (4): προφανές αν το p είναι χωρίς τετράγωνα. Αλλιώς, αν η πολλαπλότητα της $p(c) = 0$ είναι περιττός, τότε $p'(c) = 0$ με πολλαπλότητα ίση με άρτιο αριθμό και τα πρόσημα πριν και μετά το c είναι

$$[-, +], [+, +] \text{ ή } [+, -], [-, -].$$

Αν η πολλαπλότητα είναι άρτιος, τότε η πολλαπλότητα της $p'(c) = 0$ είναι περιττός και τα πρόσημα γίνονται

$$[-, -], [+, -] \text{ ή } [+, +], [-, +].$$

Οπότε η (4) ισχύει σε όλες τις περιπτώσεις.

Επικεντρώνουμε την προσοχή μας στην συνθήκη (3) και σε μια ρίζα c κάποιου πολυωνύμου στην ακολουθία. Η συνθήκη (3) ικανοποιείται αν η $p_j(c) = 0$ είναι απλή, οπότε το πλήθος αλλαγών προσήμου δεν αλλάζει.

Αν η πολλαπλότητα της $p_j(c) = 0$ ισούται με περιττό > 1, τότε η πολλαπλότητα της $p_{j+1}(c) = p'_j(c) = 0$ είναι άρτιος, άρα το p_{j+1} δεν αλλάζει πρόσημο στο c και, επιπλέον, έχει διαφορετικό πρόσημο από το p_j πριν το c. Το p_j αλλάζει από αρνητικό σε θετικό ή από θετικό σε αρνητικό στο c, οπότε το p_{j-1} παρουσιάζει ελάχιστο στο c ή, αντίστοιχα, παρουσιάζει μέγιστο. Τα πρόσημα των 3 πολυωνύμων πριν και μετά το c είναι

$$[-\tau, \tau, -\tau], [-\tau, -\tau, -\tau], \quad \tau \in \{+, -\}.$$

οπότε οι αλλαγές προσήμων αυξάνονται κατά 2. Αυτό οδηγεί το $V(a)-V(b)$ στο να υπερβαίνει το πλήθος πραγματικών ριζών κατά έναν άρτιο φυσικό αριθμό.

Αντίστοιχη ανάλυση αν η πολλαπλότητα είναι άρτιος. Η ολοκλήρωση της απόδειξης αφήνεται ως άσκηση. ΟΕΔ

Θεώρημα 5.2.8 (Milne) *θεωρήστε μια ακολουθία Sturm ενός πολυωνύμου $p(x)$. Αποδείξτε πως*

1. *$V(\infty)+V(-\infty)=l-1$, όπου l το μήκος της ακολουθίας,*
2. *αν πρόκειται για απλή ακολουθία μήκους $d+1$, όπου $d=\deg p$, τότε το $V(\infty)$ ισούται με το πλήθος των ζευγών μιγαδικών ριζών του p.*

Παράδειγμα 5.2.9 Έστω $p=p_1=x^2+x+1, p_2=2x+1, p_3=-3/4$ μια απλή ακολουθία Sturm. Οι ακολουθίες προσήμων στο $\pm\infty$ είναι $[+,-,-],[+,+,-]$. Το θεώρημα Sturm δηλώνει πως υπάρχουν $1-1=0$ πραγματικές ρίζες. Το αποτέλεσμα του Milne ισχύει γιατί $1+1=2=l-1$, όπου $l=3$ το μήκος της ακολουθίας, ενώ υπάρχει όντως ένα ζεύγος μιγαδικών ριζών. □

Στόχος είναι η απομόνωση όλων των ριζών δηλ. ο υπολογισμός ρητών διαστημάτων που καθένα περιέχει μια μοναδική ρίζα. Περιορίζουμε το διάστημα όπου βρίσκονται οι (πραγματικές) ρίζες του $p(x)$ χρησιμοποιώντας το θεώρημα 5.2.10 και το πόρισμά του. Το θεώρημα αφορά σε όλες τις ρίζες, ακόμη κι αν αυτές είναι μιγαδικές.

Θεώρημα 5.2.10 *Κάθε ρίζα α του $p(x)=x^n+\cdots+c_0$, που είναι μονικό (δηλ. με μοναδιαίο μεγιστοβάθμιο συντελεστή $c_n=1$), φράσσεται ως εξής:*

$$\begin{aligned}
[\textit{Cauchy 1829}]: \quad |\alpha| &< 1+\max_{0\le i<n}\{|c_i|\}, \quad |\alpha|\le \max_{0\le i<n}\left\{|nc_i|^{\frac{1}{n-i}}\right\},\\
[\textit{Zassenhaus}]: \quad |\alpha| &\le 2\max_{0\le i<n}\left\{|c_i|^{\frac{1}{n-i}}\right\},\\
[\textit{Yap00, lect.VI}]: \quad |\alpha| &\le \frac{1}{\sqrt[n]{2}-1}\max_{0\le i<n}\left\{\left|\frac{\sqrt[n-i]{c_i}}{\binom{n}{n-i}}\right|\right\},\\
[\textit{Landau}]: \quad |\alpha| &\le \left(c_0^2+\cdots+c_{n-1}^2\right)^{1/2}.
\end{aligned}$$

Απόδειξη. Το 1ο φράγμα Cauchy θέτει ως άνω φράγμα το $1+\|(|c_0|,\ldots,|c_{n-1}|)\|_\infty$, όπου ο 2ος όρος είναι το μέτρο του διανύσματος $(c_0,\ldots,c_{n-1})$ στη μετρική L_∞. Αν $|\alpha|\le 1$, ισχύει τετριμμένα. Αλλιώς έχουμε

$$|\alpha|^n=|-c_{n-1}\alpha^{n-1}-\cdots-c_0|\le\max\{|c_i|\}(|\alpha|^{n-1}+\cdots+1)=\max\{|c_i|\}\frac{|\alpha|^n-1}{|\alpha|-1}<\frac{\max\{|c_i|\}|\alpha|^n}{|\alpha|-1},$$

που δίνει το φράγμα. Οι υπόλοιπες αποδείξεις αφήνονται ως άσκηση. Παρατηρήστε πως το φράγμα Landau είναι $\|(c_0,\ldots,c_{n-1})\|_2$, δηλ. το Ευκλείδειο μέτρο του διανύσματος $(c_0,\ldots,c_{n-1})$. ΟΕΔ

Όταν θεωρούμε μόνο τις θετικές ρίζες, μια βελτίωση του 2ου φράγματος του Cauchy υπάρχει στο [Kioustelidis], βλ. [Tsi06]:

$$\alpha\le 2\max_{0\le i<n,c_i<0}\left\{|c_i|^{\frac{1}{n-i}}\right\},$$

όπου το μέγιστο λαμβάνεται από όλους τους αρνητικούς συντελεστές. Επιπλέον φράγματα υπάρχουν στην βιβλιογραφία, βλ. π.χ. [Tsi06, Zip93].

Ορίζουμε το ανάστροφο πολυώνυμο $q(x) = x^n p(1/x)$ και εξετάζουμε τις μη-μηδενικές ρίζες. Έστω ανώτερο φράγμα φ στη μέγιστη ρίζα του $q(x)$, την οποία συμβολίζουμε με α, δηλ. $q(\alpha) = 0 = \alpha^n p(1/\alpha) \Rightarrow 1/\varphi$ αποτελεί κατώτερο φράγμα στην ελάχιστη ρίζα $(= 1/\alpha)$ του $p(x)$.

Πόρισμα 5.2.11

$$|\alpha| > \frac{|c_0|}{1 + \max_{1\le i\le n}\{|c_i|\}}, \quad |\alpha| \ge 1/\max_{1\le i\le n}\left\{\left|\tfrac{nc_i}{c_0}\right|^{\frac{1}{n-i}}\right\},$$
$$|\alpha| \ge \frac{1}{2}\max_{1\le i\le n}\left\{\left|\frac{c_i}{c_0}\right|^{\frac{1}{n-i}}\right\}, \quad |\alpha| \ge |c_0|/\left(c_1^2 + \cdots + c_n^2\right)^{1/2}.$$

Αφήνεται σαν άσκηση η «αναστροφή» του φράγματος του Yap.

Παράδειγμα 5.2.12 Δίνεται $p = x^3 + 2x - 3 = (x-1)(x + 1/2 + i\sqrt{11/2})(x + 1/2 - i\sqrt{11/2})$. Ακολουθία Sturm:

$$p_1 = p,\ p_2 = p' = 3x^2 + 2,\ p_3 = -(p_1 \mod p_2) = -(4/3)x + 3,\ p_4 = -(p_2 \mod p_3) = -275/16.$$

Ανώτατα όρια στις πραγματικές ρίζες: Cauchy: $1+\max\{2,3\} = 4,\ \max\{6^{1/2}, 9^{1/3}\} = \max\{2.45, 2.0801\} = 2.45$ (που είναι και το καλύτερο άνω φράγμα), Zassenhaus: $2 \cdot \max\{1.414, 1.4423\} = 2.8845$.

Ανώτατα όρια στις ρίζες του $q(x) = x^3 p(1/x)$: Cauchy: $1 + \max\{1/3, 2/3\} = 5/3, \max\{1,2\} = 2$. Zassenhaus: $2\max\{0.69, 2/3\} = 1.3867$. Επομένως το καλύτερο κατώτερο όριο που συνάγεται είναι $1/1.3867 = 0.7211$.

Αφήνεται σαν άσκηση η χρήση των φραγμάτων των Yap, Landau. Προκύπτει λοιπόν ο παρακάτω πίνακας, όπου μετά το αρχικό διάστημα $(0,3)$ επελέγησαν τα σημεία $3/2, 3/4, 9/8$ με αυτή τη σειρά. □

$a =$	0	3/4	**1**	9/8	3/2	3
$p_1(a)$	−	−	**0**	+	+	+
$p_2(a)$	+	+	+	+	+	+
$p_3(a)$	+	+	+	+	+	−
$p_4(a)$	−	−	−	−	−	−
$V(a) =$	2	2	**1**	1	1	1

Λήμμα 5.2.13 *Για την ελάχιστη απόσταση s (separation) οποιουδήποτε ζεύγους (μιγαδικών) ριζών ισχύει $-\log s = O(dC)$.*

Άσκηση 5.2.14 Αποδείξτε το λήμμα 5.2.13 πως $-\log s = O(dC)$.

Καλύτερα, η παρακάτω πρόταση φράσσει το γινόμενο των αποστάσεων μεταξύ ριζών χρησιμοποιώντας το μέτρο Mahler του $p(x)$:

$$M := |c_d| \prod_{i=1}^{d} \max\{1, |\gamma_i|\},$$

όπου γ_i όλες οι μιγαδικές ρίζες του $p(x)$. Έχει αποδειχθεί πως $M^2 \le c_0^2 + \cdots + c_d^2 \le 2^{2C}(d+1)$ [Landau'05], [Yap00, lect.IV].

Πρόταση 5.2.15 [Davenport'85-88, Mahler'64, Mignotte'95, Johnson'98] *Έστω πολυώνυμο* $p(x) \in \mathbb{Z}[x]$, *πιθανώς με πολλαπλές ρίζες. Θεωρούμε δύο σύνολα ριζών του* $\{a_1, \ldots, a_k\}, \{b_1, \ldots, b_k\} \subset \mathbb{C}$. *Αν* $|a_i| > |a_{i+1}|, |b_i| > |b_{i+1}|, |a_i| > |b_i|$ *και* M *το μέτρο Mahler του* $p(x)$, *τότε*

$$\prod_{i=1}^{k} |a_i - b_i| \geq M^{1-d} d^{-d/2} (\frac{\sqrt{3}}{d})^k.$$

Καθώς $M = O(C^{d+1})$, το παραπάνω γινόμενο Π φράσσεται ως εξής: $-\lg \Pi = O(d^2 C + d \log d)$. Η μέση απόσταση ριζών θα ήταν πιο χρήσιμη, αλλά αποτελεί ένα σύγχρονο ερώτημα ανεξάρτητου ενδιαφέροντος [EGT10].

Εξετάζουμε τώρα την πολυπλοκότητα του *αλγόριθμου υποδιαίρεσης* (subdivision) με βάση τις ακολουθίες Sturm, με σκοπό την απομόνωση όλων των ριζών, όπου C το μέγιστο δυαδικό μήκος συντελεστών του $p(x)$ και με $O^*(\cdot)$ δείχνουμε πως αγνοούμε πολυ-λογαριθμικούς παράγοντες ως προς τις παρούσες ποσότητες.

Η πρώτη ανάλυση του Heindel'71 ήταν $O(d^7 C^3)$, ενώ έγινε $O_B^*(d^6 C^3)$ στο [BCL82]. Η επιτάχυνση στον υπολογισμό μιας ακολουθίας Sturm (πρόταση 5.2.16) οδήγησε την χρονική πολυπλοκότητας στο $O_B^*(d^5 C^2)$, ενώ η χωρική πολυπλοκότητα μειώθηκε σε $O(d^3 C)$ στο [RZ01]. Με χρήση της πρότασης 5.2.15, θα δείξουμε πως η δυαδική πολυπλοκότητα γίνεται $O_B^*(d^4 C^2)$ [DSY05]. Στο [EMT08] ενοποιήθηκε η απόδειξη με αυτή για τη μέθοδο Descartes και αποδείχθηκε πως στον ίδιο χρόνο υπολογίζονται και οι πολλαπλότητες.

Ο αλγόριθμος, αντί να υπολογίζει μια ακολουθία Sturm για την εφαρμογή του θεωρήματος Sturm, δύναται να υπολογίσει μόνο την ακολουθία *πηλίκων* που αντιστοιχούν σε μια ακολουθία υπολοίπων (με αντεστραμμένα πρόσημα). Η ακολουθία πηλίκων υπολογίζεται επίσης και από την ακολουθία των υπολοίπων. Η βέλτιστη πολυπλοκότητα επιτυγχάνεται σήμερα με την ακολουθία υπολοίπων Sturm-Habicht, η οποία είναι οικονομική και κατάλληλη για τις πράξεις αποτίμησης που χρειάζονται. Η ακολουθία Sturm-Habicht είναι ουσιαστικά ισοδύναμη με την ακολουθία υπο-απαλοιφουσών που εξετάσαμε στο κεφάλαιο 4 για τον αποτελεσματικό υπολογισμό της ευκλείδειας ακολουθίας.

Πρόταση 5.2.16 *Έστω πολυώνυμο* $p(x)$ *βαθμού* d *με συντελεστές μήκους* C, *το οποίο δύναται να έχει πολλαπλές ρίζες. Ο υπολογισμός της ακολουθίας Sturm-Habicht του* p *(και* p'*) γίνεται σε* $O_B^*(d^3 C)$ *και παράγει πολυώνυμα με συντελεστές μήκους* $O(dC)$ *[Lombardi, Roy, Safey El Din], [Reischert].*

Ο υπολογισμός της ακολουθίας πηλίκων Sturm-Habicht δύο πολυωνύμων βαθμού $\leq d$, *με συντελεστές μήκους* C, *έχει πολυπλοκότητα* $O_B^*(d^2 C)$ *και παράγει πολυώνυμα με συντελεστές μήκους* $O(d^2 C)$ *[Du-Sharma-Yap]. Με δεδομένη την ακολουθία πηλίκων, η αποτίμηση της ακολουθίας Sturm-Habicht σε ρητό μήκους* $O(\sigma)$ *κοστίζει* $O_B^*(d^2(C + \sigma))$ *[Lickteig-Roy, Reischert].*

Ο γενικός αλγόριθμος υποδιαίρεσης είναι ο εξής:

Έστω S το σύνολο των I τα οποία έχουν ακριβώς δύο φύλλα, δηλ. για τα οποία το πλήθος μεταβολών προσήμων είναι 2 ενώ για καθένα από τα I_L, I_R είναι 1. Το πλήθος $|S| < d$.

Λήμμα 5.2.17 *Το πλήθος υποδιαιρέσεων είναι* $O^*(dC)$.

Απόδειξη. *Παρατηρούμε πως για κάθε διάστημα* I *στο σύνολο* S, *υπάρχουν πραγματικές ρίζες* a, b *τ.ώ.* $|a-b| \leq |I|$. *Χρησιμοποιούμε το φράγμα Davenport-Mahler-Mignotte όπου φράσσουμε το μέτρο Mahler* $M = O(2^C \sqrt{d})$. *ΟΕΔ*

Algorithm 2 Υποδιαίρεση για την απομόνωση ριζών με ακολουθίες Sturm

1: Ορίζεται ένα αρχικό διάστημα I_0 που περιέχει όλες τις πραγματικές ρίζες από ένα άνω φράγμα, π.χ. του Cauchy, άρα τα άκρα του έχουν απόλυτη τιμή $\leq 2^C$. Αρχικοποίησε ένα σύνολο διαστημάτων $\{I_0\}$.
2: Υπολογίζεται η ακολουθία Sturm-Habicht ή η αντίστοιχη ακολουθία πηλίκων σε $O_B^*(d^3C)$ ή $O_B^*(d^2C)$. Οι συντελεστές αμφότερων ακολουθιών έχουν μήκος $O(dC)$.
3: Εφόσον το σύνολο διαστημάτων δεν είναι κενό, αφαίρεσε κάποιο διάστημα I και εφάρμοσε το θεώρημα Sturm. Αν το I βρίσκεται σε βάθος h στο δένδρο υποδιαιρέσεων, τότε τα άκρα του I έχουν μήκος $C+h$. Το κόστος υπολογισμού των προσήμων της ακολουθίας Sturm είναι $O_B^*(d^2(C+h))$ από την παραπάνω πρόταση.

- Αν το πλήθος ριζών είναι 0, συνέχισε.
- Αν το πλήθος ριζών είναι 1, τύπωσε στην έξοδο I.
- Αν το πλήθος ριζών είναι > 1, υπολόγισε το μέσο του I σε $O_B(C+h)$, όρισε νέα διαστήματα I_L, I_R, πρόσθεσέ τα στο σύνολο διαστημάτων και συνέχισε.

Το βάθος h φράσσεται από το πλήθος υποδιαιρέσεων, άρα είναι $O^*(dC)$. Συνεπώς το βήμα (3) του αλγορίθμου έχει κόστος $O^*(d^3C)$.

Το τελικό συμπέρασμα είναι πως η δυαδική πολυπλοκότητα είναι $O_B^*(d^4C^2)$ [Du-Sharma-Yap'05].

Στη συνέχεια προχωράμε σε γενικεύσεις της θεωρίας Sturm.

Θεώρημα 5.2.18 [Tarski] *Έστω $p, q \in K[x]$ πρώτα μεταξύ τους, p χωρίς τετράγωνα και $a < b$ που δεν είναι ρίζες του p. Τότε για κάθε ακολουθία Sturm $(p, p'q, \dots)$, $V(a) - V(b) =$*

$$= \sum_{p(\rho)=0, a<\rho<b} \text{πρόσημο } (q(\rho)) = \#\{a < \rho < b : p(\rho) = 0, q(\rho) > 0\} - \#\{a < \rho < b : p(\rho) = 0, q(\rho) < 0\}.$$

Η απλή ακολουθία για $\deg q > 1$ είναι $(p, p'q, -p, \dots)$.

Άσκηση 5.2.19 Για $p, q \in K[x]$ χωρίς τετράγωνα, $p(a)p(b) \neq 0$ και την απλή ακολουθία Sturm $(p, q, \dots)$,

$$V(a) - V(b) = \sum_{p(\rho)=0,\ a<\rho<b} \text{πρόσημο } [\ p'(\rho)\ q(\rho)\ ].$$

.

Ένα σημαντικό πρόβλημα είναι ο υπολογισμός προσήμου πολλών πολυωνύμων (των μελών της ακολουθίας) σε ένα σημείο. Ο τρόπος υπολογισμού της ακολουθίας μπορεί να φανεί χρήσιμος. Αν, για παράδειγμα, τα πολυώνυμα ικανοποιούν $a_i p_i = b_i p_{i+2} + p_{i+1} q_{i+1}$ για $a_i b_i < 0$ τότε, με δεδομένες τις τιμές των p_{i+2}, p_{i+1} αρκεί να υπολογίσουμε την τιμή του q_{i+1} για να βρούμε την τιμή του p_i. Ο υπολογισμός των προσήμων μπορεί να γίνει και σύμφωνα με τους Ben-Or,Kozen,Reif.

Οι Ben-Or, Kozen, Reif μελέτησαν την γενικευμένη έκδοση του θεωρήματος του Tarski για $q_1, \dots, q_k$ και πρότειναν αποτελεσματικούς τρόπους για τον υπολογισμό του πλήθους $\sum_{i=1}^{k} \#\{\rho \in (a,b) : p(\rho) = 0, q_i(\rho) \otimes_i 0\}$, όπου κάθε $\otimes_i \in \{<, >\}$ και τα k διαφορετικά $\otimes_i$ είναι ανεξάρτητα μεταξύ τους. Η παράλληλη πολυπλοκότητα του αλγορίθμου των Ben-Or, Kozen, Reif είναι πολυωνυμική ως προς τα $\log d, \log k$, όπου $d = \deg p$. Η σειριακή πολυπλοκότητα είναι $d^3 k$ αν εξαιρέσουμε τους 3^d υπολογισμούς προσήμου πολυωνύμου. Ο Canny μείωσε τους απαιτούμενους υπολογισμούς προσήμου σε $d^{\log d}$.

Άσκηση 5.2.20 Αποδείξτε το θεώρημα 5.2.8.

Άσκηση 5.2.21 Για κάθε φράγμα παραπάνω, βρείτε ένα πολυώνυμο για το οποίο το φράγμα αυτό είναι καλύτερο από τα υπόλοιπα.

Άσκηση 5.2.22 Έστω πολυώνυμο $f = x^3 - 13x + 12$. Δίνεται η ταυτότητα $f'(x = 18/13) = -1225/169$. Υπολογίστε μια ακολουθία Sturm και απομονώστε τις ρίζες.

Άσκηση 5.2.23 Αποδείξτε με επαγωγή στον βαθμό το θεώρημα 5.2.7.

Άσκηση 5.2.24 Ποια η σχέση της απλής ακολουθίας Sturm με την ακολουθία υπολοίπων στον Ευκλείδειο αλγόριθμο;

Άσκηση 5.2.25 Η έννοια της ακολουθίας Sturm γενικεύεται με το να αναιρέσουμε την προϋπόθεση (1) του ορισμού 5.2.1. Τότε τα διαστήματα στην προϋπόθεση (4) πρέπει να ανήκουν στο διάστημα $[a, b]$, δηλ. η προϋπόθεση (4) απλοποιείται στην περίπτωση που $c = a$ ή $c = b$. Αποδείξτε πως το θεώρημα 5.2.5 ισχύει.

5.3 Κανόνας Descartes

Η μέθοδος του Descartes οδηγεί σε έναν από τους ταχύτερους αλγόριθμους απομόνωσης πραγματικών ριζών, βλ. [Akr89, chap.7]. Μας ενδιαφέρουν διατεταγμένα σώματα, συνήθως Αρχιμήδεια, δηλ. σε αντιστοιχία με τους φυσικούς, π.χ. $\mathbb{R}, \mathbb{Q}$.

Ορισμός 5.3.1 *Ένα διατεταγμένο σώμα καλείται* Αρχιμήδειο *όταν για κάθε στοιχείο του a υπάρχει φυσικός $n = 1 + \cdots + 1$ τέτοιος ώστε $n > a$.*

Π.χ. τα $\mathbb{R}, \mathbb{Q}$ είναι Αρχιμήδεια, ενώ τα $\mathbb{R}(\epsilon), \mathbb{Q}(\epsilon)$ δεν είναι Αρχιμήδεια διότι το $1/\epsilon$ δεν φράσσεται από κανένα $n \in \mathbb{N}$.

Λήμμα 5.3.2 *Το γινόμενο πολυωνύμων με ακολουθία συντελεστών χωρίς μεταβολές προσήμου είναι πολυώνυμο με ακολουθία συντελεστών χωρίς μεταβολή προσήμου.*

Απόδειξη. Εύκολα αναγόμαστε στην περίπτωση όπου όλοι οι δεδομένοι συντελεστές είναι θετικοί. Και τότε το λήμμα είναι προφανές. ΟΕΔ

Άσκηση 5.3.3 [Budan] Έστω $p \in \mathbb{R}[x]$, $a < b \in \mathbb{R}$, $p_a(x) = p(x + a)$, $p_b(x) = p(x + b)$. Συμβολίζουμε με V_a, V_b το πλήθος εναλλαγών προσήμων των συντελεστών των p_a, p_b αντίστοιχα. Τότε $V_a \geq V_b$, και η διαφορά $V_a - V_b$ υπερβαίνει το πλήθος ριζών $c \in (a, b) : p(c) = 0$ κατά έναν άρτιο.

Θεώρημα 5.3.4 (Descartes) *Έστω πολυώνυμο $p(x) \in K[x]$, όχι απαραίτητα χωρίς τετράγωνα, όπου το K είναι Αρχιμήδειο σώμα. Το πλήθος μεταβολών προσήμου στους συντελεστές του $p(x)$ υπερβαίνει το πλήθος των θετικών πραγματικών του ριζών (μετρώντας τις πολλαπλότητες) κατά έναν άρτιο μη-αρνητικό ακέραιο.*

Απόδειξη. Από το θεώρημα του Sturm ή το λήμμα Budan. Υπόδειξη για επαγωγική απόδειξη ως προς τον βαθμό του πολυωνύμου. Για την επαγωγική βάση, σταθερό πολυώνυμο (μηδενικού βαθμού) έχει $V = 0$ εναλλαγές προσήμου στους συντελεστές του.

Για το επαγωγικό βήμα διακρίνουμε 3 περιπτώσεις:

- Το $p(x) = (x^2 + a^2)q(x)$ έχει συντελεστές ιδίου προσήμου όπως στο $q(x)$ εκτός εάν κάποιος μηδενικός ή κάποιος αρνητικός συντελεστής γίνει θετικός. Και στις δυο περιπτώσεις, το V είτε παραμένει σταθερό είτε αυξάνεται κατά 2.
- $p(x) = (x + a)q(x)$, $a > 0$, όπως παραπάνω.
- δείξτε πως το πλήθος μεταβολών προσήμου συντελεστών στο $p = (x - a)q(x)$, όπου a θετικός πραγματικός, ισούται με το άθροισμα του πλήθους μεταβολών προσήμου συντελεστών στο $q(x)$ συν έναν περιττό.

ΟΕΔ

Άσκηση 5.3.5 Αποδείξτε το θεώρημα Descartes από το θεώρημα 5.2.7 των Budan-Fourier.

Θεώρημα 5.3.6 *(α) Αν το πλήθος μεταβολών προσήμου είναι 0 ή 1, τότε δίνει ακριβώς το πλήθος των θετικών ριζών.*
(β) Αν όλες οι ρίζες έχουν αρνητικό πραγματικό μέρος, τότε όλοι οι συντελεστές είναι θετικοί και το πλήθος μεταβολών προσήμου είναι 0.

Απόδειξη. Το (α) είναι προφανές. Για το (β) δες [Akr89, Lem.7.3.6]· μια απόδειξη χρησιμοποιεί το λήμμα 5.3.2. ΟΕΔ

Άσκηση 5.3.7 Βρείτε πολυώνυμο όπου όλοι οι συντελεστές είναι θετικοί και υπάρχει ρίζα με θετικό πραγματικό μέρος. Εδώ το πλήθος μεταβολών προσήμου θα είναι 1.

Πόρισμα 5.3.8 [Yap00, lect.VII] *Αν όλες οι ρίζες πολυωνύμου είναι μη-μηδενικές και πραγματικές, τότε το πλήθος μεταβολών προσήμου στους συντελεστές του ισούται ακριβώς με το πλήθος των θετικών ριζών.*

Απόδειξη. Υπόδειξη: το πλήθος μεταβολών προσήμου στους συντελεστές του $p(x)$ συν το πλήθος για το $p(-x)$ ισούται με $\deg p$. ΟΕΔ

Παράδειγμα 5.3.9 Εξετάζουμε το παράδειγμα 5.2.9. Στο $p(x) = x^2 + x + 1$, όλοι οι συντελεστές είναι θετικοί άρα δεν υπάρχει εναλλαγή προσήμου άρα ούτε και θετική ρίζα. Στο $p(-x) = x^2 - x + 1$ η ακολουθία προσήμων συντελεστών είναι $[+, -, +]$ άρα 0 ή 2 αρνητικές ρίζες. Για να αποδείξουμε πως δεν υπάρχουν πραγματικές ρίζες θα χρειαστεί υποδιαίρεση του διαστήματος $(-\infty, 0)$.

Εξετάζουμε το παράδειγμα 5.2.12 με $p = x^3 + 2x - 3 = (x - 1)(x^2 + x + 3)$. Τα πρόσημα $[+, 0, +, -]$ έχουν μια εναλλαγή άρα υπάρχει μία θετική ρίζα. Στο $p(x)$ τα πρόσημα $[-, 0, -, -]$ δηλώνουν ορθά πως δεν υπάρχει αρνητική ρίζα, καθώς υπάρχουν 2 μιγαδικές ρίζες: $-1/2 \pm \sqrt{-11/2}$. □

Παράδειγμα 5.3.10 Έστω $p(x) = x^3 - x^2 - x + 1 = (x-1)^2(x+1)$. Τα πρόσημα $[+,-,-,+]$ υποδεικνύουν 0 ή 2 θετικές ρίζες και το θέμα μπορεί να διελευκανθεί με υποδιαίρεση του $(0,\infty)$. Στο $p(-x)$, τα πρόσημα $[-,-,+,+]$ υποδεικνύουν ακριβώς μία αρνητική ρίζα. Για τις θετικές ρίζες, εφαρμόζουμε τον αλγόριθμο με $M = 3$.

- Υπολογίζουμε το $f(x) = p(3x) = 27x^3 - 9x^2 - 3x + 1$ με ρίζες στο $(0,1)$.
- Για να τις μετρήσουμε, υπολογίζουμε το $f^*(x) = x^3 - 2x + 16$ με 2 εναλλαγές προσήμου. Καθώς $f(1/2) \neq 0$ εκτελούμε τις παρακάτω 2 αναδρομές.

□

Παρατηρήστε πως, παρόλο που το Θεώρημα Descartes συναθροίζει τις πολλαπλότητες των ριζών, ένας αλγόριθμος υποδιαίρεσης για την απομόνωσή τους δεν μπορεί να διακρίνει μια διπλή από 2 απλές ρίζες. Συνεπώς, στην επίλυση εξίσωσης με χρήση του κανόνα Descartes, θα υποθέσουμε πως υπάρχουν μόνο απλές ρίζες.

Λήμμα 5.3.11 *Έστω $f(x) \in \mathbb{Z}[x]$. Ο μετασχηματισμός*

$$f'(y) = f(y+1)$$

μετατρέπει τις ρίζες του $f(x)$ σε κάποιο διάστημα (a,b) σε ρίζες του $f'(y)$ στο διάστημα $(a-1, b-1)$. Ο μετασχηματισμός

$$f^*(y) = (y+1)^d f[1/(y+1)]$$

μετατρέπει τις ρίζες του $f(x)$ στο διάστημα $(0,1)$, σε ρίζες του $f^*(y) \in \mathbb{Z}[x]$ στο διάστημα $(0,\infty)$. Οι μετασχηματισμοί

$$f(y) = f(My),\ M > 1 \ \text{ και } f(y) = m^{-d} f(my),\ 0 < m < 1$$

αντιστοιχούν σε κάθε θετική ρίζα του $f(x)$ ακριβώς μια ρίζα του $f(y)$ στο $(0,1)$.

Απόδειξη. Ο υπολογισμός του $f^*(x)$ μπορεί ισοδύναμα να γίνει σε δύο στάδια, μέσω των μετασχηματισμών $g(y) = y^d f(1/y)$ και $f^*(z) = g(z+1)$. Για το πρώτο στάδιο θέτουμε $x = 1/y$ δηλ. οι ρίζες $x \in (0,1)$ του $f(x)$ αντιστοιχούν ακριβώς στις ρίζες $y \in (1,\infty)$ του $g(y) \in \mathbb{Z}[x]$. Στο 2ο στάδιο $y = z+1$ και σε κάθε ρίζα $y \in (1,\infty)$ αντιστοιχεί ακριβώς μία ρίζα $z \in (0,\infty)$. ΟΕΔ

Η υλοποίηση του μετασχηματισμού $f'(x)$ απαιτεί $O(n^2)$ προσθέσεις.

Θεώρημα 5.3.12 [Vincent / Uspensky] *Για ένα πολυώνυμο $f(x)$ χωρίς τετράγωνα και χωρίς μηδενική ρίζα στον δίσκο με κέντρο $(0,1/2)$ και ακτίνα $1/2$, η εφαρμογή του μετασχηματισμού $f^*(x) = x^d f(1/x)$ και έπειτα $f'(x) = f(x+1)$ οδηγούν σε πολυώνυμο με μηδενικό πλήθος μεταβολών προσήμου στους συντελεστές.*

Το θεώρημα των Vincent / Uspensky αποδεικνύει πως υπάρχει αλγόριθμος που χρησιμοποιεί τους 2 παραπάνω μετασχηματισμούς και οδηγεί, έπειτα από πεπερασμένο πλήθος βημάτων, σε πλήθος μεταβολών προσήμου $\in \{0,1\}$. Όμως το πλήθος των μετασχηματισμών μπορεί να είναι εκθετικό.

Με βάση το θεώρημα των Collins - Johnson αποδεικνύεται πως το πλήθος των μετασχηματισμών είναι ασυμπτωτικά ίσο με αυτό που απαιτεί η μέθοδος υποδιαίρεσης με ακολουθίες Sturm (αλλά οι πράξεις

Algorithm 3 Υποδιαίρεση σε πολυωνυμικό χρόνο με κανόνα Descartes

Είσοδος: πολυώνυμο $p(x) \in \mathbb{Z}[x]$ χωρίς τετράγωνα, βαθμού d και $M > 0$ που φράσσει άνωθεν τις θετικές ρίζες του $p(x) = 0$.
Έξοδος: διαστήματα απομόνωσης των θετικών ριζών του $p(x) = 0$.

1: • Αν $M \geq 1$, τότε έστω $f(x) \leftarrow p(Mx)$,
• αλλιώς $f(x) \leftarrow M^{-d} f(Mx)$.
Κάλεσε το βήμα 2: για κάθε διάστημα (a, b) που επιστρέφεται από την κλήση αυτή, επέστρεψε το διάστημα (Ma, Mb).
2: Υπολόγισε το $f^*(y) \leftarrow (y+1)^d f[1/(y+1)]$ και μέτρησε το πλήθος μεταβολών προσήμου στους συντελεστές του $f^*(y)$:
• Αν είναι 0, τερμάτισε.
• Αν είναι 1, επέστρεψε το $(0, 1)$.
• Αν είναι ≥ 2, συνέχισε με το $f(x)$ από το βήμα 1.
3: Αν $f(1/2) = 0$, τότε $f(x) \leftarrow f(x)/(2x-1)$ και τύπωσε $(M/2, M/2)$.
4: Αναδρομή του αλγορίθμου στο βήμα 2 με το $f'(y) \leftarrow 2^d f(y/2)$. Κάθε διάστημα (a, b) του f' επιστρέφεται ως $(a/2, b/2)$.
5: Αναδρομή στο βήμα 2 με το $f''(z) \leftarrow f'(z+1)$. Κάθε διάστημα (a, b) του f'' επιστρέφεται ως $((a+1)/2, (b+1)/2)$.

απλούστερες). Το θεώρημα των κύκλων των Krandick-Mehlhorn'06 έρχεται να ανανεώσει αυτού του είδους τα κριτήρια. Ο παρακάτω αλγόριθμος 5.3 εξισορροπεί την υποδιαίρεση [Collins-Akritas], [BCL82, p.90].

Απόδειξη ορθότητας του αλγόριθμου 5.3, με βάση το λήμμα 5.3.11. Βήμα 1. $f \in \mathbb{Z}[x]$ και οι θετικές ρίζες του p αντιστοιχούν στις ρίζες του f στο $(0, 1)$. Το Βήμα 2 εφαρμόζει τον κανόνα Descartes στο $f^*(y)$. Βήμα 4. Οι ρίζες του $f'(y)$ στο $(0, 1)$ είναι οι ρίζες του $f(x)$ στο $(0, 1/2)$. Βήμα 5. Οι ρίζες του $f''(z)$ στο $(0, 1)$ είναι οι ρίζες του $f'(x)$ στο $(1, 2)$ δηλ. του $f(x)$ στο $(1/2, 1)$.

Παράδειγμα 5.3.13 Έστω

$$p(x) = x^2 - 4x + 3.$$

Το φράγμα Cauchy ισούται με 5. Εφαρμόζουμε τον παραπάνω αλγόριθμο και, στο βήμα 1, υπολογίζουμε $f = 25x^2 - 20x + 3$. Στο βήμα 2, $f^* = 3x^2 - 14x + 8$ του οποίου οι συντελεστές έχουν 2 εναλλαγές προσήμου. Το $f(1/2) < 0$, οπότε προχωράμε με το f.

Βήμα 4. $f' = 25x^2 - 40x + 12$. Το $f^* = 12x^2 - 16x - 3$ έχει μια εναλλαγή προσήμου, άρα επιστρέφεται το διάστημα $(0, 1)$ και η συνάρτηση που όρισε το f' επιστρέφει $(0, 1/2)$. Η αρχική συνάρτηση επιστρέφει $(0, 5/2)$ που απομονώνει την πρώτη ρίζα $x = 1$.

Βήμα 5. $f'' = 25x^2 + 10x - 3$. Το $f^* = -3x^2 + 4x + 32$ έχει μια εναλλαγή προσήμου, άρα επιστρέφεται το διάστημα $(0, 1)$ και η συνάρτηση που όρισε το f'' επιστρέφει $(1/2, 1)$. Η αρχική συνάρτηση επιστρέφει $(5/2, 5)$ που απομονώνει την 2η ρίζα $x = 3$. □

Η πολυπλοκότητα του αλγόριθμου είχε υπολογιστεί στο $O_B^*(d^6 C^2)$ όπου C το μέγιστο μέγεθος των συντελεστών του f [BCL82, RZ01]· δες [Akr89, ενότ.7.3.4] για βελτιώσεις (υπό την προϋπόθεση πως

οι ρίζες είναι απλές) που καθιστούν το κόστος ανάλογο του d^5. Ένας άλλος αλγόριθμος προτάθηκε από τον Krandick ώστε η διάσχιση του δένδρου των εφαρμογών του κανόνα να γίνεται κατά πλάτος αντί για βάθος.

Οι πρόσφατες εργασίες των Rouillier-Zimmerman [RZ01] εξηγούν πώς ένας βελτιωμένος αλγόριθμος μετακινείται μεταξύ οποιωνδήποτε κόμβων του γράφου εφαρμογής του κανόνα. Έτσι ελαχιστοποιείται η απαίτηση μνήμης, χωρίς να μεγαλώνει η χρονική πολυπλοκότητα πέραν του $O_B^*(d^6C^2)$. Η υλοποίηση RS λύνει πολυώνυμα τύπου Chebychev βαθμού 500 σε 168sec, ενώ η κατανάλωση μνήμης για την επίλυση πολυωνύμων Wilkinson, Mignotte βαθμών 500 και 200 αντίστοιχα είναι 0.3MB.

Εναλλακτικά, μελετάται η γραφή του πολυωνύμου με βάση τα πολυώνυμα Bernstein

$$B_i^d(x) = \binom{d}{i} x^i (1-x)^{d-i},\ i = 0, \ldots, d,$$

δηλ. $f(x) = \sum_i b_i B_i^d(x)$. Έτσι απλοποιούνται οι παραπάνω μετασχηματισμοί και το κόστος παραμένει στα επίπεδα του αλγορίθμου Collins-Akritas, αν και η κατανάλωση μνήμης αυξάνεται. Συγκεκριμένα, η αριθμητική πολυπλοκότητα, υπό την προϋπόθεση πως όλες οι ρίζες είναι απλές, γίνεται

$$O_A(d^2 r\lambda), \qquad \lambda \leq \lceil \lg(2/s) \rceil,$$

όπου $d = \deg f$, $r :=$ #αλλαγών προσήμου στην $(b_0, \ldots, b_d)$, λ το πλήθος των υποδιαιρέσεων και s η ελάχιστη απόσταση μεταξύ δύο ριζών [MVY02].

Πιο πρόσφατα, η πολυπλοκότητα μειώθηκε σε $O_B^*(d^4C^2)$ Eigenwillig-Sharma-Yap'06. Στο [EMT08] ενοποιήθηκε η απόδειξη για τις μεθόδους Descartes, Bernstein και απεδείχθη πως στον ίδιο χρόνο υπολογίζονται και οι πολλαπλότητες των ριζών. Οι παραπάνω εργασίες (και αντίστοιχες υλοποιήσεις) έχουν ανάγει τον κανόνα Descartes σε μια αποτελεσματική μέθοδο απομόνωσης πραγματικών ριζών.

Άσκηση 5.3.14 Απομόνωσε τις ρίζες του $p = x^3 - 2x^2 - x + 2$ με χρήση του κανόνα Descartes και του πρώτου φράγματος Cauchy.

5.4 Αλγεβρικοί αριθμοί

Αλγεβρικοί αριθμοί ονομάζονται οι ρίζες πολυωνύμου με (ακέραιους ή) ρητούς συντελεστές. Οι απλούστεροι αλγεβρικοί αριθμοί είναι τα απλά ριζικά (radicals), π.χ. $\sqrt{5}, \sqrt[3]{17}$. Έπειτα έχουμε τα επαναλαμβανόμενα (φωλιασμένα, nested) ριζικά, π.χ. $\sqrt{\sqrt{5} + \sqrt[3]{17}}$. Από το θεώρημα του Abel γνωρίζουμε πως υπάρχουν αλγεβρικοί αριθμοί, π.χ. οι ρίζες της $x^5 + x + 1$, που δεν εκφράζονται με ριζικά.

Η αναπαράσταση ενός αλγεβρικού αριθμού απαιτεί ένα μη παραγοντοποιήσιμο (irreducible) πολυώνυμο κι ένα διάστημα απομόνωσης (isolating) το οποίο περιέχει μόνο αυτόν τον αλγεβρικό αριθμό και κανέναν άλλον. Οι ακολουθίες Sturm και ο κανόνας Descartes παρέχουν ένα εργαλείο για τη μελέτη αλγεβρικών αριθμών. Σύγχρονες ερευνητικές αναζητήσεις μελετούν την επέκταση αυτών των ιδεών στους υπολογισμούς με διαστήματα.

Από την υπόθεση ελάχιστου βαθμού έπεται πως $\mathbb{Q}(\alpha) \equiv \mathbb{Q}[x]/(f)$. Επομένως τα στοιχεία του $\mathbb{Q}(\alpha)$ είναι ακέραια διανύσματα διάστασης d, όπου $d = \deg f$, ως προς την βάση $1, \alpha, \ldots, \alpha^{d-1}$. Ας υποθέσουμε πως το πολυώνυμο f που ορίζει τον αλγεβρικό αριθμό α είναι ελάχιστου βαθμού, μονικό (δηλ. μοναδιαίου μεγιστοβάθμιου συντελεστή) και μη-παραγοντοποιήσιμο (ανάγωγο). Ο βαθμός d καλείται *βαθμός* του αλγεβρικού αριθμού. Η προσθαφαίρεση στο $\mathbb{Q}(\alpha)$ ανάγεται στην αντίστοιχη πράξη στο $\mathbb{Q}[x]$, ο πολλαπλασιασμός μπορεί να απαιτήσει και μια πράξη $\mathrm{mod} f(x)$. Η αντιστροφή αλγεβρικού αριθμού

$\beta \in \mathbb{Q}(\alpha) \equiv \mathbb{Q}[x]/(f)$ ανάγεται στον Ευκλείδειο αλγόριθμο ως εξής. Έστω $g \in \mathbb{Q}[x]/(f)$ το πολυώνυμο που αντιστοιχεί στο β, τότε υπάρχουν πολυώνυμα s, t τέτοια ώστε $sf + tg = 1 \Rightarrow t \equiv g^{-1} \bmod f$.

Το $f(-x)$ είναι το ελάχιστο πολυώνυμο του $-\alpha$. Το επόμενο θεώρημα δίνει τα ελάχιστα πολυώνυμα πιο σύνθετων αλγεβρικών αριθμών.

Θεώρημα 5.4.1 *Έστω πως τα $f(x), g(x)$ είναι πολυώνυμα επί μιας ακέραιας περιοχής (integral domain) με ρίζες α_i, β_i, τότε*

- *η απαλοίφουσα, ως προς y, των $f(y), g(x \mp y)$ είναι ένα πολυώνυμο ως προς x με ρίζες (όχι απαραίτητα διαφορετικές) τα $\alpha_i \pm \beta_j$,*
- *η απαλοίφουσα των $f(y), y^{\deg g} g(x/y)$ έχει ρίζες (όχι απαραίτητα διαφορετικές) τα $\alpha_i \beta_j$,*
- *ενώ η απαλοίφουσα των $f(y), g(xy)$ έχει ρίζες τα α_i/β_j εφόσον $f(0) \neq 0$.*
- *Επίσης, η απαλοίφουσα των $f(y), x^q - y^p$ έχει ρίζες τα $\alpha_i^{p/q}$ για $p, q \in \mathbb{Z}$.*
- *Τέλος, το ελάχιστο πολυώνυμο των αριθμών $p\alpha_i + q$ είναι το $p^{\deg f} f((x-q)/p)$.*

Απόδειξη. Δες [BCL82, p.179,p.182] και [Zip93, p.153]. ΟΕΔ

Αν I, J είναι διαστήματα (ή ορθογώνια) απομόνωσης 2 αλγεβρικών αριθμών α, β με ελάχιστα πολυώνυμα τα f, g, τότε το ελάχιστο πολυώνυμο και το διάστημα (ή ορθογώνιο) απομόνωσης του $\alpha + \beta$ υπολογίζεται με τον παρακάτω αλγόριθμο, εφόσον εργαζόμαστε επί διατεταγμένων Αρχιμήδειων σωμάτων. Η τελευταία υπόθεση είναι απαραίτητη ώστε η υποδιαίρεση να μειώνει το αντίστοιχο διάστημα (ή ορθογώνιο, σε μεγαλύτερη διάσταση).

1. Υπολογίζω την απαλοίφουσα $R(x)$ όπως στο θεώρημα 5.4.1, υπολογίζω μια παραγοντοποίηση $R(x) = D_1(x) \cdots D_k(x)^k$ χωρίς τετράγωνα και τα διαστήματα (ή ορθογώνια) απομόνωσης των ριζών των $D_i(x)$.
2. Αν το $I + J$ τέμνει μόνο ένα από τα παραπάνω διαστήματα, τότε επιστρέφω την τομή αυτή και το αντίστοιχο $D_i(x)$, αλλιώς υποδιαιρώ τα I, J και επαναλαμβάνω.

Έστω f το ελάχιστο πολυώνυμο του α. Μπορούμε να μετατρέψουμε την αναπαράσταση στο $\mathbb{Q}(\alpha)$ ενός αλγεβρικού αριθμού $\beta = g(\alpha) \in \mathbb{Q}(\alpha)$ σε μια αναπαράσταση από την απαλοίφουσα $R(x)$ των $f(y), x - g(y)$, η οποία ορίζει το β. Αυτή η αλλαγή αναπαράστασης δίνει μια εναλλακτική μέθοδο για τον υπολογισμό του προσήμου του $g(\alpha)$, η οποία βασίζεται στον υπολογισμό ενός διαστήματος απομόνωσης της ρίζας του $R(x)$ που μας ενδιαφέρει.

Θεωρήσαμε μέχρι τώρα δυο διαφορετικούς τρόπους για να εκφραστεί ένας αλγεβρικός αριθμός ως ρίζα δεδομένου πολυωνύμου, συγκεκριμένα με ένα διάστημα απομόνωσης και με έναν δείκτη που δηλώνει την σειρά του αριθμού ανάμεσα στις πραγματικές ρίζες του πολυωνύμου. Το παρακάτω θεώρημα, γνωστό ως Λήμμα του Thom, παρουσιάζει έναν τρίτο τρόπο αναπαράστασης.

Θεώρημα 5.4.2 [Thom] *Σε κάθε πραγματική ρίζα ρ του $p(x)$ αντιστοιχεί μια μοναδική ακολουθία προσήμων των τιμών $p'(\rho), p''(\rho), \ldots$.*

Μπορώ λοιπόν να χαρακτηρίσω τους αλγεβρικούς με το πρόσημό τους στην ακολουθία $p'(\rho), p''(\rho), \ldots$ (Budan-Fourier). Ο υπολογισμός των προσήμων γίνεται σύμφωνα με τους Ben-Or,Kozen,Reif για $q_i = p^{(i)}$, δες ενότητα 5.2.

Επιστρέφουμε τώρα στη μελέτη ενός σώματος που ορίζεται ως επέκταση των ρητών από έναν ή περισσότερους αλγεβρικούς αριθμούς. Έστω πως μας ενδιαφέρει ένα πεπερασμένο σύνολο αλγεβρικών αριθμών, ορισμένων από πολυώνυμα με συντελεστές σ' ένα άπειρο σώμα (δηλ. που περιέχει το $\mathbb{Z}$, και άρα αποκλείουμε τα πεπερασμένα σώματα $\mathbb{Z}_p$). Τότε, μπορούμε να αναχθούμε στη μελέτη ενός μόνο αλγεβρικού αριθμού, του λεγόμενου *πρωτογενούς στοιχείου*, σε συνάρτηση του οποίου μπορούμε να εκφράσουμε όλους τους αλγεβρικούς αριθμούς. Πιο τυπικά, οι αλγεβρικοί αριθμοί $\alpha_1, \ldots, \alpha_k$ έχουν πρωτογενές στοιχείο ένα πολυώνυμο με ρίζα το α_0 ανν $\mathbb{Q}(\alpha_1, \ldots, \alpha_k) = \mathbb{Q}(\alpha_0)$. Ο υπολογισμός του πρωτογενούς στοιχείου 2 αλγεβρικών αριθμών ανάγεται στην απαλοίφουσα 2 πολυωνύμων μιας μεταβλητής.

Παράδειγμα 5.4.3 Έστω τα $\alpha_1 = \sqrt{2}, \beta_1 = \sqrt{3}$ με ελάχιστα πολυώνυμα $f_1 = x^2 - 2, f_2 = x^2 - 3$. Αν εξετάσουμε την απαλοίφουσα των $f_1(y - x) = (y - x)^2 - 3, f_2(x) = x^2 - 2$, παίρνουμε $R(y) = y^4 - 10y^2 + 1$, με ρίζα $\theta = \sqrt{2} + \sqrt{3} = \sqrt{5 + 2\sqrt{6}}$. Αυτό είναι το πρωτογενές στοιχείο του $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ διότι $\alpha_1 = (\theta^3 - 9\theta)/2, \beta_1 = (11\theta - \theta^3)/2$. Άσκηση: δικαιολογήστε τον ορισμό του πρωτογενούς στοιχείου μέσω αυτής της απαλοίφουσας και τις εκφράσεις των α_1, β_1 σε συνάρτηση του θ. □

Γενικότερα, εξετάζουμε την απαλοίφουσα $R(y)$ των $f_1(y - cx), f_2(x)$ όπου έχει απαλειφθεί το x, για c τέτοιο ώστε $\alpha_i + c\beta_j \neq \alpha_k + c\beta_l$ για όλα τα i, j, k, l. Η πρώτη υπο-απαλοίφουσα $R_1(x, y)$ των παραπάνω πολυωνύμων είναι βαθμού 1 ως προς x, της μορφής $R_1(x, y) = d(y)x + n(y)$. Μπορούμε τώρα να ορίσουμε *ρητές συναρτήσεις*

$$r_1(y) = y + c\frac{n(y)}{d(y)},\ r_2(y) = -\frac{n(y)}{d(y)} \in \mathbb{Z}(y),$$

οι οποίες εκφράζουν τις λύσεις των δεδομένων f_1, f_2 σε συνάρτηση με το y. Επομένως πρέπει να λύσουμε το πρωτογενές στοιχείο $R(y)$, που είναι εξίσωση βαθμού $\deg f_1 \deg f_2$ ως προς y. Σε κάθε ρίζα y, οι τιμές των $r_1(y), r_2(y)$ δίνουν το αντίστοιχο α_i και β_j. Αυτή είναι η κατασκευαστική μορφή ([Can88a, lem.2.1]) του θεωρήματος του πρωτογενούς στοιχείου [vdW50].

Εναλλακτικά, θα μπορούσαμε να χρησιμοποιήσουμε την u-απαλοίφουσα των 2 πολυωνύμων, βλ. κεφάλαιο 6. Με άλλα λόγια, την απαλοίφουσα $R(u)$, όπου $u = (u_0, u_1, u_2)$, του συστήματος

$$f_0 = u_0 + u_1x_1 + u_2x_2, f_1(x_1), f_2(x_2) \ \Rightarrow\ R(u) = \prod_{i,j}(u_0 + \alpha_i u_1 + \beta_j u_2),$$

όπου η μορφή της απαλοίφουσας προκύπτει από τον τύπο Poisson. Ο ορισμός του πρωτογενούς στοιχείου και ρητών συναρτήσεων για τα α_i, β_j γίνεται αντίστοιχα με την παραπάνω συζήτηση είτε αναγόμενοι σε 2 πολυώνυμα μιας μεταβλητής και της πρώτης υπο-απαλοίφουσάς τους, είτε χρησιμοποιώντας κατάλληλες παραγώγους της $R(u)$.

Γενικότερα, η u-απαλοίφουσα οδηγεί στη μέθοδο του Πρωτογενούς στοιχείου (primitive element) του Canny [Can88b], γνωστή και ως *Πητή Μονοδιάστατη Αναπαράσταση* (Rational Univariate Representation) [Rou99], για τον υπολογισμό των κοινών πραγματικών ριζών σε γενική διάσταση.

Θυμηθείτε πως για $f_1, \ldots, f_n \in \mathbb{Q}[x_1, \ldots, x_n]$ ορίζω την u-απαλοίφουσα αυτών των πολυωνύμων και του $f_0 := u_0 + u_1x_1 + \cdots + u_nx_n$ απαλείφοντας τα x_i. Τότε, με το i να αντιστοιχεί στις μιγαδικές ρίζες $(\rho_{i1}, \ldots, \rho_{in}) \in \mathbb{C}^n$ του αρχικού συστήματος $f_1, \ldots, f_n$, έχουμε

$$R(u) = \prod_i (u_0 + u_1\rho_{i1} + \cdots + u_n\rho_{in}) \mapsto p(\lambda) = \prod_i (a_0 + \lambda b_0 + a_1\rho_{i1} + \lambda b_1\rho_{i1} + \cdots + a_n\rho_{in} + \lambda b_n\rho_{in}),$$

όπου έχουμε αντικαταστήσει κάθε u_i με $a_i+\lambda b_i$. Το πρωτογενές στοιχείο θα είναι το $p(\lambda)$ και οι ρίζες του $\lambda_i \in \mathbb{C}$ αντιστοιχούν μοναδικά στις ρίζες $\rho_i \in \mathbb{C}^n$, για μη-εκφυλισμένα a_i, b_i, ως εξής: Κατασκευάζουμε ρητές εκφράσεις

$$\frac{\partial R}{\partial u_k}/\frac{\partial R}{\partial u_0} \mapsto q_k(\lambda),\ k=1,\ldots,n,$$

με την ίδια αντιστοιχία $u_i \mapsto a_i + \lambda b_i$. Αποδεικνύεται τώρα, με κάποιες πράξεις, πως όταν $p(\lambda_i)=0$ τότε $q_k(\lambda_i)=\rho_{ik}$.

5.5 Πραγματικές ρίζες σε γενική διάσταση

Μια επέκταση της θεωρίας Sturm προτάθηκε από τον Milne και την εξετάζουμε ευθύς αμέσως. Μια άλλη ανεξάρτητη επέκταση προτάθηκε από τον Pedersen και θα την δούμε παρακάτω.

Έστω πως μελετώ το πλήθος πραγματικών ριζών συστήματος πολυωνύμων $p_1, p_2 \in \mathbb{R}[x_1, x_2]$ στο 1ο και 3ο τεταρτημόριο. Αρκεί να μελετήσω την u-απαλοίφουσα των $p_1, p_2, u + x_1x_2$. Γενικότερα, για τις πραγματικές ρίζες των $p_1, \ldots, p_n \in \mathbb{R}[x_1, \ldots, x_n]$ στην ένωση όλων των τεταρτημορίων όπου $x_1 \cdots x_n > 0$ μελετώ την u-απαλοίφουσα $R(u)$ των $p_1, \ldots, p_n, u + x_1 \cdots x_n$: αρκεί να πάρω τις αρνητικές ρίζες της $R(u)$ ώστε $u = -x_1 \cdots x_n < 0$. Αν μας ενδιαφέρουν τα τεταρτημόρια ως προς την αρχή των αξόνων $(a_1, \ldots, a_n) \in \mathbb{R}^n$, αρκεί να θέσω $x_i = y_i - a_i$. Θυμηθείτε πως

$$R(u) = \prod_k \left(u + \prod_i (\rho_{ki} - a_i) \right)$$

όπου $(\rho_{k1}, \ldots, \rho_{kn}) \in \mathbb{C}^n$ η k-οστή ρίζα των $p_1, \ldots, p_n$. Αν υπάρχει μιγαδική συντεταγμένη ρ_{ki} τότε το γινόμενο $\prod_i (\rho_{ki} - a_i)$ είναι μιγαδικό για μη-εκφυλισμένα a_i. Επιλέγω λοιπόν τα a_i με τυχαίο τρόπο.

Αν μας ενδιαφέρουν οι πραγματικές ρίζες σε ένα ορθογώνιο παραλληλεπίπεδο με όψεις παράλληλες προς τους άξονες, αρκεί να υπολογίσουμε 2^n τέτοιες απαλοίφουσες και να συνδυάσουμε τα αποτελέσματα. Για να μετρήσω τις πραγματικές ρίζες σε ορθογώνιο στο $\mathbb{R}^2$ χρησιμοποιώ διαδοχικά $(a_1, a_2) = \mathrm{N\Delta}$ (νοτιοδυτική), NA, BA, BΔ κορυφή, με αντίστοιχες απαλοίφουσες και πλήθη πραγματικών ριζών που συνδυάζονται ως εξής: $C_{N\Delta} - C_{NA} + C_{BA} - C_{B\Delta}$ ώστε να δώσουν το διπλάσιο του πλήθους στο ορθογώνιο παραλληλόγραμμο.

Εξετάζουμε τώρα την συγγενή θεωρία των Hermite, Pedersen. Μελετάμε συστήματα πολυωνύμων $p_1, \ldots, p_m \in K[x] := K[x_1, \ldots, x_n]$ με πεπερασμένο πλήθος κοινών ριζών στο $\mathbb{C}^n$, όπου $\mathbb{C}$ περιλαμβάνει την αλγεβρική θήκη του πεδίου των συντελεστών K. Εδώ μας ενδιαφέρει κυρίως η περίπτωση $K = \mathbb{R}$. Έστω I το ιδεώδες τους και $A_K = K[x_1, \ldots, x_n]/I$ ο δακτύλιος των κλάσεων ισοδυναμίας ως προς το ιδεώδες I (βλ. κεφάλαιο 6 για ορισμούς). Ο δακτύλιος $A_{\mathbb{C}}$ μελετάται στο κεφάλαιο 6, ενώ $A_{\mathbb{C}} = A_{\mathbb{R}} \otimes \mathbb{C}$ όπου η πράξη $\otimes$ ουσιαστικά επεκτείνει τις σταθερές του $A_{\mathbb{R}}$ ώστε να περιλάβουν μιγαδικούς αριθμούς, στους οποίους ορίζεται ο συζυγής.

Υπογραφή (signature) πίνακα καλείται παρακάτω η διαφορά του πλήθους των θετικών ιδιοτιμών του μείον το πλήθος των αρνητικών ιδιοτιμών. Αν γράψουμε αυτή την διαφορά ως $p - q$ τότε ο βαθμός του πίνακα ισούται με $p + q$. *Ίχνος* (trace) πίνακα καλείται το άθροισμα των στοιχείων της διαγωνίου του.

Έστω πως ορίζουμε τον πίνακα πολλαπλασιασμού M_a ενός πολυωνύμου $a \in A_{\mathbb{C}}$. Τότε μπορούμε να αντιστοιχίσουμε σε κάθε $a \in A_{\mathbb{C}}$ το ίχνος τού M_a:

$$T:\ A_{\mathbb{C}} \to \mathbb{C} : a \mapsto T(a) := \text{ίχνος}(M_a).$$

Γενικότερα, ο παραπάνω γραμμικός μετασχηματισμός μπορεί να οριστεί και ως $T : K[x] \to K : a \mapsto$ ίχνος(M_a). Έστω, επίσης, ο δι-γραμμικός μετασχηματισμός

$$Q_h : \ A_{\mathbb{R}} \times A_{\mathbb{R}} \to \mathbb{R} : (a, b) \mapsto T(hab) = \text{ίχνος}(M_{hab}),$$

για κάποιο $h \in \mathbb{R}[x]$. Καλούμε Q_h τον πίνακα (quadratic form) που εκφράζει αυτόν τον δι-γραμμικό μετασχηματισμό, ο οποίος είναι πραγματικός συμμετρικός, επομένως διαγωνοποιήσιμος στο $\mathbb{R}$.

Το παρακάτω θεώρημα διατυπώθηκε από τον Hermite για $n = 1$ [Her80] και επεκτάθηκε σε γενικό n από τον Pedersen στην διδακτορική του διατριβή [Ped90] και στο [PRS93].

Θεώρημα 5.5.1 [Hermite,Pedersen] *Ο βαθμός του Q_h ισούται με το πλήθος των διαφορετικών μιγαδικών ριζών $\alpha \in \mathbb{C}$ του συστήματος $p_1 = \cdots = p_m = 0$ τ.ώ. $h(\alpha) \neq 0$. Η υπογραφή του Q_h ισούται με την διαφορά του πλήθους των πραγματικών ριζών α του συστήματος τ.ώ. $h(\alpha) > 0$ μείον το πλήθος πραγματικών ριζών α τ.ώ. $h(\alpha) < 0$ δηλ. $\#\{\alpha : h(\alpha) > 0\} - \#\{\alpha : h(\alpha) < 0\}$ όπου α διατρέχει τις πραγματικές ρίζες του συστήματος $p_1 = \cdots = p_m = 0$.*

Κατασκευάζουμε τώρα τον πίνακα $Q_1 := [T(x^{a+b})]_{a,b}$, όπου τα $a, b \in D$ για μια βάση μονωνύμων D του $A_{\mathbb{R}}$.

Πόρισμα 5.5.2 *Ο βαθμός του Q_1 ισούται με το πλήθος των διαφορετικών μιγαδικών ριζών του συστήματος $p_1 = \cdots = p_m = 0$, $p_i \in \mathbb{R}[x_1, \ldots, x_n]$. Η υπογραφή του Q_1 ισούται με το πλήθους των διαφορετικών πραγματικών ριζών του συστήματος.*

Η παραπάνω θεωρία υλοποιείται μέσω του υπολογισμού του πίνακα πολλαπλασιασμού M_a, ο οποίος γίνεται με βάση τις μεθόδους της επιλύουσας ή των βάσεων Groebner. Στην συνέχεια απαιτεί τον υπολογισμό του πίνακα Q_h. Κλείνουμε με ένα σχετιζόμενο θεώρημα το οποίο αποφεύγει τον υπολογισμό του πίνακα Q_h.

Θεώρημα 5.5.3 *Στην περίπτωση καλώς ορισμένων συστημάτων, δηλ. για $m = k$, θεωρήστε την Ιακωβιανή J των $p_1, \ldots, p_m$, η οποία είναι η ορίζουσα ενός πίνακα $m \times m$. Ο βαθμός και η υπογραφή του πίνακα Bézout της επιλύουσας του συστήματος $p_1, \ldots, p_m, J$ (ορίζεται στο κεφάλαιο 6) παρέχει τις ίδιες πληροφορίες όπως ο Q_1 στο πόρισμα 5.5.2.*

5.6 Κυλινδρική υποδιαίρεση

Μελετάμε το πρόβλημα της απαλοιφής των ποσοδεικτών (quantifier elimination) σε πραγματικούς χώρους και n διαστάσεις, το οποίο γενικεύει τα παραπάνω ερωτήματα σε πραγματικές ρίζες πολυωνύμων. Σήμερα μόνο με αλγεβρικές μεθόδους λύνεται και αυτό το πρόβλημα, που έχει πρακτικές εφαρμογές στην γεωμετρία σε πραγματικούς χώρους, ρομποτική (σχεδιασμός κίνησης, πλοήγηση), βελτιστοποίηση, υπολογιστικά οικονομικά κλπ. Δες: [DST88, pp.111-7].

Η γενίκευση της έννοιας του σημείου και του διαστήματος βρίσκεται στο εξής: *Ημι-αλγεβρικό στοιχείο* καλείται κάθε σύνολο που ορίζεται από πολυωνυμικές εξισώσεις και ανισότητες: $\{x \in \mathbb{R}^n : p_1(x) = \cdots = p_m(x) = 0, q_1(x) > 0, \ldots, q_k(x) > 0\} \subset \mathbb{R}^n$.

Ορισμός 5.6.1 *Ένα ημι-αλγεβρικό σύνολο είναι είτε ένα ημι-αλγεβρικό στοιχείο είτε το αποτέλεσμα συνδυασμού δύο (ή περισσοτέρων πεπερασμένου πλήθους) στοιχείων μετά από ένωση, τομή ή διαφορά συνόλων. Ένα οποιοδήποτε σύνολο λέγεται συνδεδεμένο εάν μεταξύ 2 οποιωνδήποτε σημείων του υπάρχει ένα μονοπάτι που τα ενώνει το οποίο βρίσκεται εξ ολοκλήρου μέσα στο σύνολο αυτό.*

Ημι-αλγεβρική *υποδιαίρεση* του $\mathbb{R}^n$ (ή υποσυνόλου) είναι ένα σύνολο πεπερασμένου πλήθους ημι-αλγεβρικών στοιχείων, μη επικαλυπτόμενα και συνδεδεμένα, των οποίων η ένωση ισούται με το $\mathbb{R}^n$ (ή το υποσύνολο).

Σημειακή λέγεται μια ημι-αλγεβρική υποδιαίρεση εάν σε κάθε ημι-αλγεβρικό στοιχείο αντιστοιχίζεται ένα σημείο με συντεταγμένες ρητούς (ή αλγεβρικούς) αριθμούς. Για ένα σύνολο πολυωνύμων, μια ημι-αλγεβρική υποδιαίρεση λέγεται σταθερή ως προς πρόσημο εάν σε κάθε στοιχείο όλα τα δεδομένα πολυώνυμα έχουν σταθερό πρόσημο.

Πρόταση 5.6.2 *Έστω ημι-αλγεβρικό σύνολο A και μια υποδιαίρεση σταθερή ως προς πρόσημο U για τα πολυώνυμα που ορίζουν το A. Τότε κάθε ημι-αλγεβρικό στοιχείο της U είναι είτε ξένο προς A είτε υποσύνολό του.*

Η μελέτη του $\mathbb{R}^n$ (ή υποσυνόλου του) γίνεται αλγοριθμικά με διαφορετικούς τρόπους. Ένας από τους πρώτους αποτελεσματικούς αλγορίθμους βασίζεται στις κυλινδρικές υποδιαιρέσεις:

Ορισμός 5.6.3 [Collins'75] Κυλινδρική *λέγεται μια υποδιαίρεση U του $\mathbb{R}^n$ εάν $n = 0$ ή $n > 0$ και υπάρχει μια κυλινδρική υποδιαίρεση U' του $\mathbb{R}^{n-1}$ τέτοια ώστε για κάθε στοιχείο Σ της U υπάρχει ένα στοιχείο Σ' της U' ώστε $\Sigma = \{(x, x_n) : x \in \Sigma',\ x_n \in (a, b)\}$ όπου τα a, b είναι το $\pm\infty$ ή ρίζες πολυωνυμικών εξισώσεων.*

Παράδειγμα 5.6.4 Έστω a, b ρίζες πολυωνύμων τότε μια κυλινδρική υποδιαίρεση είναι $\mathbb{R} = (-\infty, a) \cup \{a\} \cup (a, b) \cup \{b\} \cup (b, \infty)$ □

Αλγόριθμοι υπάρχουν για τον υπολογισμό σημειακής κυλινδρικής υποδιαίρεσης σταθερής ως προς πρόσημα δεδομένων πολυωνύμων: Έστω m πολυώνυμα n μεταβλητών συνολικού βαθμού d με ακέραιους συντελεστές μήκους H. Πολυπλοκότητα: [Collins'75] $= (2d)^{2^{2n+8}}$, [McCallum'85, Davenport'85] $(dm)^{2^n} H^3$. Γενικά, το μειονέκτημα των κυλινδρικών υποδιαιρέσεων είναι το μεγάλο πλήθος κελιών που δημιουργούν. Κατώτατο όριο [Davenport Heinz'87] $\Omega(2^{2^n})$ (ο εκθέτης εκφράζει την συνδυαστική πολυπλοκότητα).

Μια πιο σύγχρονη αλγοριθμική προσέγγιση διατάξεων (arrangements) υπερεπιπέδων (που ορίζονται από τα δεδομένα πολυώνυμα) στους πραγματικούς βρίσκεται στο βιβλίο των Benedetti-Risler και σε αυτό των Sharir-Agarwal [SA95]. Στο δεύτερο δίνεται το κάτω φράγμα $\Omega(m^n)$ στο πλήθος κελιών στην διάταξη m πραγματικών αλγεβρικών επιφανειών στο $\mathbb{R}^n$. Επίσης, το φράγμα $O(m^{2n-4}\lambda_s(m))$ [Chazelle et.al'89,'91] στο πλήθος ανοιχτών κελιών, όπου s είναι μια σταθερά που εξαρτάται από τα d, n. Κάθε κελί φράσσεται από το πολύ $2n$ επιφάνειες [SA95, Thm.8.21].

Κεφάλαιο 6

Επίλυση στους μιγαδικούς

Το κεφάλαιο αυτό πραγματεύεται την εύρεση όλων των μιγαδικών λύσεων μιας πολυωνυμικής εξίσωσης ή συστήματος εξισώσεων. Ξεκινάμε με μια σύντομη επισκόπηση μεθόδων που χρησιμοποιούνται για την προσέγγιση όλων των μιγαδικών ριζών πολυωνύμου. Στη συνέχεια μελετάμε συστήματα με διαφορετικούς τρόπους, επικεντρώνοντας το ενδιαφέρον μας στη μέθοδο της απαλοίφουσας. Καλούμε τον αναγνώστη να παρατηρήσει τις αντιστοιχίες και διαφορές μεταξύ της επίλυσης στους μιγαδικούς και τους πραγματικούς που εξετάστηκαν στο προηγούμενο κεφάλαιο.

6.1 Επίλυση πολυωνυμικής εξίσωσης

Έστω πολυώνυμο $p(x)$ με ρητούς συντελεστές και βαθμό n. Οι (μιγαδικές) ρίζες είναι αριθμητικά ασταθείς ως προς τις μεταβολές στους συντελεστές. Π.χ. η διαταραχή του x^n σε $x^n - 2^{-bn}$ (στο bn-στό ψηφίο) μεταβάλλει τις ρίζες από 0 σε $2^{-b}e^{2k\pi i/n}$ (αλλαγή στο b-στό ψηφίο).

Υπάρχουν τρεις οικογένειες μεθόδων, τις οποίες εξετάζουμε παρακάτω. Για μια πλήρη επισκόπηση των αριθμητικών μεθόδων, δες [Pan97].

Πρώτα, οι *Αναλυτικές μέθοδοι*. Βασισμένες στην επαναληπτική μέθοδο του Newton για την εύρεση μιας ρίζας:

$$z_{i+1} = z_i - [p(z_i)/p'(z_i)]a_i.$$

όπου η ακολουθία z_i τείνει σε μία (μιγαδική) ρίζα του πολυωνύμου η οποία εξαρτάται από το σημείο εκκίνησης z_0 και a_i ($= 1$ συνήθως) είναι το βήμα της επανάληψης. Η επανάληψη συνάγεται άμεσα από την προσέγγιση Taylor για το πολυώνυμο σε μια ρίζα z: $p(z) = p(z_i) + (z - z_i)p'(z_i) +$ (όροι βαθμού > 1 ως προς $(z - z_i)) \Rightarrow$

$$0 \cong p(z_i) + (z_{i+1} - z_i)p'(z_i).$$

Η αριθμητική πολυπλοκότητα είναι πολύ ικανοποιητική (σχεδόν γραμμική ως προς n). Κύριο πρόβλημα η επιλογή σημείου εκκίνησης, που επηρεάζει και την αριθμητική σταθερότητα και την ρίζα η οποία προσεγγίζεται. Το χειρότερο: δεν υπάρχει εγγύηση για το ποια ρίζα προσεγγίζεται.

Για ένα σύστημα k πολυωνύμων $p_1, \ldots, p_k$ σε k αγνώστους $x_1, \ldots, x_k$, η ακολουθία των z_i είναι μια ακολουθία διανυσμάτων, η τιμή του συστήματος στο z_i είναι ένα διάνυσμα και η τιμή του παρονομαστή στο z_i είναι η ορίζουσα του *Ιακωβιανού πίνακα* με (l, j) στοιχείο την τιμή $(\partial p_l/\partial x_j)(z_i)$.

Για την ταυτόχρονη προσέγγιση όλων των ριζών υπάρχουν οι μέθοδοι τύπου Durand-Kerner και άλλες [Pan97]. Για την ρίζα j, $j = 1, \ldots, n$:

$$z_{i+1}(j) = z_i(j) - [p(z_i(j))/\Pi_{k \neq j}(z_i(j) - z_i(k))].$$

Συνολική πολυπλοκότητα ανάλογη με $O(n^2)$ ή $O(n \log n)$, ανάλογα με το ανεκτό αριθμητικό σφάλμα. Πάλι το κύριο πρόβλημα είναι το σημείο εκκίνησης.

Δεύτερο, οι *Γεωμετρικές μέθοδοι*. Όπως π.χ. η μέθοδος του [Wey24], βελτιωμένη από τον [Pan97] για τον υπολογισμό όλων των ριζών. Η μέθοδος θεωρεί ένα τετράγωνο στο μιγαδικό επίπεδο και το υποδιαιρεί σε 4 μικρότερα. Χρησιμοποιεί ένα τεστ που δηλώνει εάν σε κάποιο δεδομένο τετράγωνο δεν υπάρχουν ρίζες. Συνεχίζει επαγωγικά αγνοώντας τα υποτετράγωνα που δεν περιέχουν ρίζες, μέχρι να απομονώσει επαρκώς τις ρίζες ανά μία ή ανά ομάδες (clusters). Τότε καλεί μια αναλυτική μέθοδο για την γρήγορη προσέγγισή τους.

Δυαδική πολυπλοκότητα $= O(n^2 \log n \log(bn))$ όπου 2^{-b} είναι το σχετικό σφάλμα στην προσέγγιση. Πλεονέκτημα: εγγυημένα προσεγγίζει ΌΛΕΣ τις ρίζες.

Τρίτον, αλγόριθμοι τύπου *Διαίρει και βασίλευε*. Με βάση τον υπολογισμό ενός διαχωριστικού δακτυλίου (κενού ριζών) στο μιγαδικό επίπεδο, που διαιρεί τις ρίζες περίπου ισομερώς. Δυαδική πολυπλοκότητα $= O(n \log^2 n \log(bn))$.

6.2 Έννοιες αλγεβρικής γεωμετρίας

Μας ενδιαφέρει η μελέτη και επίλυση (μη γραμμικών) πολυωνυμικών (δηλ. αλγεβρικών) συστημάτων, το οποίο αποτελεί το θεμελιώδες πρόβλημα της υπολογιστικής αλγεβρικής γεωμετρίας. Βιβλιογραφία: [CLO97, CLO05], [DST88, pp.95-105], [DEKP99, pp.10-13].

Το σύνολο των πολυωνύμων $K[x]$, όπου το x συμβολίζει n μεταβλητές, είναι αντιμεταθετικός δακτύλιος (ring), δηλ. κλειστό ως προς την πρόσθεση και τον πολλαπλασιασμό με αντίστροφο μόνο για την πρόσθεση, όπου το K είναι το $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$.

Ορισμός 6.2.1 *Ένα* ιδεώδες (ideal) I *είναι ένα υποσύνολο του πολυωνυμικού δακτυλίου* R *κλειστό ως προς την πρόσθεση μέσα στο ιδεώδες και ως προς τον πολλαπλασιασμό με οποιοδήποτε μέλος του δακτυλίου, δηλ.*

$$a, b \in I, p \in R \Rightarrow a + b, ap \in I.$$

Το ενδιαφέρον του ιδεώδους έγκειται στο ότι οποιοδήποτε πολυώνυμο ανήκει σε ιδεώδες που παράγεται από ένα σύνολο πολυωνύμων, μηδενίζεται στις κοινές ρίζες αυτού του συνόλου.

Μονώνυμο $x^\alpha \in \mathbb{C}[x]$ καλείται ένα πολυώνυμο σε n μεταβλητές $x = (x_1, \ldots, x_n)$ με ένα μόνον όρο, συντελεστή $= 1$ και ακέραιο διάνυσμα $\alpha = (\alpha_1, \ldots, \alpha_n)$ ως εκθέτη.

Μελετάμε τώρα την βασική γεωμετρική έννοια στη μελέτη συστημάτων πολυωνυμικών εξισώσεων.

Ορισμός 6.2.2 *Έστω* n *μεταβλητές και ένα πεπερασμένο σύνολο πολυωνύμων από το* $K[x]$. *Αλγεβρικό σύνολο (variety, zero-set) των πολυωνύμων ονομάζεται το υποσύνολο του* $\overline{K}^n$ *που ορίζεται ως το σύνολο των κοινών λύσεων όλων των πολυωνύμων.*

Για K ίσο με $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, ισχύει $\overline{K} = \mathbb{C}$. Γενικά, η *αλγεβρική θήκη* (algebraic closure) $\overline{K}$ περιέχει όλες τις ρίζες πολυωνύμων στο $K[x]$. Συγκρίνετε το αλγεβρικό σύνολο με την αντίστοιχη έννοια στη διαφορική γεωμετρία, που είναι η ποικιλότητα (manifold), γνωστή και ως «σύνολο πολλαπλότητας».

Παράδειγμα 6.2.3 Έστω $V(S)$ το αλγεβρικό σύνολο πολυωνυμικού συνόλου S: $V(x^2 + 1) = \{\pm\sqrt{-1}\}$, $V(\mathbb{Q}[x_1, \ldots, x_n]) = \emptyset$, $V(\emptyset) = \mathbb{C}^n$. □

Διάσταση του αλγεβρικού συνόλου καλείται η γεωμετρική διάστασή του, δηλ. για μη κενά σύνολα ένας ακέραιος μεταξύ 0 (πεπερασμένο σύνολο σημείων) έως n (αν και μόνο αν αλγεβρικό σύνολο $= \mathbb{C}^n$).

Παράδειγμα 6.2.4

- $\dim(V) = 0 \Leftrightarrow V =$ σημειοσύνολο: αυτή είναι η μόνη περίπτωση το αλγεβρικό σύνολο να έχει πεπερασμένο πληθάριθμο.
- Διάσταση πεπερασμένου συνόλου ευθειών ή επιπέδων $= 1$ ή 2. Γενικά, $\dim(V) = 1 \Leftrightarrow V$ περιέχει μια καμπύλη (ίσως ευθεία), δύναται να περιέχει σημεία, αλλά όχι συνιστώσες διάστασης ≥ 2.
- $\dim($υπερεπιπέδου$) = n - 1 = \dim V(f)$, για οποιοδήποτε f με τυχαίους συντελεστές.
- $\dim(V) = n \Leftrightarrow V = \mathbb{C}^n$.

□

Ορισμός 6.2.5 *Δεδομένου ιδεώδους I σε αντιμεταθετικό δακτύλιο R, το ριζικό ιδεώδες του I (radical ideal) ορίζεται ως* $\sqrt{I} := \{r \in R \,|\, r^n \in I, \exists n > 0\}$.

Παράδειγμα 6.2.6 $\sqrt{(8)} = (2), \sqrt{(12)} = (6), \sqrt{(x^3)} = (x), \sqrt{(x^2, x-2y, y^3)} = (x, y)$. □

Διαισθητικά, το ριζικό ιδεώδες αντιστοιχεί στο ίδιο αλγεβρικό σύνολο, όπου όμως οι ρίζες είναι όλες απλές.

Για κάθε σύνολο $X \subset \mathbb{C}^n$ ορίζουμε το σύνολο $J(X) := \{f \in \mathbb{Q}[x] : f(x) = 0, \forall x \in X\}$, το οποίο είναι ιδεώδες. Επιπλέον ισχύουν τα εξής (άσκηση 6.2.10):

- $J(\mathbb{C}^n) = \emptyset, J(\emptyset) = \mathbb{Q}[x]$,
- $X \subset Y \Rightarrow J(Y) \subset J(X)$,
- $S \subset J(V(S))$, $X \subset V(J(X))$,

όπου $V(S)$ το αλγεβρικό σύνολο πολυωνυμικού συνόλου S. Μπορούμε τώρα να διατυπώσουμε το βασικότερο θεώρημα της αλγεβρικής γεωμετρίας πολυωνύμων, που είναι το θεώρημα των μηδενικών (Nullstellensatz) του Hilbert:

Θεώρημα 6.2.7 (Hilbert's Nullstellensatz) *Για κάθε πολυωνυμικό ιδεώδες I ισχύει*

$$J(V(I)) = \sqrt{I}.$$

Ουσιαστικά, κάθε ιδεώδες του δακτυλίου των πολυωνύμων ορίζει ένα μοναδικό αλγεβρικό σύνολο. Κάθε αλγεβρικό σύνολο μπορεί να οριστεί από ένα ιδεώδες, μοναδικό αν διαλέξουμε το «απλούστερο» ιδεώδες (χωρίς πολλαπλές ρίζες). Το ιδεώδες αυτό είναι το ριζικό ιδεώδες (radical ideal), σύμφωνα με το θεώρημα των μηδενικών (Nullstellensatz) του Hilbert.

Μελετάμε τώρα τον αριθμό των εξισώσεων ως προς τον αριθμό μεταβλητών. Όπως και προηγούμενα, έστω n ο αριθμός των μεταβλητών. Στα γραμμικά συστήματα $n \times n$, το αλγεβρικό σύνολο είναι κενό αν και μόνο αν ο πίνακας M των συντελεστών έχει ορίζουσα$= 0$ (ισοδύναμα τάξη δηλ. rank $< n$) και υπάρχει μια ασύμβατη εξίσωση $0 = \beta, \beta \neq 0$. Βαθμός$(M) = \rho < n$ σημαίνει πως το σύστημα ισοδύναμα γράφεται με ρ εξισώσεις που λύνονται ενώ κάποια από τις επιπλέον $n - \rho$ εξισώσεις είναι ασύμβατη $0 = \beta$. Ουσιαστικά έχουμε περισσότερες ανεξάρτητες εξισώσεις από $\rho =$ πλήθος αγνώστων ως προς τους οποίους επιλύουμε.

Παράδειγμα 6.2.8 $x+2y=-1, 2x+4y=0 \Rightarrow$ τάξη $(M)=1$, ενώ μετά την απαλοιφή η 2η εξίσωση γίνεται $0+0=2$. □

Το αλγεβρικό σύνολο δεν είναι κενό: το πλήθος ανεξάρτητων εξισώσεων είναι ίσο με την τάξη $(M) = \rho \leq n$. Υποπερίπτωση: $\rho = n$, τότε υπάρχει μοναδική λύση, σημείο στο $\mathbb{C}^n$ δηλ. διάσταση αλγεβρικού συνόλου $= 0$. Υποπερίπτωση $\rho < n$, τότε υπάρχει απειρία λύσεων και $n-\rho$ εξισώσεις της μορφής $0=0$, διάσταση αλγεβρικού συνόλου$=n-\rho=$ πλήθος επιπλέον μεταβλητών.

Παράδειγμα 6.2.9 $x+2y=-1, 2x+4y=-2$. Υπάρχει απειρία λύσεων $(-2y-1, y)$ για οποιοδήποτε y (διάσταση αλγεβρικού συνόλου $= 1$). □

Σε δεδομένο πρόβλημα, ένα σύνολο δεδομένων καλείται *γενικό* (generic), ισοδύναμα δεν αποτελούν *ειδικά ή εκφυλισμένα* (degenerate, singular) δεδομένα, όταν λειτουργούν σε αυτό το πρόβλημα όπως τα περισσότερα τέτοια σύνολα. Στην πράξη γενικά δεδομένα υπολογίζονται με μεγάλη πιθανότητα χρησιμοποιώντας τυχαία επιλογή. Πιο αυστηρά, το σύνολο γενικών δεδομένων έχει την ίδια διάσταση με το χώρο όλων των δυνατών δεδομένων, ενώ το σύνολο εκφυλισμένων δεδομένων έχει διάσταση $= 0$ σε αυτό το χώρο.

Εφεξής θεωρούμε πως οι δεδομένες εξισώσεις είναι ανεξάρτητες και πως οι συντελεστές είναι γενικοί. Στα (μη) γραμμικά συστήματα:

- Πλήθος εξισώσεων $>$ πλήθος μεταβλητών (υπερ-προσδιορισμένο) $\Rightarrow$ γενικά δεν υπάρχουν ρίζες.
- Πλήθος εξισώσεων $=$ πλήθος μεταβλητών (καλώς ορισμένο) $\Rightarrow$ γενικά υπάρχει πεπερασμένο πλήθος ριζών, το οποίο φράσσεται από τα διάφορα όρια (στα γραμμικά συστήματα μοναδική ρίζα). Διάσταση αλγεβρικού συνόλου$=0$.
- Πλήθος εξισώσεων $<$ πλήθος μεταβλητών (υπο-προσδιορισμένο) $\Rightarrow$ απειρία λύσεων, διάσταση συνόλου > 0.

Άσκηση 6.2.10 Αποδείξτε πως:

1. για κάθε $X \subset \mathbb{C}^n$, το $J(X)$ είναι ιδεώδες,
2. $J(\mathbb{C}^n) = \emptyset, J(\emptyset) = \mathbb{Q}[x]$,
3. $X \subset Y \Rightarrow J(Y) \subset J(X)$,
4. $S \subset J(V(S))$, $X \subset V(J(X))$,

όπου $V(S)$ το αλγεβρικό σύνολο πολυωνυμικού συνόλου S.

6.3 Όρια στον αριθμό των μιγαδικών ριζών

Μελετάμε το όριο Bézout και το αραιό όριο Bernstein [Ber76]. Έστω πολυώνυμα $p_1, \ldots, p_n$ στο $\mathbb{C}[x]$, όπου το $x = (x_1, \ldots, x_n)$ συμβολίζει n μεταβλητές, το καθένα συνολικού βαθμού $\deg\ p_i$.

Ορισμός 6.3.1 *Ο προβολικός χώρος $\mathbb{P}^n_{\mathbb{C}}$, ή απλούστερα $\mathbb{P}^n$, είναι το σύνολο, διάστασης n, των κλάσεων ισοδυναμίας των διανυσμάτων στο $\mathbb{C}^{n+1}$ που έχουν τουλάχιστον ένα μη μηδενικό στοιχείο, όπου ταυτίζουμε διανύσματα που διαφέρουν κατά ένα μη μηδενικό σταθερό πολλαπλάσιο:*

$$\mathbb{P}^n := \{(\alpha_1 : \cdots : \alpha_{n+1}) \in \mathbb{C}^{n+1} | (\alpha_1 : \cdots : \alpha_{n+1}) \neq 0^{n+1}, (\alpha_1 : \cdots : \alpha_{n+1}) \sim (\lambda\alpha_1 : \cdots : \lambda\alpha_{n+1}), \lambda \in \mathbb{C}^*\}.$$

Ο προβολικός χώρος $\mathbb{P}^n$ προβάλλεται με 1-1 αντιστοιχία στον $\mathbb{C}^n$ εάν θέσουμε $\alpha_{n+1} = 1$, και προβάλλεται στο άπειρο εάν θέσουμε $\alpha_{n+1} = 0$.

Θεώρημα 6.3.2 [Béz79] *Το πλήθος των κοινών ριζών στο $\mathbb{P}^n_{\mathbb{C}}$ για σύστημα πολυωνύμων $p_1, \ldots, p_n$ με n μεταβλητές και δεδομένους συνολικούς βαθμούς $\deg p_i$ φράσσεται από το*

$$\prod_{i=1}^{n} \deg\ p_i,$$

όπου οι πολλαπλές ρίζες μετρούνται με την πολλαπλότητά τους. Εάν οι συντελεστές είναι γενικοί (δηλ. αρκετά τυχαίοι) τότε το όριο είναι ακριβές.

Υπάρχουν βελτιώσεις επί του θεωρήματος όταν τα πολυώνυμα γράφονται ως άθροισμα ομογενών όρων, όπου κάθε όρος έχει συγκεκριμένο βαθμό ως προς ένα υποσύνολο των μεταβλητών. Ένα τέτοιο σύστημα καλείται πολυ-ομογενές (m-homogeneous) [DE03, MSW94]. Ειδικότερα:

Ορισμός 6.3.3 *Έστω μια διαμέριση των μεταβλητών σε m υποσύνολα $X_1, \ldots, X_m$. Ένα πολυώνυμο καλείται* πολυ-ομογενές *ή m-ομογενές αν είναι ομογενές ως προς κάθε υποσύνολο X_i για $i = 1, \ldots, m$.*

Με άλλα λόγια, το πολυώνυμο ομογενοποιείται με την εισαγωγή μιας τεχνητής μεταβλητής για κάθε υποσύνολο X_i. Παρατηρήστε πως το πολυώνυμο είναι συνεπώς και ομογενές. Ένα σύστημα που αποτελείται από πολυ-ομογενή πολυώνυμα, ως προς την ίδια διαμέριση μεταβλητών, καλείται m-ομογενές.

Έστω η διαμέριση των μεταβλητών $X_1, \ldots, X_m$, όπου το υποσύνολο X_i περιέχει n_i μεταβλητές και $n_1 + \cdots + n_m = n$ το σύνολο των μεταβλητών. Έστω ένα m-ομογενές σύστημα n πολυωνύμων, όπου το i-στό πολυώνυμο έχει βαθμό d_{ij} ως προς τις μεταβλητές X_j, κατόπιν ομογενοποίησης με την εισαγωγής της μεταβλητής με αριθμό $n_j + 1$.

Παράδειγμα 6.3.4 Το $f = c_{110}x_1x_2y_0 + c_{201}x_1^2y_1 + c_{111}x_1x_2y_1 + c_{001}x_0^2y_1$ είναι πολυ-ομογενές ως προς τα $X_1 = (x_0, x_1, x_2)$, $X_2 = (y_0, y_1)$ με $m = 2$, όπου $n_1 = 2, n_2 = 1$ και $d_1 = 2, d_2 = 1$. □

Θεώρημα 6.3.5 *[m-Bézout] Το πολυομογενές φράγμα m-Bézout φράσσει το πλήθος των απομονωμένων ριζών στο $\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_m}$ από τον συντελεστή του $y_1^{n_1} \cdots y_m^{n_m}$ στο νέο πολυώνυμο*

$$\prod_{i=1}^{n} (d_{i1}y_1 + \cdots + d_{im}y_m)$$

Για πολυώνυμα με τυχαίους συντελεστές, το φράγμα είναι ακριβές.

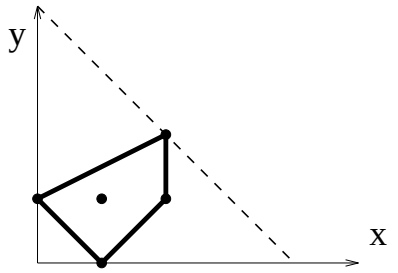
Τα πολυ-ομογενή πολυώνυμα προσφέρουν μια ενδιάμεση θεώρηση μεταξύ της κλασικής προβολικής θεωρίας και της θεωρίας αραιής απαλοιφής. Παρακάτω εξετάζουμε τη θεωρία της αραιής απαλοιφής (sparse, or toric, elimination) που γενικεύει όλα τα παραπάνω όρια [CLO05].

Ορισμός 6.3.6 *Έστω πολυώνυμο n μεταβλητών με m μη-μηδενικούς όρους. Θεωρούμε τα ακέραια διανύσματα των m εκθετών ως σημεία στον $n-$διάστατο χώρο. Το κυρτό περίβλημα των m σημείων (μικρότερο κυρτό πολύεδρο που περιλαμβάνει τα σημεία) καλείται* πολύεδρο του Νεύτωνα *του πολυωνύμου.*

Συνεπώς το πολύεδρο του Νεύτωνα εξαρτάται μόνο από ένα υποσύνολο των μη μηδενικών όρων, αλλά όχι από την ακριβή τιμή των συντελεστών τους. Το πολύεδρο του Νεύτωνα εκφράζει την «πολυπλοκότητα» του πολυωνύμου, με μεγαλύτερη ακρίβεια απ΄ό,τι ο συνολικός βαθμός.

Παράδειγμα 6.3.7 Στο πολυώνυμο $P(x,y) = 3x^2 - y + 2xy + 5x^2y + 6x^2y^2 - 2x^3y^2$ αντιστοιχούμε το σύνολο των εκθετών που εμφανίζονται $\{(2,0),(0,1),(1,1),(2,1),(2,2),(3,2)\}$. □

Έστω μια εξίσωση $f = c_0 + c_1x + \cdots + c_bx^b$ ως προς x, βαθμού b. Το πολύεδρο του Νεύτωνα εδώ είναι το ευθύγραμμο τμήμα $[0,b]$ και ο όγκος του ισούται με το μήκος b. Γνωρίζουμε από το Θεμελιώδες Θεώρημα της Άλγεβρας πως το πλήθος των μιγαδικών ριζών της εξίσωσης $f = 0$ ισούται με b. Αν έχουμε 2 εξισώσεις με 2 αγνώστους x, y, οι οποίες έχουν το ίδιο πολύεδρο του Νεύτωνα (το οποίο ονομάζουμε P), τότε το διπλάσιο του όγκου του πολυέδρου ισούται με το πλήθος των κοινών μιγαδικών ριζών του συστήματος, δηλ. το πλήθος των ζευγών (x,y) για τα οποία και οι 2 εξισώσεις μηδενίζονται.



Σχήμα 6.1: Πολύγωνο του Νεύτωνα για αραιό πολυώνυμο 2 μεταβλητών συνολικού βαθμού 4 και αντίστοιχο πολύγωνο του Νεύτωνα για αντίστοιχο πυκνό πολυώνυμο με τον ίδιο συνολικό βαθμό.

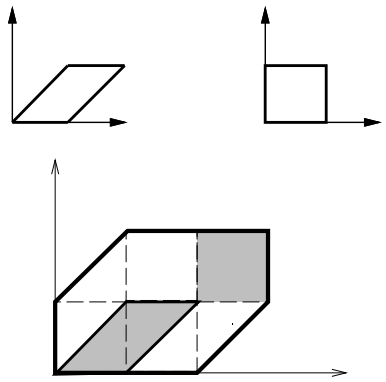
Γενικά, ένα σύστημα n εξισώσεων με n αγνώστους, όπου όλα τα πολύεδρα του Νεύτωνα είναι ίδια, έχει το πολύ $n!V$ μιγαδικές ρίζες, όπου V ο όγκος του πολυέδρου του Νεύτωνα. Αυτό αποτελεί ειδική περίπτωση του παρακάτω θεωρήματος 6.3.9.

Γενικότερα, υπάρχουν όρια στο πλήθος ριζών συστήματος πολυωνύμων σε συνάρτηση του Μικτού όγκου των αντίστοιχων πολυέδρων του Νεύτωνα, ακριβέστερα από τα κλασικά όρια του Bézout, τα οποία αποτελούν συνάρτηση του συνολικού βαθμού. Για να δούμε πώς το πολύγωνο του Νεύτωνα δίνει ακριβέστερη πληροφορία από τον συνολικό βαθμό, θεωρήστε το παράδειγμα στο σχήμα 6.1. Είναι σαφές πως το πολύγωνο αυτό είναι πολύ μικρότερο από το αντίστοιχο πολύγωνο (τρίγωνο) του Νεύτωνα για πυκνό πολυώνυμο συνολικού βαθμού 4, το οποίο φαίνεται με διακεκομμένες γραμμές.

Παράδειγμα 6.3.8 Έστω τα πολυώνυμα $c_0+c_1x+c_2x^2y+c_3xy, b_0+b_1x+b_2y+b_3xy$, και οποιαδήποτε μη-μηδενικά c_i, b_i. Το σχ. 6.2 δείχνει τα αντίστοιχα πολύγωνα του Νεύτωνα.

□

Διανυσματικό άθροισμα (ή άθροισμα Minkowski) $A+B$ δύο συνόλων (πεπερασμένων ή άπειρων) ακέραιων διανυσμάτων είναι $\{\alpha+\beta : \alpha \in A, \beta \in B\}$. Εάν A, B κυρτά σύνολα τότε $A+B$ κυρτό. Ορίζεται επίσης ο μικτός όγκος των πολυέδρων, ο οποίος μπορεί να υπολογιστεί μέσω του αθροίσματος Minkowski. Το άθροισμα Minkowski δύο σημειοσυνόλων A, B είναι το σημειοσύνολο $A+B$ που περιέχει όλα τα



Σχήμα 6.2: Δύο πολύγωνα Νεύτωνα, άθροισμα Minkowski, μικτή υποδιαίρεση, και υπολογισμός μικτού όγκου.

διανυσματικά αθροίσματα $a+b$ για κάθε $a \in A, b \in B$. Το άθροισμα Minkowski 2 πολυγώνων φαίνεται στο σχήμα 6.2 παρακάτω. Στο ίδιο σχήμα δείχνουμε και μια «μικτή υποδιαίρεση» του αθροίσματος Minkowski με την οποία υπολογίζουμε το Μικτό όγκο και, τελικά, ένα φράγμα στο πλήθος ριζών των αντίστοιχων πολυωνύμων. Στο παράδειγμα (σχήμα 6.2) ο Μικτός όγκος ισούται με 3.

Θεώρημα 6.3.9 [Ber76] *Ο μικτός όγκος των n πολυέδρων Νεύτωνα των πολυωνύμων φράσσει το πλήθος των κοινών ριζών στο* $(\mathbb{C}-\{0\})^n$ *για οποιοδήποτε σύστημα με δεδομένους τους μη-μηδενικούς όρους. Οι πολλαπλότητες συνυπολογίζονται, ενώ σπάνια προσμετρούνται ρίζες στο άπειρο. Εάν οι συντελεστές είναι γενικοί τότε το όριο είναι ακριβές.*

Το όριο Bernstein είναι επίσης γνωστό ως όριο Bernstein-Khovanskii-Kushnirenko.

Η χρησιμότητα του ορίου δικαιολογείται από 2 παράγοντες: (α) Τυπικά είναι πολύ κατώτερο του ορίου Bézout, (β) εξαρτάται μόνο από τα πολύεδρα του Νεύτωνα των πολυωνύμων οπότε είναι συνάρτηση της δομής των πολυωνύμων και της αραιότητάς τους (καλείται και αραιό όριο).

Για απολύτως πυκνά πολυώνυμα (μη μηδενικοί όλοι οι δυνατοί όροι) τα όρια Bernstein και Bézout συμπίπτουν. Υπάρχει μια επέκταση [HS97] στο $\mathbb{C}^n$.

Παράδειγμα 6.3.10 Στη δομική βιολογία, μελετάμε τις διαμορφώσεις του κυκλοεξανίου, δηλ. ενός δακτυλίου έξι σημειακών μαζών, με 6 περιστρεφόμενους βαθμούς ελευθερίας. Από την γεωμετρία αποστάσεων ή την Ευκλείδειο γεωμετρία, κατασκευάζουμε ένα σύστημα 3×3 που περιγράφει τις δυνατές διαμορφώσεις:

$$f_i = \beta_{i1} + \beta_{i2} t_j^2 + \beta_{i3} t_k^2 + \beta_{i4} t_j t_k + \beta_{i5} t_j^2 t_k^2, \qquad \{i,j,k\} = 0,1,2.$$

Οι μεταβλητές t_0, t_1, t_2 αντιστοιχούν στην εφαπτόμενη της μισής γωνίας των 3 αλγεβρικώς ανεξάρτητων γωνιών, οι οποίες καθορίζουν μια διαμόρφωση.

Το φράγμα Bézout ισούται με $4^3 = 64$.

Το πολυομογενές φράγμα m-Bézout φράσσει το πλήθος ριζών στο $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$. Οι βαθμοί των πολυωνύμων στις μεταβλητές t_0, t_1, t_2 είναι αντίστοιχα $(0,2,2), (2,0,2), (2,2,0)$. Το φράγμα ισούται με τον συντελεστή του $y_1 y_2 y_3$ στο

$$\prod_i (d_{i1} y_1 + d_{i2} y_2 + d_{i3} y_3) = \cdots + (2y_2 + 2y_3)(2y_1 + 2y_3)(2y_1 + 2y_2) + \cdots = \cdots + 2y_2 \cdot 2y_1 \cdot 2y_3 + 2y_3 \cdot 2y_1 \cdot 2y_2 + \cdots$$

δηλ. το φράγμα είναι 16.

Τέλος, θεωρούμε τα 3 πολύεδρα του Νεύτωνα Q_0, Q_1, Q_2. Είναι και τα 3 τετράγωνα, με μήκος ακμής 2, που βρίσκονται σε διαφορετικά επίπεδα, δηλ. στο επίπεδο των t_1t_2, των t_0t_2 και των t_0t_1 αντίστοιχα. Το άθροισμα Minkowski $Q_0 + Q_1 + Q_2$ είναι κύβος με μήκος ακμής 4 και όγκο $4^3 = 64$. Ο Μικτός Όγκος των 3 πολυέδρων είναι, από τον τύπο εγκλεισμού-αποκλεισμού,

$$V(Q_0 + Q_1 + Q_2) - \sum_{i \neq j} V(Q_i + Q_j) + \sum_i V(Q_i) = 4^3 - 3 \cdot 4 \cdot 2 \cdot 2 + 0 = 16,$$

όπου κάθε άθροισμα $Q_i + Q_j$ είναι ορθογώνιο παραλληλεπίπεδο με μήκος ακμών $4, 2, 2$. □

6.4 Μέθοδος της απαλοίφουσας

Η *απαλοίφουσας (ή επιλύουσα)* (resultant or eliminant) παρέχει μια Συνθήκη ύπαρξης ριζών σε ένα υπερ-προσδιορισμένα σύστημα $n+1$ πολυωνύμων σε δακτύλιο $K[x_1, \ldots, x_n]$. Δες: [CLO05].

Ορισμός 6.4.1 *Η απαλοίφουσα R του συστήματος $n+1$ πολυωνύμων σε n μεταβλητές και με συμβολικούς συντελεστές είναι ένα πολυώνυμο με ακέραιους συντελεστές και μεταβλητές τους συμβολικούς συντελεστές του αρχικού συστήματος. Όταν οι συμβολικοί συντελεστές λάβουν συγκεκριμένες τιμές, $R = 0$ αν και μόνο αν το αρχικό σύστημα έχει κοινή ρίζα.*

Ο παραπάνω ορισμός είναι ηθελημένα ασαφής ως προς τον χώρο των κοινών ριζών. Θα δούμε παρακάτω, πως η ύπαρξη προβολικών ριζών εκφράζεται από την προβολική (κλασική) απαλοίφουσα, ενώ η τορική απαλοίφουσα εκφράζει την ύπαρξη ριζών σε ένα τορικό αλγεβρικό σύνολο.

Για συστήματα δύο πολυωνύμων με $n = 1$, η συζήτηση της απαλοίφουσας βρίσκεται στην ενότητα 4.3 όπου ορίζεται ο πίνακας Sylvester S. Θυμίζουμε το θεώρημα 4.3.2:

Θεώρημα 6.4.2 *Έστω 2 πολυώνυμα στο $\mathbb{Z}[x]$. Υποθέτουμε ότι τουλάχιστον ένας εκ των μεγιστοβάθμιων όρων των πολυωνύμων είναι μη μηδενικός. Τότε $\det S = 0$ αν και μόνο αν τα πολυώνυμα έχουν κοινή ρίζα.*

Ο πίνακας Sylvester περιέχει 2 υποπίνακες Toeplitz άρα είναι Toeplitz κατά ομάδες γραμμών.

6.4.1 Γραμμικά συστήματα $n+1$ πολυωνύμων

Έστω γραμμικό σύστημα $n+1$ πολυωνύμων που γράφεται ως $Ax = b, x \in \mathbb{C}^n, b \in \mathbb{C}^{n+1}$, όπου ο A είναι ο πίνακας των συντελεστών των $n+1$ πολυωνύμων και διάστασης $(n+1) \times n$. Το σύστημα έχει κοινή ρίζα αν και μόνο αν το σταθερό διάνυσμα b ανήκει στον χώρο των στηλών του πίνακα $A \Leftrightarrow$ τάξη$(M) < n+1 \Leftrightarrow \det M = 0$, όπου ο πίνακας $M = [Ab]$ είναι $(n+1) \times (n+1)$ και ισούται με τον πίνακα A των συντελεστών επαυξημένο με τη στήλη b.

Έστω M_{ij} ο υποπίνακας $n \times n$ που προκύπτει από το M σβήνοντας τη γραμμή και τη στήλη που περιέχουν το στοιχείο (i, j). Όταν $\det M_{(n+1)(n+1)} \neq 0$ τότε λύνουμε το αντίστοιχο υποσύστημα με τον κανόνα Cramer ώστε $\alpha_j = (-1)^j \det M_{(n+1)j} / \det M_{(n+1)(n+1)}$. Αυτή είναι ρίζα και της τελευταίας εξίσωσης αν και μόνο αν

$$\begin{aligned} & c_{(n+1)1}\alpha_1 + \ldots + c_{(n+1)n}\alpha_n = b_{n+1} \Leftrightarrow \\ & \Leftrightarrow c_{(n+1)1}(-1) \det M_{(n+1)1} + \ldots + c_{(n+1)n}(-1)^n \det M_{(n+1)n} = b_{n+1} \det M_{(n+1)(n+1)} \\ & \Leftrightarrow \det M = 0 \end{aligned} \tag{6.1}$$

επειδή παρατηρούμε πως πρόκειται για το ανάπτυγμα της $\det M$ ως προς την τελευταία σειρά.

Παράδειγμα 6.4.3 $x+2y=-1, 2x+3y=0, x+y=1 \Rightarrow$ τάξη $(M)=2$, κοινή ρίζα $=(3,-2)$. □

Αυτή η ορίζουσα $\det M$ ισούται με την απαλοίφουσα του γραμμικού συστήματος. Οι στήλες του M αντιστοιχούν στις δυνάμεις του x ενώ οι γραμμές περιέχουν τα πολυώνυμα p_i. Αν τάξη $(M)=n$ τότε υπάρχει μοναδική ρίζα, αλλιώς απειρία λύσεων.

Για $\alpha=[\alpha_1,\ldots,\alpha_n,1]$, $M\alpha=$ διάνυσμα τιμών πολυωνύμων στο σημείο α άρα (ανάμεσα) στα μηδενικά διανύσματα που βρίσκονται στον πυρήνα του M υπάρχει το διάνυσμα που αποτελείται από τις συντεταγμένες της κοινής ρίζας.

Παρατήρηση: ο πολλαπλασιασμός από αριστερά διανύσματος $w=[w_1,\ldots,w_{n+1}]$ επί M δίνει ένα γινόμενο διάνυσμα που αντιπροσωπεύει το $\Sigma_{i=1,\ldots,n+1}w_ip_i$.

6.4.2 Γενικά συστήματα $n+1$ πολυωνύμων

Θυμηθείτε τον ορισμό 6.4.1, που ορίζει την απαλοίφουσα R ενός υπερ-προσδιορισμένου συστήματος $n+1$ πολυωνύμων σε n μεταβλητές ως το « μικρότερο » πολυώνυμο στους συντελεστές των $n+1$ πολυωνύμων, το οποίο εκφράζει την επιλυσιμότητα του υπερ-προσδιορισμένου συστήματος.

Θεώρημα 6.4.4 *Τύπος Poisson: $R=C\prod_{\alpha\in A}p_k(\alpha)$, όπου A είναι το σύνολο κοινών ριζών των $p_1,\ldots,p_{k-1},p_{k+1},\ldots,p_{n+1}$ και C μια σταθερά ανεξάρτητη από τους συντελεστές του p_k.*

Πόρισμα 6.4.5 *Ο βαθμός της απαλοίφουσας ως προς τους συντελεστές του $p_k(x)$ δίνεται από το όριο στο πλήθος κοινών ριζών των $p_1,\ldots,p_{k-1},p_{k+1},\ldots,p_{n+1}$.*

Ορισμός 6.4.6 *Η κλασική απαλοίφουσα [Euler,Cayley,Sylvester,Bézout] αφορά στις προβολικές μιγαδικές ρίζες συνεπώς ο βαθμός της ως προς τους συμβολικούς συντελεστές του αρχικού συστήματος εξαρτάται από το όριο Bézout, ενώ στον τύπο Poisson το A περιλαμβάνει όλες τις μιγαδικές προβολικές ρίζες.*

Στη θεωρία αραιής απαλοιφής, μελετάμε τορικά αλγεβρικά σύνολα T που ορίζονται από τα πολύεδρα του Νεύτωνα. Γενικά, κάθε T περιέχει το $(\mathbb{C}-\{0\})^n$ ως πυκνό υποσύνολο και βρίσκεται μέσα στο $\mathbb{P}^N$, όπου N το πλήθος όψεων στο άθροισμα Minkowski των πολυέδρων του Νεύτωνα. Άρα το T μπορεί να τέμνει τον προβολικό χώρο στο άπειρο για συγκεκριμένους, μη γενικούς συντελεστές.

Ορισμός 6.4.7 [CLO05, GKZ94, PS93] *Η αραιή απαλοίφουσα εκφράζει την ύπαρξη ριζών σε ένα τορικό αλγεβρικό σύνολο T συνεπώς ο βαθμός της συναρτάται από το όριο Bernstein ενώ $A\subset T$.*

Αντίθετα με τις προηγούμενες ειδικές περιπτώσεις μίας μεταβλητής και γραμμικών συστημάτων, δεν υπάρχει γενικός τύπος για την απαλοίφουσα σε συνάρτηση των συντελεστών. Πρόσφατα, κατασκευάστηκαν οι απαλοίφουσες ορισμένων νέων κατηγοριών συστημάτων ως ορίζουσες [DE03, Khe03].

Γενικά, πάντως, αρκούμαστε στον υπολογισμό πολλαπλασίων της ως ορίζουσες πινάκων που γενικεύουν τον πίνακα συντελεστών γραμμικού συστήματος και τον πίνακα Sylvester. Επιδιώκουμε συνεπώς να κατασκευάσουμε τετράγωνους πίνακες M για τους οποίους:

- η ορίζουσα $\det M$ δεν είναι γενικά μηδέν,

- η ορίζουσα $\det M$ διαιρείται από την απαλοίφουσα, άρα αποτελεί μια αναγκαία συνθήκη ύπαρξης ριζών,
- ο πίνακας M έχει το μικρότερο δυνατό μέγεθος και οι επιπλέον παρασιτικές ρίζες που μηδενίζουν $\det M$ χωρίς να είναι ρίζες του συστήματος είναι σημειακές δηλ. διάστασης$= 0$, ειδάλλως απαιτούνται ειδικές επιπρόσθετες πράξεις πινάκων.

Υπάρχουν οι εξής βασικοί τύποι πινάκων:

Bézout ή Dixon [Dix08, EM00], όπου τα στοιχεία είναι πολυώνυμα ως προς τους συμβολικούς αρχικούς συντελεστές, επομένως έχουν μικρότερο μέγεθος και συχνά λιγότερες εξαιρέσεις.

Sylvester που στην γενική περίπτωση ερευνήθηκε από το [Mac02] για την κλασική απαλοίφουσα και τους [CE93, CE00, D'A02, Stu93, Stu94] (τύπος Newton) για την αραιή.

Υβριδικός αποτελεί συνδυασμό των 2 παραπάνω, π.χ. [DD01].

6.4.3 Κατασκευή πινάκων τύπου Sylvester

Μας ενδιαφέρουν πίνακες απαλοίφουσας τύπου Sylvester. Η βέλτιστη (δηλ. ελάχιστη) διάστασή τους ισούται με τον συνολικό βαθμό της απαλοίφουσας. Σ' αυτή την περίπτωση η ορίζουσά τους δίνει την απαλοίφουσα ως πολυώνυμο στους αρχικούς συντελεστές. Άρα ο πίνακας των συντελεστών γραμμικού συστήματος και ο πίνακας Sylvester είναι οι μικρότεροι δυνατοί.

Ο πίνακας κατασκευάζεται ως γενίκευση του πίνακα Sylvester με $n+1$ ομάδες γραμμών, μία ανά πολυώνυμο. Οι γραμμές στην ομάδα $i = 1, \ldots, n+1$ εκφράζουν τα πολλαπλάσια του δεδομένου πολυωνύμου p_i επί ένα σύνολο από μονώνυμα B_i. Οι στήλες στον πίνακα αντιστοιχούν στα μονώνυμα C, έτσι ώστε

$$\sum_{i=1}^{n+1} |B_i| = |C|,\ \det M \neq 0,\ R|\det M.$$

Ο πίνακας τύπου Sylvester έχει την γνωστή ιδιότητα πολλαπλασιασμού με διάνυσμα από δεξιά: έστω v ένα διάνυσμα που περιέχει τις τιμές των μονωνύμων C σε κάποιο $n-$διάστατο σημείο α. Τότε Mv εκφράζει τις τιμές των πολυωνύμων των γραμμών στο α. Εάν α είναι κοινή ρίζα των $n+1$ πολυωνύμων, τότε v ανήκει στον πυρήνα του M. Αυτή η ιδιότητα οδηγεί στο παρακάτω:

Λήμμα 6.4.8 *Έστω τετράγωνος πίνακας M τύπου Sylvester, δηλ. με γραμμές που αντιστοιχούν σε γινόμενα των $n+1$ πολυωνύμων επί μονώνυμα στις n μεταβλητές. Η ορίζουσα $\det M$ διαιρείται από την προβολική ή την τορική απαλοίφουσα του συστήματος.*

Απόδειξη. Αν το πολυωνυμικό σύστημα έχει κοινή ρίζα α, τότε κατασκεύασε το διάνυσμα v που περιέχει τις τιμές των μονωνύμων των στηλών στο α. Το γινόμενο Mv περιέχει τις τιμές των πολυωνύμων στο α, άρα πρόκειται για το μηδενικό διάνυσμα.

Στην προβολική περίπτωση, τα μονώνυμα στηλών περιέχουν το 1, άρα $v \neq 0$. Στην τορική περίπτωση, $\alpha \in (\mathbb{C}^*)^n$, άρα $v \neq 0$. Επομένως $\det M = 0$ όποτε μηδενίζεται η προβολική ή τορική απαλοίφουσα. ΟΕΔ

Ομοίως από αριστερά θεωρούμε πως το v περιέχει τους συντελεστές $n+1$ πολυωνύμων q_i σε αντιστοιχία με τα μονώνυμα B_i. Το vM περιέχει τους συντελεστές του $\Sigma_{i=1\ldots n+1} p_i q_i$ σε αντιστοιχία με τα μονώνυμα C.

Αυτή η ιδιότητα φανερώνει μια γενικευμένη δομή Toeplitz. Ο πίνακας τύπου Sylvester περιέχει $n+1$ υποπίνακες με δομή μη-γραμμική Toeplitz, άρα είναι μη-γραμμικός Toeplitz κατά ομάδες γραμμών όπου κάθε ομάδα αντιστοιχεί σε ένα πολυώνυμο, και καλείται quasi-Toeplitz. Παρατηρούμε πως η αντιμετάθεση στηλών (και γραμμών εφόσον δεν παραβιάζεται η ομαδοποίηση) δίνει ένα νέο πίνακα quasi-Toeplitz, με τις ίδιες ιδιότητες.

Πίνακας Macaulay

Μελετάμε τον αλγόριθμο Macaulay για τον πίνακα της προβολικής απαλοίφουσας. Ο αλγόριθμος γενικεύει την κατασκευή Sylvester. Έστω B_i το σύνολο μονωνύμων που πολλαπλασιάζει το πολυώνυμο f_i. Τα B_i θα είναι όλα υποσύνολα του συνόλου μονωνύμων B με συνολικό βαθμό μέχρι

$$\rho := (\sum_{i=0}^{n} d_i) - n.$$

Θέτουμε:

$$B_1 = \{x^a/x_1^{d_1} | a_1 \geq d_1\},\ B_2 = \{x^a/x_2^{d_2} | a_1 < d_1, a_2 \geq d_2\}, \ldots, B_{n+1} = \{x^a | a_i < d_i,\ i = 1, \ldots, n\}.$$

Αποδεικνύεται εύκολα πως τα B_i είναι ξένα μεταξύ τους και διαμερίζουν το B. Επίσης τα μονώνυμα στο γινόμενο $x^a f_i$, για κάθε $x^a \in B_i$, ανήκουν στο B. Άρα ορίζεται τετράγωνος πίνακας M με γραμμές και στήλες που αντιστοιχούν στο B. Η διάσταση του M ισούται με την πληθικότητα του B:

$$\dim M = |B| = \binom{n+\rho}{n}.$$

Βλέπουμε πως $|B_{n+1}| = \prod_i d_i$ δηλ. ισούται με το φράγμα Bézout για το σύστημα $f_1 = \cdots = f_n = 0$, άρα ισούται με τον βαθμό της απαλοίφουσας ως προς τους συντελεστές του f_{n+1}.

Λήμμα 6.4.9 $\det M \neq 0$ *όταν οι συντελεστές των* f_i *βρίσκονται σε γενική θέση. Επιπλέον, κάθε κύρια (principal) υπο-ορίζουσα είναι μη-μηδενική.*

Απόδειξη. Θέτουμε $f_i = x_i^{d_i}$ για $i = 1, \ldots, n$ και $f_0 = 1$. Παρατηρήστε πως τώρα $M = I$ άρα $\det M = 1$. Η ολοκλήρωση της απόδειξης αφήνεται ως άσκηση. ΟΕΔ

Το επίτευγμα του Macaulay ήταν να ορίσει υποπίνακα M' τ.ώ. $R = \det M / \det M'$ [Mac02].

Άσκηση 6.4.10 Εφαρμόστε τον αλγόριθμο Macaulay στην περίπτωση $n = 1$ και στην περίπτωση γραμμικών πολυωνύμων: περιγράψτε τους πίνακες M, M' που προκύπτουν.

Άσκηση 6.4.11 Εφαρμόστε τον αλγόριθμο Macaulay και περιγράψτε τους πίνακες M, M' που προκύπτουν για το σύστημα

$$f_i = a_i x + b_i y + c_i xy + d_i,\ i = 0, 1, 2.$$

Πίνακες της τορικής απαλοίφουσας

Μελετάμε αλγόριθμους κατασκευής πινάκων Newton για την τορική απαλοίφουσα. Οι γραμμές στην ομάδα $i = 1, \ldots, n+1$ ορίζονται από τα B_i, όπου B_i ανήκει στο διανυσματικό άθροισμα των πολυέδρων του Νεύτωνα των άλλων n πολυωνύμων. Οι στήλες αντιστοιχούν στα μονώνυμα C, υποσύνολο του διανυσματικού αθροίσματος όλων των $n+1$ πολυέδρων του Νεύτωνα.

Ο αλγόριθμος [CE93, CE00] χρησιμοποιεί το διανυσματικό άθροισμα των πολυέδρων του Νεύτωνα και κατασκευάζει πίνακες με διάσταση ίση με το πλήθος των ακέραιων σημείων σε μια απειροελάχιστη διατάραξη αυτού του αθροίσματος. Υπάρχει επίσης η βελτίωση των [CP93, Stu94].

Ο αλγόριθμος [EC95] είναι αυξητικός (incremental) και δοκιμάζει διαδοχικούς ορθογώνιους πίνακες μέχρι να βρεθεί κάποιος με πλήρη τάξη (rank) για γενικούς συντελεστές, οπότε και επιλέγεται ένας τετράγωνος υποπίνακας γενικά μη αντιστρέψιμος. Τυπικά, ο αυξητικός δίνει μικρότερους πίνακες από τον προηγούμενο αλγόριθμο.

Ο πίνακας Newton ταυτίζεται με τον πίνακα των συντελεστών, τον πίνακα Sylvester ή Macaulay εάν, αντίστοιχα, το σύστημα είναι γραμμικό, περιέχει 2 πολυώνυμα, ή τα πολυώνυμα είναι απολύτως πυκνά.

Παράδειγμα 6.4.12 (συνέχεια παραδείγματος 6.3.10) Μελετάμε τις διαμορφώσεις του κυκλοεξανίου με αλγεβρικό σύστημα 3×3 (παρατηρήστε την αρίθμηση των εξισώσεων f_1, f_2, f_3):

$$f_i = \beta_{i1} + \beta_{i2} t_j^2 + \beta_{i3} t_k^2 + \beta_{i4} t_j t_k + \beta_{i5} t_j^2 t_k^2, \qquad \{i, j, k\} = 1, 2, 3.$$

Για τη χρήση της απαλοίφουσας θεωρούμε τα 3 πολυώνυμα ως πολυώνυμα σε 2 μεταβλητές t_1, t_2 και συντελεστές $c_{ij} \in \mathbb{Q}[t_3]$:

$$\begin{aligned} f_1 &= c_{11} + c_{12} t_2 + c_{13} t_2^2 = 0, \\ f_2 &= c_{21} + c_{22} t_1 + c_{23} t_1^2 = 0, \\ f_3 &= c_{31} + c_{32} t_2^2 + c_{33} t_1 t_2 + c_{34} t_1^2 + c_{35} t_1^2 t_2^2 = 0. \end{aligned} \tag{6.2}$$

Ο βαθμός της αραιής απαλοίφουσας στα c_{1j} είναι $\mathrm{MO}(f_2, f_3) = 4$, όπου τα αντίστοιχα πολύεδρα Νεύτωνα είναι ένα ευθύγραμμο τμήμα κι ένα τετράγωνο στο $\mathbb{R}^2$. Ομοίως και για το βαθμό στα c_{2j}. Ο βαθμός της αραιής απαλοίφουσας στα c_{3j} είναι 4 διότι τα f_1, f_2 έχουν πολύγωνα Νεύτωνα 2 κάθετα ευθύγραμμα τμήματα. Αρα ο βέλτιστος πίνακας τύπου Sylvester θα είχε μέγεθος 12×12.

Και οι 2 παραπάνω αλγόριθμοι (με χρήση υποδιαίρεσης του αθροίσματος Minkowski κι ο αυξητικός) παράγουν τον παρακάτω πίνακα 16×16:

Οι στήλες του πίνακα αντιστοιχούν στους εξής όρους:

$$\left[1, t_2, t_2^2, t_2^3, t_1, t_1 t_2, t_1 t_2^2, t_1 t_2^3, t_1^2, t_1^2 t_2, t_1^2 t_2^2, t_1^2 t_2^3, t_1^3, t_1^3 t_2, t_1^3 t_2^2, t_1^3 t_2^3\right].$$

□

Κλείνουμε την ενότητα με στοιχεία χρήσιμα για τον αυξητικό αλγόριθμο, ειδικά τον έλεγχο ενός υποψήφιου πίνακα για το αν αποτελεί πίνακα της αραιής απαλοίφουσας. Έστω ορθογώνιος πίνακας M διαστάσεων $a \times c$, $a \geq c$, κατασκευασμένος από τον αυξητικό αλγόριθμο με πλήρη τάξη ο οποίος συνεπώς μας παρέχει έναν πίνακα Newton $c \times c$. Έστω T ένας αντιστρέψιμος πίνακας $t \times a$. Τότε ο $t \times c$ πίνακας TM έχει τις ιδιότητες ενός πίνακα απαλοίφουσας και επίσης παρέχει έναν πίνακα Newton. Θυμηθείτε (ενότητες 3.6, 4.5) πως $\mu(\lambda) | \chi(\lambda) = \det(M - \lambda I)$ ενώ τα δυο πολυώνυμα (ελάχιστο και χαρακτηριστικό) ισούνται αν και μόνο αν όλες οι ιδιοτιμές έχουν μοναδιαία πολλαπλότητα. Φυσικά, $\det A = 0$ αν και μόνο αν είναι μηδέν ο σταθερός όρος του $\chi(x)$ ή, ισοδύναμα, του $\mu(x)$.

$$M_s = \begin{bmatrix}
c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & c_{11} & c_{12} & c_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 & 0 & 0 & 0 & 0 \\
0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} & 0 \\
0 & 0 & 0 & 0 & 0 & c_{31} & 0 & c_{32} & 0 & 0 & c_{33} & 0 & 0 & c_{34} & 0 & c_{35} \\
c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & c_{21} & 0 & 0 & 0 & c_{22} & 0 & 0 & 0 & c_{23}
\end{bmatrix}$$

6.4.4 Επίλυση συστήματος $n \times n$

Χρησιμοποιούμε τον πίνακα της απαλοίφουσας για την αριθμητική προσέγγιση όλων των ριζών. Σε ορισμένα σημεία παρακάτω εστιάζουμε στον πίνακα Newton, ενώ αντίστοιχα μπορούν να χρησιμοποιηθούν και οι άλλοι τύποι πίνακα απαλοίφουσας. Γενικά, υπάρχουν δύο τρόποι ώστε να αναχθούμε σε ένα υπερπροσδιορισμένο σύστημα:

- Προσθέτουμε μια γραμμική εξίσωση $p_0 = x_1u_1 + \cdots + x_nu_n + u_0$ όπου τα $u_1, \ldots, u_n$ είναι τυχαίες σταθερές (ή παράμετροι) και το u_0 είναι μια παράμετρος στο σώμα των συντελεστών, άρα τα στοιχεία του πίνακα της απαλοίφουσας είναι σταθερές και το u_0 (ή και τα $u_1, \ldots, u_n$). Το πολυώνυμο p_0 λέγεται u-πολυώνυμο και η αντίστοιχη απαλοίφουσα λέγεται u-απαλοίφουσα. Άρα $M(u_0) = M_0 + M_1u_0$ όπου M_0, M_1 περιέχουν μόνο σταθερές.

  Πλεονέκτημα: διαχωρίζει τις πολλαπλές ρίζες ως προς κάποιο x_i του αρχικού συστήματος εφόσον $p_0(\alpha) \neq p_0(\alpha')$, για διαφορετικές ρίζες $\alpha \neq \alpha'$. Μειονέκτημα: αυξάνει τον αριθμό των εξισώσεων.

- Κρύβουμε τη μεταβλητή x_n στο πεδίο των συντελεστών ώστε τα n πολυώνυμα θεωρούνται μέλη του δακτυλίου $(\mathbb{C}[x_n])[x_1, \ldots, x_{n-1}]$ δηλ. σε $n-1$ μεταβλητές. Τα στοιχεία του πίνακα είναι σταθερές ή πολυώνυμα του x_n βαθμού μέχρι d, οπότε ο πίνακας γράφεται $M(x_n) = M_0 + M_1x_n + \cdots + M_dx_n^d$ όπου οι πίνακες M_i περιέχουν μόνο σταθερά στοιχεία. Προφανώς αντί για το x_n μπορούμε να επιλέγουμε κάποια άλλη μεταβλητή.

Άσκηση 6.4.13 Αποδείξτε, με χρήση της u-απαλοίφουσας, πως η επίλυση καλώς ορισμένου αλγεβρικού συστήματος ανάγεται στην παραγοντοποίηση ενός πολυωνύμου.

Σε συνέχεια της παραπάνω άσκησης, μπορούμε να υπολογίσουμε μια συντεταγμένη κάθε πραγματικής ρίζας λύνοντας ένα πολυώνυμο σε μια μεταβλητή. Ο υπολογισμός των υπόλοιπων συντεταγμένων με « ανύψωση » προτάθηκε από τον Canny [Can88b] και είναι σήμερα γνωστή ως μέθοδος του Πρωτογενούς στοιχείου (primitive element) ή ως Ρητή Μονοδιάστατη Αναπαράσταση (Rational Univariate Representation), βλ. και [Rou99]. Η μέθοδος παρουσιάζεται στην ενότητα 5.4.

Παράδειγμα 6.4.14 Παρουσιάζουμε ένα παράδειγμα όπου κρύβουμε τη μεταβλητή x για δυο δεδομένα πολυώνυμα σε δυο αγνώστους: $p_1 = y(x+1) + x^2 + 2x - 1, p_2 = -y^2 + 2y + x^2 + 3x - 1 \in (\mathbb{Z}[x])[y]$. Ο πίνακας Sylvester δίνεται παρακάτω κι έχει δεξιό πυρήνα της μορφής $(1, y, y^2)$:

$$S = \begin{bmatrix} x^2+2x-1 & x+1 & 0 \\ 0 & x^2+2x-1 & x+1 \\ x^2+3x-1 & 2 & -1 \end{bmatrix} \Rightarrow \det S = -x^3 - 2x^2 + 3x \Rightarrow x \in \{0, -3, 1\}.$$

Για κάθε λύση του x ο πυρήνας του αντίστοιχου πίνακα δίνει $y = 1, 1, -1$.

Εφόσον το φράγμα Bézout είναι 4, αυτό σημαίνει πως υπάρχει προβολική ρίζα του συστήματος που βρίσκεται στο προβολικό άπειρο $\mathbb{P}^2 \setminus \mathbb{C}^2$, δηλ. για $z = 0$ όπου z η μεταβλητή ομογενοποίησης. Με άλλα λόγια, ψάχνουμε τις ρίζες όταν μηδενίζονται οι μεγιστοβάθμιοι όροι κάθε εξίσωσης, $xy + x^2 = -y^2 + x^2 = 0$. Αν $x = 0 \Rightarrow y = 0$ που δεν αποτελεί δεκτή λύση. Αν $x \neq 0 \Rightarrow y = -x$ και οι λύσεις στο άπειρο είναι $(x : -x : 0)$, δηλ. ένα μονοδιάστατο σύνολο. □

Παράδειγμα 6.4.15 Έστω καλώς ορισμένο γραμμικό σύστημα $f_i = c_{i0}x_0 + \cdots + c_{in}x_n - b_i, i = 0, \ldots, n$. Αυτό εκφράζεται ως $Ax = b$, όπου $x \in \mathbb{C}^{n+1}, b \in \mathbb{C}^{n+1}$. Κρύβοντας τη μεταβλητή x_0, έχουμε

$$[c_{i0}x_0 - b_i \, c_{ij}] \begin{bmatrix} 1 \\ x_1 \\ \vdots \\ x_n \end{bmatrix} = 0 \in \mathbb{C}^{n+1}.$$

Άρα, ισοδύναμα, $x_0[c_{i0}] - [b_i] + [c_{ij}][x_1, \ldots, x_n]^T = 0$, δηλαδή, $[c_{i0} \, c_{ij}][x_0, x_1, \ldots, x_n]^T = [b_i]$. Η εξίσωση αυτή γράφτηκε $Ax = b$ στην ενότητα 6.4.1. □

Με βάση την θεωρία της απαλοίφουσας, μας ενδιαφέρουν οι τιμές της παραμέτρου ή της κρυμμένης μεταβλητής για τις οποίες μηδενίζεται η ορίζουσα του πίνακα της απαλοίφουσας. Και οι 2 μέθοδοι ενοποιούνται και ανάγουν την επίλυση του αρχικού συστήματος στην επίλυση του γραμμικού συστήματος $M(x) = M_0 + M_1 x + \cdots + M_d x^d$, ($d = 1$ στην πρώτη περίπτωση), όπου έστω m η διάστασή του. Διαπιστώνουμε εδώ το πλεονέκτημα της μεθόδου της απαλοίφουσας για την επίλυση συστημάτων.

Στα παρακάτω, έστω I ο μοναδιαίος πίνακας της διάστασης που απαιτείται. Οι τιμές του x που μηδενίζουν την ορίζουσα $\det M(x)$ είναι οι τιμές του u_0 ή του x_n στις ρίζες του αρχικού συστήματος.

- M_d αντιστρέψιμος: Εάν $d = 1, M(x) = 0$ ισοδυναμεί με $\det(-M_1^{-1}M_0 - Ix) = 0$ οπότε οι ρίζες του ξ ανήκουν στο σύνολο των ιδιοτιμών του $-M_1^{-1}M_0$ διάστασης m. Για μεγαλύτερα d, έχουμε $M(x) = M_d x^d + \cdots + M_1 x + M_0$. Η υπόθεση $|M_d| \neq 0$ οδηγεί στο:

  $$\det M(x) = \det M_d \det(I_N x^d + \cdots + M_d^{-1}M_1 x + M_d^{-1}M_0)$$

  και ο $M(x)$ είναι μη-αντιστρέψιμος ανν το x ισούται με τις ιδιοτιμές του συντροφικού πίνακα (companion matrix) C, διάστασης dm. Το ίδιο πρόβλημα γράφεται $\det(C_0 + C_1 x) = 0$ με $\det C_1 \neq 0$, δηλ. $\det(-C_1^{-1}C_0 - Ix) = 0$. Τα ιδιοδιανύσματα v_α του αρχικού πίνακα αντιστοιχούν στα ιδιοδιανύσματα του C ως εξής, όπου β μια ιδιοτιμή του αρχικού πίνακα:

  $$M(\beta)v_\alpha = 0 \Leftrightarrow \left(\begin{bmatrix} 0 & I_N & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & I_N \\ -M_d^{-1}M_0 & \cdots & \cdots & -M_d^{-1}M_{d-1} \end{bmatrix} - \beta I_{Nd} \right) \begin{bmatrix} v_\alpha \\ \beta v_\alpha \\ \vdots \\ \beta^{d-1} v_\alpha \end{bmatrix} = 0.$$

- $\det M_d = 0$: τα x στα οποία μηδενίζεται η $\det(M_0 + M_1 x) = 0$, για $d = 1$, λέγονται γενικευμένες ιδιοτιμές και υπολογίζονται αριθμητικά με κόστος μια κυβική συνάρτηση της διάστασης, αλλά με ψηλότερη σταθερά και χειρότερη αριθμητική ακρίβεια απ' ό,τι οι απλές ιδιοτιμές. Για μεγαλύτερα d, ορίζονται πίνακες A_0, A_1 διάστασης dm, τέτοιοι ώστε το ίδιο πρόβλημα γενικευμένων ιδιοτιμών γράφεται $\det(A_0 + A_1 x) = 0$, με $\det A_1 = 0$. Για μια ιδιοτιμή β και το αντίστοιχο ιδιοδιάνυσμα v_α έχουμε:

$$M(\beta)v_\alpha = 0 \Leftrightarrow \left(\begin{bmatrix} 0 & I_N & & \\ & & \ddots & \\ & & & I_N \\ -M_0 & -M_1 & \cdots & -M_{d-1} \end{bmatrix} - \beta \begin{bmatrix} I_N & & & \\ & \ddots & & \\ & & I_N & \\ & & & M_d \end{bmatrix} \right) \begin{bmatrix} v_\alpha \\ \beta v_\alpha \\ \vdots \\ \beta^{d-1} v_\alpha \end{bmatrix} = 0.$$

Πώς βρίσκουμε τώρα τα υπόλοιπα στοιχεία των διανυσμάτων που αποτελούν ρίζες του αρχικού συστήματος; Χρησιμοποιούμε την ιδιότητα του πίνακα της απαλοίφουσας σχετικά με τον πολλαπλασιασμό επί διάνυσμα από δεξιά, που μας οδηγεί στον υπολογισμό του πυρήνα του $m \times m$ πίνακα $M(x)$. Ενοποιούμε τις περιπτώσεις για κάθε d γράφοντας το πρόβλημα ισοδύναμα ως τον υπολογισμό των διανυσμάτων v τέτοια ώστε $(C_0 + C_1 x)v = 0$, όπου διάσταση πινάκων $= md$.

Έστω v στον πυρήνα δηλ. $(-C_1^{-1}C_0 - Ix)v = 0$ εφόσον ο C_1 είναι αντιστρέψιμος, οπότε αρκεί ο υπολογισμός των ιδιοδιανυσμάτων του $-C_1^{-1}C_0$, διάστασης md. Αν $\det C_1 = 0$ τότε υπολογίζουμε τα γενικευμένα ιδιοδιανύσματα $(C_0 + C_1 x)v = 0$.

Τέλος, τα στοιχεία του v είναι τύπου α^b για μονώνυμο b, άρα μπορούμε να υπολογίσουμε τις συντεταγμένες της ρίζας α με ορισμένες διαιρέσεις. Π.χ.: για $2-$διάστατο α, παίρνουμε δύο στοιχεία με εκθέτες $(1,2)$ και $(1,3)$, άρα το πηλίκο δίνει την 2η συντεταγμένη.

Τα διανύσματα α που υπολογίζουμε από τα (γενικευμένα) ιδιοδιανύσματα είναι συνήθως περισσότερα από τις ρίζες του αρχικού συστήματος, διότι ο πίνακας της απαλοίφουσας δεν έχει συνήθως την βέλτιστη (δηλ. ελάχιστη) διάσταση. Επομένως υπολογίζουμε τις τιμές των αρχικών πολυωνύμων στα α που έχουμε υπολογίσει και απορρίπτουμε αυτά στα οποία τα πολυώνυμα δε μηδενίζονται.

Ο πίνακας της απαλοίφουσας δίνει περαιτέρω πληροφορία. Μια σημαντική πληροφορία αφορά στον πίνακα πολλαπλασιασμού (multiplication table) στον δακτύλιο πηλίκο $K[x]/I$, όπου $K[x]$ ο αρχικός δακτύλιος των πολυωνύμων και I το ιδεώδες που ορίζουν τα $f_1, \ldots, f_n$.

Ας περιοριστούμε, προς το παρόν, στην περίπτωση που η διάσταση του αλγεβρικού συνόλου $V(I)$ είναι μηδέν και το I είναι ριζικό, δηλ. $I = \sqrt{I}$. Ισοδύναμα, το σύστημα $f_1 = \cdots = f_n = 0$ έχει μεμονωμένες ρίζες και απλές. Ο δακτύλιος πηλίκο $K[x]/I$ γράφεται και $K[x] \bmod I$ και περιέχει τις κλάσεις ισοδυναμίας των υπολοίπων κατά την διαίρεση με το I. Από την αντιμεταθετική άλγεβρα γνωρίζουμε πως, όταν $\dim V(I) = 0$, το $K[x]/I$ είναι διανυσματικός χώρος πάνω στο K.

Θεώρημα 6.4.16 *Υποθέτουμε πως $I = \sqrt{I}$, $\dim V(I) = 0$. Έστω $f_0 \in K[x]$ τ.ώ. να έχει διαφορετικές τιμές στις ρίζες του συστήματος $f_1 = \cdots = f_n = 0$. Έστω $B_0 \in \mathbb{N}^n$ το σύνολο μονωνύμων που πολλαπλασιάζουν το f_0 στην κατασκευή Macaulay. Τότε το B_0 είναι βάση του διανυσματικού χώρου $K[x]/I$ πάνω στο K.*

Απόδειξη. Έστω $m = \prod_{i=1}^n \deg(f_i)$ το φράγμα Bézout του συστήματος. Τότε $|B_0| = m$ και θέτουμε $B_0 = \{b_1, \ldots, b_m\}$.

Θα χρησιμοποιήσουμε τον πίνακα M', μεγέθους $m \times m$, που προκύπτει από το συμπλήρωμα Schur στον πίνακα Macaulay, όπως είδαμε παραπάνω. Θυμηθείτε πως οι ιδιοτιμές του M' είναι της μορφής $f_0(\alpha)$, όπου $\alpha \in \mathbb{C}^n$ μια ρίζα του καλώς ορισμένου συστήματος.

Εξ υποθέσεως οι ιδιοτιμές $f_0(\alpha)$ είναι διαφορετικές, άρα υπάρχουν m ιδιοδιανύσματα γραμμικώς ανεξάρτητα της μορφής $[\alpha^{b_1}, \ldots, \alpha^{b_m}]$. Δεδομένου ότι το συνολικό πλήθος ιδιοδιανυσμάτων είναι m, έπεται πως όλα τα ιδιοδιανύσματα είναι της μορφής $[\alpha^{b_1}, \ldots, \alpha^{b_m}]$.

Αν το B_0 δεν είναι βάση του διανυσματικού χώρου, τότε υπάρχουν $k_1, \ldots, k_m \in K$ τέτοια ώστε $\sum_{i=1}^{m} k_i x^{b_i} = 0 \pmod I$, άρα για κάθε ρίζα α έπεται πως $\sum_{i=1}^{m} k_i \alpha^{b_i} = 0$. Θεωρήστε τον πίνακα με στήλες τα ιδιοδιανύσματα του M', ο οποίος είναι αντιστρέψιμος λόγω ανεξαρτησίας των στηλών του. Η παραπάνω σχέση σημαίνει πως αν πολλαπλασιαστεί κάθε γραμμή με k_i, το άθροισμά τους μηδενίζεται, δηλ. ο πίνακας δεν είναι αντιστρέψιμος, πράγμα άτοπο. ΟΕΔ

Οι παραπάνω ιδιότητες έχουν μια βαθύτερη ερμηνεία, η οποία στηρίζεται στο γεγονός πως, όπως θα δούμε παρακάτω, οι πίνακες της απαλοίφουσας μπορούν να εκφράσουν πολλαπλασιασμό πολυωνύμων. Ας ξεκινήσουμε λοιπόν με τον πολλαπλασιασμό πολυωνύμων και τις πράξεις των αντίστοιχων πινάκων. Έστω πίνακας M_f που εκφράζει τον πολλαπλασιασμό με το πολυώνυμο $f(x)$ modulo έναν δεδομένο ιδεώδες I, δηλαδή:

$$[g]^T M_f = [gf \bmod I]^T,$$

όπου $[g], [gf \bmod I]$ το διάνυσμα-στήλη των συντελεστών του $g(x), g(x)f(x) \bmod I$ αντίστοιχα.

Λήμμα 6.4.17 *Το γινόμενο $M_{f_1} M_{f_2}$ ισούται με $M_{f_1 f_2}$ και το άθροισμα $M_{f_1} + M_{f_2}$ ισούται με $M_{f_1+f_2}$.*

Άσκηση 6.4.18 Μελετήστε τον πίνακα Macaulay στην περίπτωση της u-απαλοίφουσας. Αποδείξτε πως με απαλοιφή κατά Gauss προκύπτει τετράγωνος πίνακας διάστασης ίσης με το φράγμα Bézout του αρχικού καλώς προσδιορισμένου συστήματος, ο οποίος εκφράζει τον πολλαπλασιασμό πολυωνύμου mod το ιδεώδες του συστήματος.

6.5 Βάσεις Groebner

Ακολουθούμε την παρουσίαση στο [CLO97, ch.2]. Κάθε μονώνυμο αντιστοιχεί σε ένα μοναδικό ακέραιο διάνυσμα, άρα θα συμβολίζουμε τα μονώνυμα και ως ακέραια διανύσματα.

Ορισμός 6.5.1 *Διάταξη μονωνύμων n μεταβλητών καλείται μια πλήρης διάταξη των αντίστοιχων ακέραιων διανυσμάτων (για κάθε 2 διανύσματα ορίζεται σχέση $<, =$ ή $>$) τέτοια ώστε για διανύσματα α, β, γ, $\alpha > \beta \Rightarrow \alpha + \gamma > \beta + \gamma$ και όλα τα διανύσματα θετικών ακεραίων είναι > 0.*

Ορισμός 6.5.2 *Λεξικογραφική διάταξη: $\alpha >_{lex} \beta$ ανν $\alpha_i = \beta_i$ για $i < k$ και $\alpha_k > \beta_k$.*
Αντίστροφη λεξικογραφική: $\alpha >_{ilx} \beta$ ανν $\alpha_k < \beta_k$ και $\alpha_i = \beta_i$ για $i > k$.
Βαθμωτή λεξικογραφική: $\alpha > \beta$ ανν $|\alpha| > |\beta|$ ή $|\alpha| = |\beta|$ και $\alpha >_{lex} \beta$, όπου $|\alpha|$ είναι η 1-νόρμα του διανύσματος δηλ. το άθροισμα των στοιχείων του.
Αντίστροφη βαθμωτή λεξικογραφική: $\alpha > \beta$ ανν $|\alpha| > |\beta|$ ή $|\alpha| = |\beta|$ και $\alpha >_{ilx} \beta$.

Παράδειγμα 6.5.3 Λεξικογραφικά $x > y > z \Rightarrow x^2 > y > z^2, x^3 > x^2 z > xy^2 > z^2$.
Βαθμωτή λεξικογραφική: $x > y > z \Rightarrow x^2 > z^2 > y, x^2 z^2 > xy^2 z > x^3 > z^2$. □

Θεωρούμε τη διαίρεση με υπόλοιπο πολυωνύμων με n μεταβλητές $x_1, \ldots, x_n$, όπου υπάρχουν s διαιρέτες και διαιρετέος το πολυώνυμο f: $f = q_1 f_1 + \cdots + q_s f_s + r$. Εφόσον έχω ορίσει μια διάταξη μονωνύμων, ο αλγόριθμος διαιρεί κάθε όρο του f με το μεγαλύτερο μονώνυμο κάθε f_i ως προς τη διάταξη. Αν ο όρος του f δεν διαιρείται, τον προσθέτουμε στο τρέχον υπόλοιπο ώστε να πάρουμε τελικά το πολυώνυμο r.

Επομένως, αν $r \neq 0$, κανένας όρος του δεν ανήκει στο ιδεώδες που παράγεται από τα αρχικά μονώνυμα των f_i. Ο αλγόριθμος τερματίζει και το αποτέλεσμα είναι καλώς ορισμένο για δεδομένη διάταξη, αλλά το r δεν είναι μοναδικά ορισμένο εφόσον εξαρτάται από τη σειρά που εξετάζω τα f_i. Αν τα f_i αποτελούσαν μια βάση Gröbner τότε το υπόλοιπον θα ήταν μοναδικό, για τη δεδομένη διάταξη μονωνύμων.

Παράδειγμα 6.5.4 $f = x^2y + xy^2 + y^2, f_1 = xy - 1, f_2 = y^2 - 1 : f = f_1(x + y) + (y^2 + x + y)$ διότι το αρχικό (λεξικογραφικά) μονώνυμο x^2y διαιρείται από το αρχικό xy του f_1. Επίσης, $y^2 + x + y = f_2 + (x + y + 1)$, άρα $f = f_1(x + y) + f_2 + (x + y + 1)$, όπου το πηλίκο δεν περιέχει όρους στο ιδεώδες των αρχικών μονωνύμων των f_i. Αν αλλάξω τη σειρά διαιρέσεων (πρώτα το f_2, μετά το f_1), καταλήγω σε διαφορετικά πηλίκα και υπόλοιπο. □

Ιδεώδες μονωνύμων καλείται κάθε ιδεώδες που παράγεται από κάποιο πεπερασμένο ή μη πεπερασμένο σύνολο μονωνύμων.

Λήμμα 6.5.5 $x^b \in \langle x^a : a \in A \subset \mathbb{N}^n \rangle \Leftrightarrow \exists\, c \in A : x^c \mid x^b$.

Άσκηση 6.5.6 Αποδείξτε το λήμμα.

Λήμμα 6.5.7 $f \in I := \langle x^a : a \in A \subset \mathbb{N}^n \rangle \Leftrightarrow \forall$ *μονώνυμο* x^b *του* f, $x^b \in I$.

Άσκηση 6.5.8 Αποδείξτε το λήμμα.

Πόρισμα 6.5.9 $\langle x^a : a \in A \subset \mathbb{N}^n \rangle = \langle x^b : b \in B \subset \mathbb{N}^n \rangle$ *ανν τα δυο ιδεώδη περιέχουν ακριβώς τα ίδια μονώνυμα (χωρίς καμιά αναφορά στα πολυώνυμα).*

Η συνθήκη ουσιαστικά λέει πως αρκεί να ελέγξουμε αν το A παράγει το B και αντιστρόφως.

Άσκηση 6.5.10 Αποδείξτε το λήμμα.

Θεώρημα 6.5.11 [Λήμμα Dickson] *Κάθε* $I := \langle x^a : a \in A \subset \mathbb{N}^n \rangle$ *έχει μια πεπερασμένη βάση, υποσύνολο του* A.

Απόδειξη. Επαγωγή στο $n =$ πλήθος των μεταβλητών. Για $n = 1$, βάση είναι το x^a με a τον ελάχιστο εκθέτη στο A.

Επαγωγικό βήμα: έστω ένα ιδεώδες μονωνύμων $I \subset K[x_1, \ldots, x_{n-1}, y], J := \langle x^{a_i} : \exists x^{a_i} y^{m_i} \in I \rangle$, όπου $a_i \in \mathbb{N}^{n-1}, m_i \in \mathbb{N}$. Το J είναι ουσιαστικά η «προβολή» του I σε μια διάσταση λιγότερο, οπότε εφαρμόζεται η επαγωγική υπόθεση και υπάρχει πεπερασμένη βάση μονωνύμων ώστε $J = \langle x^{a_1}, \ldots, x^{a_s} \rangle$. Κάθε x^{a_i} αντιστοιχεί σε ένα $x^{a_i} y^{m_i} \in I$. Θέτω $m := \max\{m_1, \ldots, m_s\}$ κι ορίζω $J_k := \langle x^b : \exists x^b y^k \in I \rangle$, $\forall k \in [0, m)$. Σημειώστε πως ορίζεται ομοίως και το J_m, όπου $J_m \subset J$ και μπορεί να έχω $J_m \neq J$.

Αν $B(l)$ είναι η πεπερασμένη βάση μονωνύμων του ιδεώδους μονωνύμων l και $B(l)y^t$ συμβολίζει το σύνολο των στοιχείων της βάσης πολλαπλασιασμένα με το y^t, επιθυμώ να αποδείξω πως

$$I = \left\langle B(J)y^m \cup \left(\cup_{k=0}^{m-1} B(J_k)y^k \right) \right\rangle .$$

Η απόδειξη ανάγεται σε δυο σχέσεις υποσυνόλων. Η σχέση $I \supset \langle \cdots \rangle$ είναι προφανής. Για το αντίστροφο, θεωρώ $x^a y^t \in I$. Αν $t \geq m \Rightarrow x^a \in J$ εξ ορισμού του J και $y^m | y^t$, άρα $x^a y^t \in \langle \cdots \rangle$. Αν $t < m \Rightarrow x^a \in J_t \Rightarrow x^b | x^a$ για κάποιο $x^b \in B(J_t)$ από το λήμμα 6.5.5 και συνεπώς $x^a y^t \in \langle \cdots \rangle$.

Έχουμε βρει λοιπόν μια πεπερασμένη βάση για το I κι αρκεί πλέον να δείξουμε πως τα στοιχεία της ανήκουν στο A. Από το λήμμα 6.5.5, για κάθε στοιχείο της x^b υπάρχει $x^a \in A : x^a | x^b$. Άρα το I παράγεται από όλα τα αντίστοιχα x^a. ΟΕΔ

Παράδειγμα 6.5.12 Έστω ένα ιδεώδες μονωνύμων, που για χάριν απλουστεύσεως δίνεται από μια πεπερασμένη βάση. Παρόλο που τυπικά δεν χρειάζεται το λήμμα του Dickson, ας το εφαρμόσουμε: $I = \langle x^2y^5, x^3y, x^3y^2, x^2y^3, x^2y^4\rangle, J = \langle x^2, x^3, x^4\rangle = \langle x^2\rangle$, $m = 3, J_0 = \emptyset, J_1 = \langle x^3\rangle, J_2 = \langle x^3\rangle$. Εδώ $J_3 = \langle x^2\rangle = J$. Συνεπώς $I = \langle x^2y^3, x^3y, x^3y^2\rangle$. Παρατηρήστε πως δεν πρόκειται για την ελάχιστη βάση διότι $I = \langle x^2y^3, x^3y\rangle$.

Παράδειγμα για $n = 3$: $I = \langle x^3yz^2, x^2y^2z\rangle, J = \langle x^3y, x^2y^2\rangle$, $m = \max\{2, 1\} = 2, J_0 = \emptyset, J_1 = \langle x^2y^2\rangle, J_2 = \langle x^3y, x^2y^2\rangle$. Συνεπώς $I = \langle x^2y^2z, x^3yz^2, x^2y^2z^2\rangle$. Παρατηρήστε πως πρόκειται για μια βάση μεγαλύτερη από την αρχική.

Το τελευταίο βήμα της απόδειξης του λήμματος του Dickson βρίσκει, για κάθε μονώνυμο στα $x^2y^2z, x^3yz^2, x^2y^2z^2$ το αντίστοιχο στην αρχική βάση A δηλ. τα $x^2y^2z, x^3yz^2, x^2y^2z$. Άρα προκύπτει η βάση με την οποία ξεκινήσαμε. □

Τώρα μπορούμε να προχωρήσουμε στο θεώρημα του Hilbert σχετικά με την περατότητα της βάσης κάθε ιδεώδους, που στηρίζεται στο λήμμα του Dickson.

Υποθέστε πως ορίζουμε μια διάταξη μονωνύμων. Τότε για κάθε πολυώνυμο υπάρχει ο αρχικός του όρος (initial term), που συμβολίζεται $A(f)$, καθώς και το αρχικό του μονώνυμο $M(f)$ οπότε $A(f) = cM(f)$ για κάποιο $c \neq 0$. Παρατηρήστε πως $A(f + g) = A(f) + A(g)$.

Έστω μη μηδενικό ιδεώδες I: οι αρχικοί του όροι ορίζουν το σύνολο $A(I) = \{cx^a | \exists f \in I : cx^a = A(f)\}$. Αν τα $f_1, \ldots, f_s$ είναι μια βάση του ιδεώδους I, τότε προφανώς, το ιδεώδες μονωνύμων που παράγουν οι όροι $A(f_i)$ ανήκει στο ιδεώδες μονωνύμων που παράγει το σύνολο $A(I)$, δηλ. $\langle A(f_1), \ldots, A(f_s)\rangle \subset \langle A(I)\rangle$. Θα δούμε πως τα δυο ιδεώδη ισούνται ανν τα $f_1, \ldots, f_s$ είναι μια βάση Gröbner.

Θεώρημα 6.5.13 [Hilbert] *Κάθε ιδεώδες $I \subset K[x_1, \ldots, x_n]$ έχει μια πεπερασμένη βάση.*

Απόδειξη. Από το λήμμα του Dickson, για κάποια $g_i \in I$,

$$\langle A(g_1), \ldots, A(g_t)\rangle = \langle A(I)\rangle,$$

άρα $\langle g_1, \ldots, g_t\rangle \subset I$. Επιθυμούμε να δείξουμε πως τα g_i αποτελούν βάση. Για κάθε $f \in I$ χρησιμοποιώ τον αλγόριθμο της διαίρεσης ως προς κάποια διάταξη μονωνύμων οπότε $f = q_1g_1 + \cdots + q_tg_t + r$. Έχουμε $r \in I \Rightarrow A(r) \in \langle A(I)\rangle = \langle A(g_1), \ldots, A(g_t)\rangle \Rightarrow A(r)$ διαιρείται από κάποιο $A(g_i)$. Συνεπώς το r δεν περιέχει κανέναν όρο δηλ. $r = 0$ και κάθε f όντως παράγεται από τα g_i. ΟΕΔ

Το θεώρημα των αυξανόμενων αλυσίδων ιδεωδών της Noether είναι ισοδύναμο με το θεώρημα 6.5.13 του Hilbert:

Θεώρημα 6.5.14 [Noether] *Για κάθε αλυσίδα ιδεωδών $I_1 \subset I_2 \subset \cdots$ υπάρχει $N \geq 1$ όπου η αλυσίδα σταθεροποιείται δηλ. $I_N = I_{N+1} = \cdots$.*

Μπορούμε τώρα να ορίσουμε τις βάσεις Gröbner και να μελετήσουμε τις ιδιότητές τους. Ονομάστηκαν έτσι από το φοιτητή του Gröbner, τον Buchberger, ο οποίος τις μελέτησε θεωρητικά και αλγοριθμικά, ξεκινώντας στη δεκαετία του '60. Ονομάστηκαν και standard bases, από τον Hironaka, την ίδια εποχή.

Ορισμός 6.5.15 *Για μια δεδομένη διάταξη μονωνύμων και ιδεώδες I, μια βάση του $\langle g_1, \ldots, g_t\rangle = I$ καλείται βάση Gröbner ανν $\langle A(g_1), \ldots, A(g_t)\rangle = \langle A(I)\rangle$.*

Λήμμα 6.5.16 *Έστω $G = \{g_1, \ldots, g_t\}$ μια βάση Gröbner του $I \subset K[x_1, \ldots, x_n]$ και $f \in K[x_i]$. Υπάρχει μοναδικό υπόλοιπο $r \in K[x_i]$ από τη διαίρεση του f με τα g_i τέτοιο ώστε οι όροι του r να μην διαιρούνται από τους $A(g_i)$ και να υπάρχει $g \in I : f = g + r$.*

Απόδειξη. Άσκηση. ΟΕΔ

Λήμμα 6.5.17 *Έστω $G = \{g_i\}_i$ μια βάση Gröbner του I. Τότε $f \in I \Leftrightarrow f \bmod G = 0$.*

Αυτή η ιδιότητα μπορεί χρησιμοποιείται κάποτε ως ορισμός της βάσης Gröbner π.χ. [DST88]. Ακόμη και σ' αυτή την περίπτωση τα πηλίκα q_i δεν είναι μοναδικά διότι εξαρτώνται από τη σειρά εφαρμογής των g_i.

Απόδειξη. Άσκηση. ΟΕΔ

6.6 Αλγόριθμος Buchberger

Για λεπτομέρειες βλ. [CLO97, ch.2], [DEKP99].

Ορισμός 6.6.1 *Έστω πολυώνυμα f, g και μια διάταξη μονωνύμων. Θέτω x^γ = ΕΚΠ των αρχικών μονωνύμων των f, g, δηλ. $\gamma_i = \max\{\alpha_i, \beta_i\} \in \mathbb{N}$ αν x^a, x^b τα αντίστοιχα αρχικά μονώνυμα. Τότε ορίζουμε ως S-πολυώνυμο των f, g το*

$$S(f,g) := \frac{x^\gamma}{A(f)} f - \frac{x^\gamma}{A(g)} g.$$

Στο $S(f, g)$ έχουν απλοποιηθεί οι αρχικοί όροι $A(f), A(g)$. Αν τα f, g ήταν γραμμικά και αντιστοιχούσαν σε γραμμές κάποιου πίνακα με στήλες ορισμένες από ένα διατεταγμένο σύνολο μονωνύμων (θυμηθείτε τους πίνακες της απαλοίφουσας, π.χ.) τότε η πράξη που ορίζει το $S(f, g)$ είναι ο γραμμικός συνδυασμός των δυο αυτών γραμμών στην απαλοιφή του Gauss.

Παράδειγμα 6.6.2 $S(x^3 + 2, x^2 - x + 1) = x^2 - x + 2, S(x^2y - y, xy^2 + x) = -x^2 - y^2$. $S(x^{(2,1,2)} + x^{(2,1,1)}, x^{(1,2,2)}) = x^{(2,2,1)}$ ως προς τη λεξικογραφική διάταξη: παρατηρούμε πως το αρχικό μονώνυμο του $S(f, g)$ δεν είναι απαραίτητα μικρότερο από τα αρχικά μονώνυμα των f, g. Όμως, εάν $M(f)|x^b = M(g) \Rightarrow \gamma = b$ τότε το αρχικό μονώνυμο του $S(f, g)$ είναι μικρότερο του x^b. □

Το παρακάτω λήμμα ισχυρίζεται πως κάθε απλοποίηση αρχικών μονωνύμων σε γραμμικό συνδυασμό πολυωνύμων εκφράζεται από κάποιο σύνολο S-πολυωνύμων. Έστω $M(f)$ το αρχικό μονώνυμο του f.

Λήμμα 6.6.3 *Έστω $f := \sum_i c_i x^{\alpha(i)} g_i$, για κάποιες σταθερές c_i. Υποθέτω πως έχω πολυώνυμα g_i και διάνυσμα $\delta \in \mathbb{N}^n$ τ.ώ. $x^{\alpha(i)} M(g_i) = x^\delta$ για κάθε $c_i \neq 0$. Υποθέτω πως $M(f)$ είναι μικρότερο του x^δ στη διάταξη μονωνύμων. Τότε,*

$$\exists c_{jk} \ : \ f = \sum_{j,k} c_{jk} x^{\delta - \gamma(j,k)} S(g_j, g_k), \quad x^{\gamma(j,k)} = \ \text{ΕΚΠ}\ (M(g_j), M(g_k)).$$

Παρατηρήστε πως $M(S(g_j, g_k)) < x^{\gamma(j,k)} \Rightarrow$ το αρχικό μονώνυμο του αθροίσματος $\sum_{j,k}$ είναι μικρότερο του x^δ.

Θεώρημα 6.6.4 *Έστω $I = \langle g_i \rangle_i$. Τα $\{g_i\}_i$ αποτελούν βάση Gröbner ως προς μια συγκεκριμένη διάταξη μονωνύμων ανν $S(g_i, g_j) \bmod \{g_i\}_i = 0,\ \forall i \neq j$, όπου το υπόλοιπο υπολογίζεται ως προς την ίδια διάταξη μονωνύμων.*

Απόδειξη. [⇒] από το λήμμα 6.5.17.

[⇐] Για $f \in I$ αρκεί να δείξουμε πως $A(f) \in \langle A(g_i) \rangle$. Τώρα, $f = \sum_i h_i g_i$ και θέτω $\delta := \max_i\{\deg(h_i g_i)\} \in \mathbb{N}^n$ όπου $\deg(h_i g_i) \in \mathbb{N}^n$. Υποθέτω πως από όλες τις δυνατές γραφές του f ως πολυωνυμικού συνδυασμού, έχω επιλέξει αυτήν που δίνει το ελάχιστο $\delta \in \mathbb{N}^n$.

Αν $M(f) = x^\delta \Rightarrow x^\delta = \sum_i h'_i M(g_i) \Rightarrow x^\delta \in \langle A(g_i) \rangle$ για κάποια πολυώνυμα h'_i (με support υποσύνολο του support των h_i). Εδώ το θεώρημα αποδείχθηκε.

Αλλιώς, θα καταλήξω σε άτοπο. Έστω πως υπάρχει το εξής υπο-άθροισμα στο f, το μόνο που συνεισφέρει μονώνυμα x^δ:

$$T := \sum_t A(h_t) g_t \ : \ M(h_t g_t) = x^\delta,$$

όπου το αρχικό μονώνυμο του αθροίσματος είναι $M(\sum_t) < \delta$. Από το λήμμα 6.6.3 έπεται πως υπάρχουν σταθερές c_{jk} τ.ώ. το παραπάνω άθροισμα $T = \sum_{j,k} c_{jk} x^{\delta - \gamma(j,k)} S(g_j, g_k)$ όπου $M(S(g_j, g_k)) < x^{\gamma(j,k)}$, χρησιμοποιώντας τους παραπάνω συμβολισμούς. Εξ υποθέσεως, $S(g_j, g_k) \bmod \{g_i\}_i = 0$ άρα

$$S(g_j, g_k) = \sum_i a_i g_i \ : \ M(a_i g_i) \leq M(S(g_j, g_k)),$$

από τον αλγόριθμο διαίρεσης, για κάποια πολυώνυμα a_i. Δηλ. στο άθροισμα του $S(g_j, g_k)$ υπάρχουν προσθετέοι με αρχικά μονώνυμα που δεν απλοποιούνται, δηλ. ισχύει $M(a_i g_i) = M(S(g_j, g_k))$ για κάποιο i. Το παραπάνω υπο-άθροισμα γράφεται

$$T = \sum_{j,k} c_{jk} x^{\delta - \gamma(j,k)} \sum_i a_i g_i,$$

δηλ. το αρχικό του μονώνυμο είναι της μορφής $x^{\delta-\gamma(j,k)} M(a_i g_i) \leq x^{\delta-\gamma(j,k)} M(S(g_j, g_k)) < x^\delta$. Τότε κανένας προσθετέος στο T δεν είναι βαθμού δ, το οποίο είναι αντίθετο με την υπόθεση. ΟΕΔ

Μπορούμε τώρα να διατυπώσουμε τον αλγόριθμο του Buchberger. Με δεδομένο σύνολο $F = \{f_1, \ldots, f_s\}$, ο αλγόριθμος υπολογίζει μια βάση Gröbner $G = \{g_1, \ldots, g_t\}$ του ιδεώδους $I = \langle f_i \rangle_i$ τ.ώ. $F \subset G$.

1. Αρχικοποιώ $G' \leftarrow F$.
2. Επαναλαμβάνω τα εξής βήματα: (α) $G \leftarrow G'$.
   (β) Για κάθε $p \neq q \in G,\ S \leftarrow S(p, q) \bmod G$. Αν $S \neq 0$ τότε $G' \leftarrow G' \cup \{S\}$.
   Η επανάληψη συνεχίζεται μέχρις ότου $G = G'$.

Θεώρημα 6.6.5 *Ο αλγόριθμος τερματίζει και είναι ορθός.*

Απόδειξη. Εκ κατασκευής $F \subset G$. Αφού $S \in I$ τότε $G \subset I$. Εάν τερματίσει ο αλγόριθμος, τότε κάθε $S \bmod G = 0$ άρα πρόκειται για μια βάση Gröbner σύμφωνα με το θεώρημα 6.6.4.

Γιατί τερματίζει ο αλγόριθμος; θεωρήστε το ιδεώδες μονωνύμων $\langle A(g) \rangle_{g \in G}$ το οποίο μεγαλώνει αυστηρά ανν το G μεγαλώνει αυστηρά δηλ. $G \subset G' : G \neq G' \Rightarrow \langle A(g) \rangle_{g \in G} \subset \langle A(g') \rangle_{g' \in G'}, \langle A(g) \rangle \neq \langle A(g') \rangle$. Για να αποδείξουμε την ανισότητα θεωρούμε $S \in G' \neq G$ δηλ. $S \bmod G \neq 0$ άρα $A(S) \notin \langle A(g) \rangle$ ενώ $A(S) \in \langle A(g') \rangle$.

Μια αλυσίδα ιδεωδών δε μπορεί να μεγαλώνει αυστηρά επ' άπειρον και κάποτε τερματίζει, από το θεώρημα της Noether. Άρα και η αλυσίδα των G τερματίζει και συνεπώς κι ο αλγόριθμος. ΟΕΔ

Παράδειγμα 6.6.6 $F = \{f_1 = x^3 - 2xy, f_2 = x^2y - 2y^2 + x\}$ με βαθμωτή λεξικογραφική διάταξη. Το F δεν είναι βάση Gröbner διότι το $f_3 := S(f_1, f_2) = -x^2$ έχει αρχικό μονώνυμο $x^2 \notin \langle x^3, x^2y\rangle$. Υπολογίζουμε

$$f_4 := S(f_1, f_3) = -2xy,\ \ f_5 := S(f_2, f_3) = -2y^2 + x$$

και διαπιστώνουμε πως πλέον όλα τα S-πολυώνυμα μηδενίζονται $\mod\{f_1, \ldots, f_5\}$. Παρατηρήστε πως $A(f_1) \in \langle A(f_i)\rangle_{i\leq 2}$. Αυτό σημαίνει πως μια μικρότερη βάση Gröbner είναι το σύνολο $\{f_2, \ldots, f_5\}$. Επιπλέον $A(f_2) \in \langle A(f_i)\rangle_{i\leq 3}$ άρα μια ακόμη μικρότερη βάση Gröbner είναι το $\{f_3, f_4, f_5\}$.

Πρόκειται για μια *ελάχιστη* βάση Gröbner αν μετατρέψω τα πολυώνυμα σε μονικά. Άλλες βάσεις Gröbner με τον ίδιο πληθικό αριθμό είναι της μορφής $\{x^2 + cxy, xy, y^2 - x/2\}$, για κάθε σταθερά c. □

Ο αλγόριθμος του Buchberger ανάγεται ουσιαστικά σε αυτόν του Ευκλείδη για $n = 1$.

Παράδειγμα 6.6.7 $F = \{f_1 = x^3 + 2x - 3, f_2 = 3x^2 + 2\}$ δίνει $f_3 := S(f_1, f_2) = (4/3)x - 3$ δηλ. το υπόλοιπο $f_1 \bmod f_2$. Διαπιστώνουμε πως $f_1 \bmod \{f_2, f_3\} = 0$ άρα το f_1 δεν είναι απαραίτητο στη βάση. Τώρα $S(f_2, f_3) = (27/4)x + 2$, δηλ. το υπόλοιπο της διαίρεσης με τον αρχικό μόνο όρο του πηλίκου. Συνεχίζοντας παρατηρούμε πως αρκεί να κρατάμε ένα μόνο πολυώνυμο στη βάση, κι αυτό είναι τελικά ο ΜΚΔ. Αυτό ισχύει άλλωστε από την γενική παρατήρηση πως ο δακτύλιος $K[x]$ είναι περιοχή κύριων ιδεωδών (principal ideal domain, βλ. ορισμό 4.1.5) για οποιοδήποτε σώμα K. Ισοδύναμα, όλα τα ιδεώδη του είναι κύρια, δηλ. παράγονται από ένα στοιχείο, το οποίο είναι ο $\text{ΜΚΔ}(f_1, \ldots, f_s)$. □

Ορισμός 6.6.8 *Μια ελάχιστη βάση Gröbner G είναι μια βάση Gröbner τ.ώ. όλοι οι συντελεστές των αρχικών όρων πολυωνύμων στην G να είναι 1 (δηλ. με μονικά πολυώνυμα) και για κάθε $g \in G$ ισχύει $A(g) \notin \langle A(g')\rangle$ για $g' \in G - \{g\}$.*

Αν δεν ισχύει κάποια προϋπόθεση του ορισμού τότε υπολογίζουμε μια «μικρότερη» βάση.

Ορισμός 6.6.9 *Μια* αναγμένη (reduced) *βάση Gröbner G είναι μια βάση Gröbner τ.ώ. όλοι οι συντελεστές των αρχικών όρων πολυωνύμων στην G να είναι 1 (δηλ. με μονικά πολυώνυμα) και για κάθε $g \in G$ και μονώνυμο m του g ισχύει $m \notin \langle A(g')\rangle$ για $g' \in G - \{g\}$.*

Θεώρημα 6.6.10 *Για κάθε ιδεώδες και δεδομένη διάταξη μονωνύμων, υπάρχει μοναδική αναγμένη βάση Gröbner.*

Συνεπώς δυο ιδεώδη ισούνται ανν έχουν την ίδια αναγμένη βάση Gröbner, για συγκεκριμένη διάταξη μονωνύμων.

Η χρησιμότητα των βάσεων Gröbner στη μελέτη και επίλυση αλγεβρικών συστημάτων είναι προφανής, ακόμη κι αν πρόκειται για υπερ- ή υπό-προσδιορισμένα συστήματα. Η βασική ιδιότητα είναι πως το σύνολο λύσεων του αρχικού συστήματος ισούται με το σύνολο λύσεων της βάσης, αφού πρόκειται για το ίδιο ιδεώδες. Αν μια βάση περιέχει μια σταθερά τότε το σύστημα δεν έχει λύσεις στην αλγεβρική θήκη του σώματος των συντελεστών.

Αλλιώς, σε μια λεξικογραφική βάση (με διάταξη $x_1 > \cdots > x_n$) λύνουμε το τελευταίο πολυώνυμο ως προς x_n κι αντικαθιστούμε τις λύσεις στα υπόλοιπα. Το αμέσως προηγούμενο πολυώνυμο περιέχει τώρα μια μεταβλητή x_{n-1} κοκ. Πρόκειται για μια γενίκευση της αντίστοιχης διαδικασίας back-substitution στα γραμμικά συστήματα. Τυπικά, για μια βάση Gröbner G, ορίζουμε τα υποσύνολα $G_i := G \cap K[x_{i+1}, \ldots, x_n]$. Για κάθε i λύνουμε τα $g \in G_i$ ως προς x_{i+1} διότι τα $x_{i+2}, \ldots, x_n$ έχουν πάρει συγκεκριμένες τιμές. Αν υπάρχει i για το οποίο κανένα πολυώνυμο στο G_i δεν περιέχει το x_{i+1} τότε υπάρχουν άπειρες λύσεις, οι οποίες μπορούν να εκφραστούν παραμετρικά με την παράμετρο x_{i+1}.

Παράδειγμα 6.6.11 (Συνέχεια του παραδ. 6.6.6) Ελέγχουμε εάν η βάση $G = \{f_3 = -x^2, f_4 = -2xy, f_5 = -2y^2 + x\}$, που είχαμε υπολογίσει στο παράδ. 6.6.6 με τη βαθμωτή λεξικογραφική διάταξη, είναι επίσης μια λεξικογραφική βάση. Παρατηρούμε πως όλα τα S-πολυώνυμα (ως προς τη λεξικογραφική διάταξη) δίνουν υπόλοιπο 0, εκτός του $f_6 := S(f_1, f_5) \bmod G = 4y^3$. Τώρα όλα τα S-πολυώνυμα μηδενίζονται $\bmod\{f_3, f_4, f_5, f_6\}$ άρα πρόκειται για μια λεξικογραφική βάση. Άρα η μόνη λύση του συστήματος είναι $y = 0 = x$. □

Μια σημαντική εφαρμογή είναι η αλγεβρικοποίηση παραμετρικής (υπερ)επιφάνειας $x_i = f_i(t_1, \ldots, t_m)$. Χρησιμοποιούμε τη λεξικογραφική διάταξη $t_1 > \cdots > t_m > x_1 > \cdots > x_n$ οπότε η βάση Gröbner περιέχει ως τελευταίο πολυώνυμο το $g \in K[x_1, \ldots, x_n]$. Η αλγεβρική έκφραση της επιφάνειας είναι το g ή κάποιος παράγων του, εάν το g ισούται με μια δύναμη f^d ή παραγοντοποιείται $g = f^d h$. Αν υπάρχουν περισσότερα $g_i \in K[x_1, \ldots, x_n]$ τότε η επιφάνεια ανήκει στην τομή των αντίστοιχων αλγεβρικών συνόλων $\cap_i V(g_i)$.

Παράδειγμα 6.6.12 Έστω σφαίρα με παραμετρική αναπαράσταση

$$x = \cos\theta\cos\phi = \frac{1-s^2}{1+s^2}\frac{1-t^2}{1+t^2},\ y = \sin\theta\cos\phi = \frac{2s}{1+s^2}\frac{1-t^2}{1+t^2},\ z = \sin\phi = \frac{2t}{1+t^2}.$$

Στη λεξικογραφική βάση Gröbner έχουμε $g = (x^2 + y^2 + z^2 - 1)^2$ διότι η αρχική παραμετροποίηση καλύπτει τη σφαίρα δυο φορές. □

Κλείνουμε με ορισμένα αποτελέσματα τα οποία περιγράφουν το $K[x]/I, x = (x_1, \ldots, x_n)$. Έστω μια βάση Gröbner G ιδεώδους $I \subset K[x]$ και πολυώνυμο $f \in K[x]$.

Πόρισμα 6.6.13 *Υπάρχει μοναδικό υπόλοιπο $f \bmod G$ που ονομάζεται κανονική μορφή (normal form) του f στο $K[x]/I$ και γράφεται ως K-γραμμικός συνδυασμός μονωνύμων στο συμπλήρωμα του $\langle A(g)\rangle_{g\in G}$ (δηλ. μονωνύμων «κάτω» από τη σκάλα των αρχικών μονωνύμων). Άρα το $K[x]/I$ είναι ισόμορφο με τον διανυσματικό χώρο D στο K που παράγεται από τα $\{x^a \notin \langle A(g)\rangle_{g\in G}\}$.*

Συνεπώς, αν $f' = f \bmod I$, έχουμε $f + g \bmod I = f' + g', fg \bmod I = f'g' \bmod I$.

Θεώρημα 6.6.14 *Αν $K = \mathbb{C}$ ή, γενικότερα, το K είναι αλγεβρικά κλειστό δηλ. ίσο με την αλγεβρική του θήκη, οι επόμενες προτάσεις είναι ισοδύναμες, όπου G μια βάση Gröbner του ιδεώδους I:*

- *Το $V(I)$ είναι πεπερασμένο.*
- *$\forall i, \exists m_i \in \mathbb{N} : x_i^{m_i} \in \langle A(g)\rangle$, άρα $|V(I)| \le \prod_i m_i$. Συγκεκριμένα, το πλήθος ριζών ισούται με το πλήθος μονωνύμων εκτός $\langle A(g) : g \in G\rangle$ δηλ. κάτω από τη σκάλα (staircase).*
- *$\forall i, \exists m_i \in \mathbb{N} : x_i^{m_i} = A(g)$ για κάποιο $g \in G$.*
- *ο διανυσματικός χώρος D έχει $\dim D < \infty$ δηλ. $\dim(\mathbb{C}[x]/I) < \infty$ ως διανυσματικός χώρος στο $\mathbb{C}$. Μάλιστα η διάστασή του ισούται με $|V(I)|$.*

Παράδειγμα 6.6.15 Για $I = \langle x^2 - 2x + 3\rangle, \mathbb{C}[x]/I = \mathbb{C} \oplus \mathbb{C}x$ δηλ. όλα τα γραμμικά πολυώνυμα μιας μεταβλητής. Το πλήθος ριζών είναι 2 καθώς ικανοποιούνται οι συνθήκες του θεωρήματος. Τα μονώνυμα κάτω από τη σκάλα είναι $\{1, x\}$. □

Άσκηση 6.6.16 Κατασκευάστε ένα αντίστοιχο παράδειγμα με 2 μεταβλητές και εξετάστε τις συνθήκες του θεωρήματος.

Βιβλιογραφία

[AHU74] A.V. Aho, J.E. Hopcroft, and J.D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Mass., 1974.

[Akr89] A.G. Akritas. *Elements of Computer Algebra with Applications*. J. Wiley & Sons, New York, 1989.

[Bar68] E.H. Bareiss. Sylvester's identity and multistep integer-preserving gaussian elimination. *Math. Comp.*, 22:565–578, 1968.

[BCL82] B. Buchberger, G.E. Collins, and R. Loos, editors. *Computer Algebra: Symbolic and Algebraic Computation*, volume 4 of *Computing Supplementum*. Springer-Verlag, Wien, 2nd edition, 1982.

[BEPP99] H. Brönnimann, I.Z. Emiris, V. Pan, and S. Pion. Sign determination in Residue Number Systems. *Theor. Comp. Science, Spec. Issue on Real Numbers & Computers*, 210(1):173–197, 1999.

[Ber76] D.N. Bernstein. The number of integral points in integral polyhedra. *Funct. Anal. & Appl.*, 10:223–224, 1976. Transl. from *Funktsional'nyi Analiz i Ego Prilozheniya,* 10(3):72–73, 1976.

[Béz79] E. Bézout. Théorie générale des équations algébriques. Paris, 1779.

[BP94] D. Bini and V.Y. Pan. *Polynomial and Matrix Computations*, volume 1: Fundamental Algorithms. Birkhäuser, Boston, 1994.

[BPR03] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*. Springer-Verlag, Berlin, 2003.

[Can88a] J. Canny. Some algebraic and geometric computations in PSPACE. In *Proc. ACM Symp. Theory of Computing*, pages 460–467, 1988.

[Can88b] J.F. Canny. *The Complexity of Robot Motion Planning*. M.I.T. Press, Cambridge, Mass., 1988.

[CE93] J. Canny and I. Emiris. An efficient algorithm for the sparse mixed resultant. In G. Cohen, T. Mora, and O. Moreno, editors, *Proc. Intern. Symp. on Applied Algebra, Algebraic Algor. and Error-Corr. Codes (Puerto Rico)*, number 263 in Lect. Notes in Comp. Science, pages 89–104, Berlin, 1993. Springer-Verlag.

[CE00] J.F. Canny and I.Z. Emiris. A subdivision-based algorithm for the sparse resultant. *J. ACM*, 47(3):417–451, May 2000.

[CLO97] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition, 1997.

[CLO05] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer, 2nd edition, 2005.

[CP93] J. Canny and P. Pedersen. An algorithm for the Newton resultant. Technical Report 1394, Comp. Science Dept., Cornell University, 1993.

[D'A02] C. D'Andrea. Macaulay-style formulas for the sparse resultant. *Trans. of the AMS*, 354:2595–2629, 2002.

[DD01] C. D'Andrea and A. Dickenstein. Explicit formulas for the multivariate resultant. *J. Pure Appl. Algebra*, 164(1-2):59–86, 2001.

[DE03] A. Dickenstein and I.Z. Emiris. Multihomogeneous resultant formulae by means of complexes. *J. Symbolic Computation*, 36(3-4):317–342, 2003. Special issue on ISSAC 2002.

[DEKP99] A. Díaz, I.Z. Emiris, E. Kaltofen, and V.Y. Pan. Algebraic algorithms. In M.J. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 16. CRC Press, Boca Raton, Florida, 1999. Revised chapter 17: Algebraic and Numeric Algorithms, 2010 edition, by I.Z. Emiris, V.Y. Pan and E. Tsigaridas, eds M.J. Atallah and M. Blanton.

[Dix08] A.L. Dixon. The eliminant of three quantics in two independent variables. *Proc. London Math. Society*, 6:49–69, 209–236, 1908.

[DST88] J.H. Davenport, Y. Siret, and E. Tournier. *Computer Algebra*. Academic Press, London, 1988.

[DSY05] Z. Du, V. Sharma, and C. K. Yap. Amortized bound for root isolation via Sturm sequences. In D. Wang and L. Zhi, editors, *Proc. Intern. Workshop on Symbolic Numeric Computing*, pages 113–129, Beijing, 2005.

[EC95] I.Z. Emiris and J.F. Canny. Efficient incremental algorithms for the sparse resultant and the mixed volume. *J. Symbolic Computation*, 20(2):117–149, 1995.

[EGT10] I.Z. Emiris, A. Galligo, and E. Tsigaridas. Random polynomials and expected-case complexity of real root isolation. In *Proc. Annual ACM Intern. Symp. on Symbolic and Algebraic Computation*, pages 235–242. ACM Press, 2010.

[EM00] M. Elkadi and B. Mourrain. Algorithms for residues and Lojasiewicz exponents. *J. Pure & Appl. Algebra*, 153:27–44, 2000.

[EMT08] I.Z. Emiris, B. Mourrain, and E.P. Tsigaridas. Real algebraic numbers: Complexity analysis and experimentations. In P. Hertling, C. Hoffmann, W. Luther, and N. Revol, editors, *Reliable Implementation of Real Number Algorithms: Theory and Practice*, volume 5045 of *LNCS*, pages 57–82. Springer, 2008.

[EP99] I.Z. Emiris and V.Y. Pan. Applications of FFT. In M.J. Atallah, editor, *Handbook of Algorithms and Theory of Computation*, chapter 17. CRC Press, Boca Raton, Florida, 1999. Revised chapter 18: Applications of FFT and Structured matrices, 2010 edition, eds M.J. Atallah and M. Blanton.

[GCL92] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, Norwell, Massachusetts, 1992.

[GKZ94] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Birkhäuser, Boston, 1994.

[Her80] C. Hermite. *Sur l'Extension du Théorème de M. Sturm à un Système d'Equations Simultanées*, volume 3 of *Oeuvres de C. Hermite*. 1880.

[HS97] B. Huber and B. Sturmfels. Bernstein's theorem in affine space. *Discr. Comput. Geometry*, 17(2):137–142, March 1997.

[Khe03] A. Khetan. The resultant of an unmixed bivariate system. *J. Symbolic Computation*, 36:425–442, 2003.

[Knu97] D.E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms*, volume 2. Addison-Wesley, Reading, Massachusetts, 3 edition, 1997.

[KO63] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Dokl.*, 7:595–596, 1963.

[KV01] E. Kaltofen and G. Villard. On the complexity of computing determinants. In K. Shirayanagi and K. Yokoyama, editors, *Proc. Fifth Asian Symp. Computer Math.*, volume 9 of *Lect. Notes in Computing*, pages 13–27. World Scientific, Singapore, 2001.

[KV05] E. Kaltofen and G. Villard. On the complexity of computing determinants. *Computational Complexity*, 13:91–130, 2005.

[Mac02] F.S. Macaulay. Some formulae in elimination. *Proc. London Math. Soc.*, 1(33):3–27, 1902.

[Mer00] J-P. Merlet. ALIAS: an interval analysis based library for solving and analyzing systems of equations. In *Systèmes d'Equations Algébriques*, Toulouse, 2000.

[Mis93] B. Mishra. *Algorithmic Algebra*. Springer-Verlag, New York, 1993.

[Moo66] R. E. Moore. *Interval Analysis*. Prentice Hall, Englewood Cliffs, NJ, 1966.

[MSW94] A.P. Morgan, A.J. Sommese, and C.W. Wampler. A product-decomposition bound for Bézout numbers. *SIAM J. Numerical Analysis*, 32(4), 1994.

[MVY02] B. Mourrain, M. Vrahatis, and J.C. Yakoubsohn. On the complexity of isolating real roots and computing with certainty the topological degree. *J. Complexity*, 18(2), 2002.

[Pan97] V.Y. Pan. Solving a polynomial equation: Some history and recent progress. *SIAM Rev.*, 39(2):187–220, 1997.

[Ped90] P. Pedersen. Counting real zeros. Technical Report 243, Robotics Lab, Courant Institute, NYU, 1990. PhD Thesis.

[PRS93] P. Pedersen, M-F. Roy, and A. Szpirglas. Counting real zeros in the multivariate case. In F. Eyssette and A. Galligo, editors, *Computational Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 203–224. Birkhäuser, Boston, 1993. (Proc. MEGA '92, Nice).

[PS93] P. Pedersen and B. Sturmfels. Product formulas for resultants and Chow forms. *Math. Zeitschrift*, 214:377–396, 1993.

[Rou99] F. Rouillier. Solving zero-dimensional polynomial systems through the rational univariate representation. *Applic. Algebra Engineer., Communic. & Computing*, 9(5):433–461, 1999.

[RZ01] F. Rouillier and P. Zimmermann. Efficient isolation of a polynomial real roots. Technical Report 4113, INRIA–Lorraine, 2001.

[SA95] M. Sharir and P. Agarwal. *Davenport-Schinzel sequences and applications in computational geometry.* Cambridge University Press, Cambridge, 1995.

[Stu93] B. Sturmfels. Sparse elimination theory. In D. Eisenbud and L. Robbiano, editors, *Proc. Computat. Algebraic Geom. & Commut. Algebra 1991*, pages 264–298, Cortona, Italy, 1993. Cambridge Univ. Press.

[Stu94] B. Sturmfels. On the Newton polytope of the resultant. *J. Algebraic Combin.*, 3:207–236, 1994.

[Syl53] J.J. Sylvester. On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest algebraic common measure. *Philosophical Trans.*, 143:407–548, 1853.

[Tsi06] E.P. Tsigaridas. *Algebraic algorithms and applications in computational geometry.* PhD thesis, Dept. Informatics & Telecoms, National U. Athens, Greece, 2006. In greek.

[vdW50] B.L. van der Waerden. *Modern Algebra.* F. Ungar Publishing Co., New York, 3rd edition, 1950.

[vzGG99] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra.* Cambridge Univ. Press, Cambridge, U.K., 1999.

[Wey24] H. Weyl. Randbemerkungen zu Hauptproblemen der Mathematik, II, Fundamentalsatz der Algebra and Grundlagen der Mathematik. *Math. Z.*, 20:131–151, 1924.

[Yap00] C.K. Yap. *Fundamental Problems of Algorithmic Algebra.* Oxford University Press, New York, 2000.

[Zip93] R. Zippel. *Effective Polynomial Computation.* Kluwer Academic Publishers, Boston, 1993.