Μάθημα
Εισαγωγή στις Τηλεπικοινωνίες

Κωδικοποίηση πηγής- καναλιού
Μάθημα 9ο -10ο

ΕΘΝΙΚΟ & ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

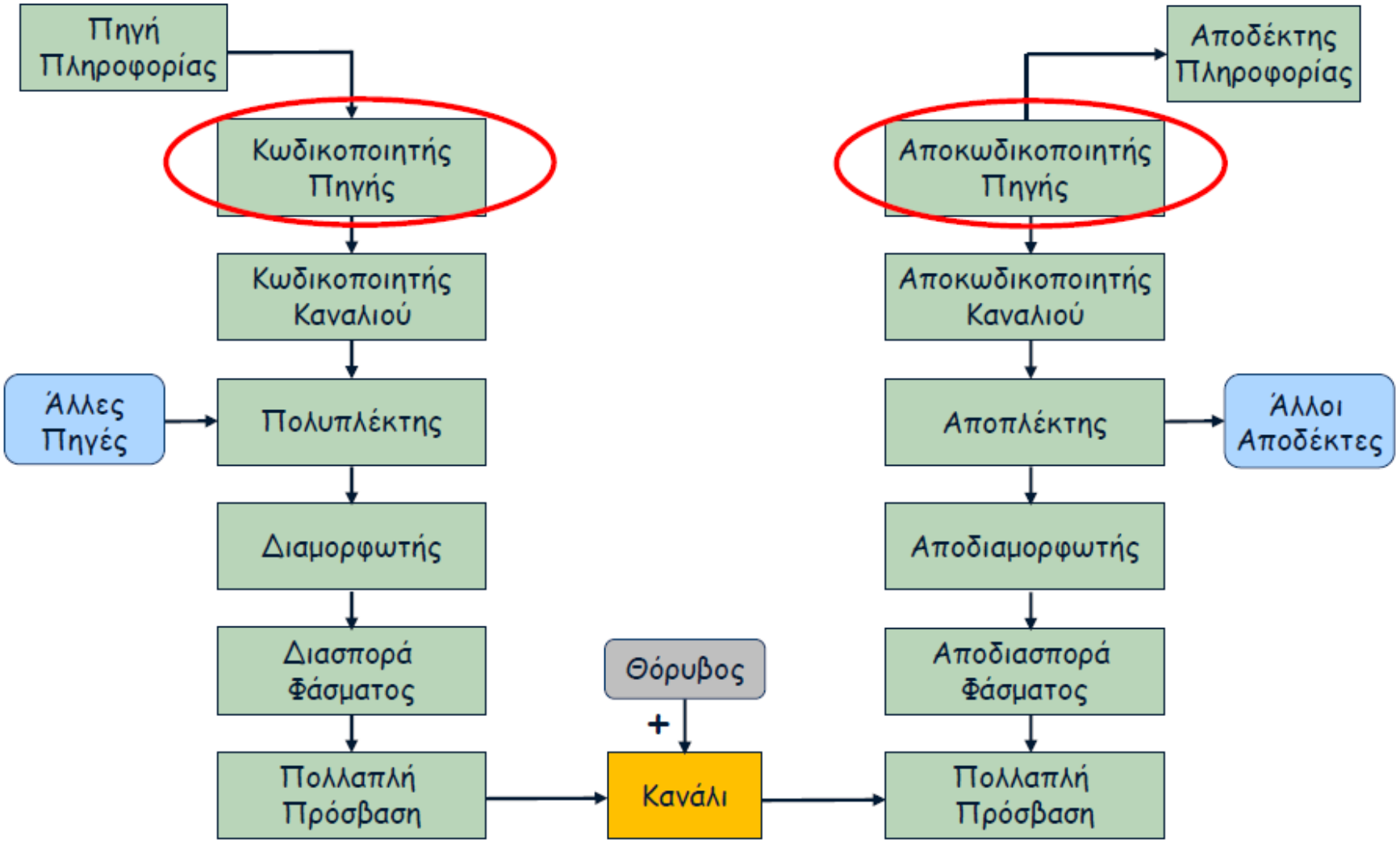
Τομέας Επικοινωνιών και Επεξεργασίας Σήματος

Τμήμα Πληροφορικής & Τηλεπικοινωνιών

Περιεχόμενα Ενότητας

- Κωδικοποίηση Πηγής
  - Προθεματικοί κώδικες
  - Αλγόριθμος Huffman
  - Αλγόριθμος Lempel-Ziv
- Κωδικοποίηση Καναλιού
  - Γραμμικοί κώδικες block
  - Συνελικτικοί κώδικες
  - Κώδικες turbo

Μοντέλο Ψηφιακών Επικοινωνιών



Πληροφορία& Ψηφιακά Συστήματα

- **Βασικοί Στόχοι στις Τηλεπικοινωνίες:**

1. η αποδοτική αναπαράσταση των δεδομένων που εξάγει μια πηγή πληροφορίας

2. η αποδοτική αξιόπιστη μετάδοση της πληροφορίας πάνω από ένα κανάλι

  - Με το πρώτο ζήτημα ασχολείται η κωδικοποίηση πηγής (source coding) →συμπίεση δεδομένων
  - Με το δεύτερο ζήτημα ασχολείται η κωδικοποίηση καναλιού(channel coding) → ανίχνευση και διόρθωση σφαλμάτων

Κωδικοποίηση Πηγής & Καναλιού

Κωδικοποίηση Πηγής

- Η έξοδος της πηγής είναι μια τυχαία διαδικασία. Αν ήταν ντετερμινιστική, δεν θα υπήρχε λόγος μετάδοσης...
- τι αποτέλεσμα έχει στην πληροφορία η εφαρμογή κάποιας επεξεργασίας (π.χ. μετατροπή A/D);

- Για τη θεωρητική ανάλυση → πηγές πληροφορίας με διακριτό αλφάβητο
  - Πληροφορία ενός συμβόλου (Information) s_i με πιθανότητα εμφάνισης $p_i = p(s_i)$:

$$I(s_i) = \log_\alpha \frac{1}{p(s_i)} = -\log_\alpha p(s_i)$$

  - Δυαδική πηγή χωρίς μνήμη: $S = \{0,1\}$ $\{p, 1-p\}$
  - Για $p = 0.5$ → δυαδική συμμετρική πηγή χωρίς μνήμη

Η Εντροπία

- Η εντροπία μιας DMS ορίζεται ως

$$H(S)=\sum_{i=1}^{N} p_i I(s_i)=-\sum_{i=1}^{N} p_i \log_2 p_i$$

- Ίδια βάση λογαρίθμου με την πληροφορία.
- Μονάδες → bits/σύμβολο (για βάση α=2).
- Φυσική σημασία:
  - μέση τιμή πληροφορίας ανά σύμβολο
  - κάτω όριο μέσου αριθμού bits για την αναπαράσταση ενός συμβόλου χωρίς σφάλματα (όριο συμπίεσης δεδομένων)
- Όσο μεγαλύτερη εντροπία έχει μια πηγή,
  - τόσο περισσότερη πληροφορία φέρει, και
  - τόσο περισσότερα bits χρειάζονται για την κωδικοποίησή της
- Παρατήρηση: $\lim_{p\to 0+}(p \log p)=0$

Η εντροπία μιας Ν-αδικής DMS (Ν πλήθος συμβόλων): ⇨ $0 \le H(S) \le \log_2 N$

- Αν η πηγή παράγει R_s σύμβολα ανά δευτερόλεπτο, ο μέσος ρυθμός πληροφορίας είναι: $R_b = R_s\, H$
- Ο μέσος ρυθμός πληροφορίας έχει μονάδες (symbol/sec) × (bit/symbol) = bit/sec (ή bps)
- Ο χρόνος μεταξύ δύο διαδοχικών συμβόλων (σε sec/symbol) προκύπτει: $T_s = 1/R_s$

Παράδειγμα: Μια πηγή παράγει ένα σύμβολο κάθε 5 ms ανάμεσα από $n = 32$ ισοπίθανα σύμβολα. R_b=?

Πλεονασμός Πηγής

- Έμφυτος πλεονασμός πηγής πληροφορίας
  - π.χ. «Τν επμεν Δευτα δεν θα γνι το μαθμ γιαι εναι η Κθρη Δευτα»
- Αγγλική γλώσσα → πλεονασμός 50%.
- **Πλεονασμός** πηγής πληροφορίας = ποσοστό "άχρηστης πληροφορίας" (δηλ. περιττών επαναλήψεων) που μεταφέρει η έξοδος της.

$$\pi = \frac{\mathrm{H}_{\max} - H}{H_{\max}} = 1 - \frac{H}{H_{\max}}$$

- Ουσιαστικά είναι η διαφορά της τρέχουσας κατάστασης από την ιδανική περίπτωση της μέγιστης εντροπίας (στην οποία τα σύμβολα της πηγής χρησιμοποιούνται ισοπίθανα).

Κωδικοποίηση Πηγής Ι

- Αποδοτική αναπαράσταση/αντιστοίχιση συμβόλων μιας πηγής πληροφορίας σε κωδικές λέξεις.
- Αφαίρεση πιθανού πλεονασμού → συμπίεση πληροφορίας
- Είδη κωδικοποίησης:
  1. Αντιστρεπτή ή χωρίς απώλειες (lossless coding): επιτρέπει την ακριβή ανακατασκευή των αρχικών δεδομένων κατά την αποκωδικοποίηση (π.χ. αλγόριθμοί Huffman, Lempel-Ziv με χρήσεις στα GIF, PNG, ZIP).
  2. Μη αντιστρεπτή ή με απώλειες (lossy coding): χαρακτηρίζεται από μη αναστρέψιμη απώλεια πληροφορίας (χαμηλότερη ποιότητα με υψηλούς βαθμούς συμπίεσης π.χ. PCM, JPEG, MPEG).
- Είδη κωδίκων:
  1. Σταθερού μήκους: όλες οι κωδικές λέξεις έχουν το ίδιο μήκος.
  2. Μεταβλητού μήκους: διαφορετικές κωδικές λέξεις έχουν διαφορετικό μήκος [αξιοποίηση γνώσης στατιστικών ιδιοτήτων πηγής (γνώση πιθανοτήτων συμβόλων)].
- Αποκωδικοποίηση πηγής: η αντίστροφη διαδικασία της κωδικοποίησης πηγής, δηλαδή ανάκτηση της αρχικής πληροφορίας γνωρίζοντας τη μέθοδο κωδικοποίησης πηγής.

Θεώρημα Κωδικοποίησης Πηγής

- Ερώτημα: πόσο μπορεί να συμπιεστεί μια πηγή χωρίς να εισαχθούν σφάλματα;

Θεώρημα κωδικοποίησης πηγής (1° Θεώρημα του Shannon): Έστω πηγή με εντροπία (ή ρυθμό εντροπίας) H που κωδικοποιείται (συμπιέζεται) με H_c *(bits/έξοδο πηγής)*.

– Αν $H_c \geq H$, η πηγή μπορεί να κωδικοποιηθεί με οσοδήποτε μικρή πιθανότητα σφάλματος,

– Αν $H_c < H$, όσο πολύπλοκος κι αν είναι ο κωδικοποιητής πηγής, η πιθανότητα σφάλματος θα είναι μακριά από το 0.

- Σχόλια:
  - Το H_c αντιστοιχεί στο μέσο μήκος κώδικα $\bar{L}$.
  - Ρυθμός δεδομένων (data rate): $R_b = r_s \cdot R$ (bits/sec)

$$H_c = \bar{L}$$

Κωδικοποίηση Πηγής II

Ένας κωδικοποιητής πηγής δέχεται ως είσοδο σύμβολα από πηγή πληροφορίας και εξάγει bit

- Αντιστοίχιση συμβόλων s_i μιας N-αδικής πηγής σε κωδικές λέξεις $C(s_i)$ μήκους $l(s_i)$.
- Λειτουργικές απαιτήσεις:
  - M-αδικές κωδικές λέξεις (συνήθως δυαδικές)
  - Μοναδικά αποκωδικοποιήσιμος κώδικας
- Μέσο μήκος κώδικα: $\bar{L} = \sum_{i=1}^{N} p(s_i) l(s_i)$
- Απόδοση κώδικα: $\eta = \frac{H(S)}{\bar{L}} \leq 1$

Παράδειγμα: Πηγή παράγει τα σύμβολα {Α, Β, Γ}, με πιθανότητες {0.5, 0.25, 0.25}, τα οποία κωδικοποιούνται ως εξής: s_1 = Α → $c(s1)$ = 01, s_2 = Β → $c(s2)$ = 110, s_3 = Γ → c(s3) = 00

- Για την ακολουθία συμβόλων ΑΑΓΒΒΓ, ο κωδικοποιητής θα παραγάγει την ακολουθία bit:
- 01 01 00 110 110 00

- Το μέσο μήκος των κωδικολέξεων είναι:

$$\overline{L} = 0.5 \times 2 + 0.25 \times 3 + 0.25 \times 2$$
$$= 2.25 \text{ bit}$$

Προθεματικοί κώδικες

- Πρόβλημα: συγχρονισμός
  - πώς μπορώ να βρω τα όρια των μπλοκ στην έξοδο για να γίνει η αποκωδικοποίηση;
- Λύση: προθεματικοί κώδικες (prefix codes)
- Προθεματικός κώδικας: καμία κωδική λέξη δεν αποτελεί πρόθεμα κάποιας άλλης
  - άμεσος (επιτρέπει απευθείας αποκωδικοποίηση)
  - μονοσήμαντα αποκωδικοποιήσιμος (κάθε έξοδος αντιστοιχεί σε μοναδική είσοδο)

- Αλγόριθμοι κωδικοποίησης (συμπίεσης) πηγής.
- Επιτυγχάνουν ρυθμούς κωδικοποίησης κοντά στην εντροπία (όριο συμπίεσης).
- Κωδικοποίηση από σταθερό σε μεταβλητό μήκος
  - είσοδος: μπλοκ συμβόλων σταθερού μήκους
  - έξοδος: μπλοκ bits μεταβλητού μήκους

Κωδικοποίηση Πηγής ΙΙΙ

Σύμβολο	Πιθανότητα	Κώδικας 1	Κώδικας 2	Κώδικας 3	Κώδικας 4
a_1	$p_1=\frac{1}{2}$	1	1	0	00
a_2	$p_2=\frac{1}{4}$	01	10	10	01
a_3	$p_3=\frac{1}{8}$	001	100	110	10
a_4	$p_4=\frac{1}{16}$	0001	1000	1110	11
a_5	$p_5=\frac{1}{16}$	00001	10000	1111	110

- Κώδικας 1: αυτό-συγχρονιζόμενος, μονοσήμαντα αποκωδικοποιήσιμος, άμεσος, $\bar{L} = \frac{31}{16}$
- Κώδικας 2: αυτό-συγχρονιζόμενος, μονοσήμαντα αποκωδικοποιήσιμος
- Κώδικας 3: αυτό-συγχρονιζόμενος, μονοσήμαντα αποκωδικοποιήσιμος, άμεσος, $\bar{L} = \frac{30}{16}$
- Κώδικας 4: δεν είναι μονοσήμαντα αποκωδικοποιήσιμος

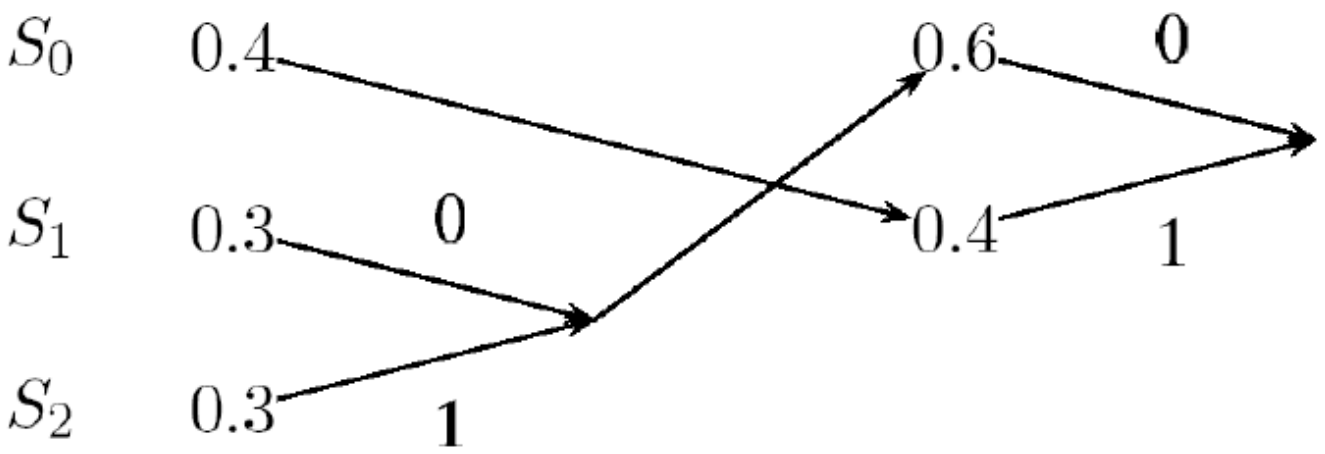
Αλγόριθμος Κωδικοποίησης Huffman

- Αποτελεί προθεματικό κώδικα.
- Κωδικοποίηση από σταθερό σε μεταβλητό μήκος.
- Βασική ιδέα: απεικόνιση των συχνότερα εμφανιζόμενων συμβόλων σε βραχύτερες δυαδικές ακολουθίες.
- Βέλτιστος κώδικας: ελάχιστο μέσο μήκος κώδικα ανάμεσα σε άλλους προθεματικούς κώδικες.
- Βήματα αλγορίθμου κωδικοποίησης Huffman:
  1. Διέταξε τα σύμβολα κατά φθίνουσα σειρά πιθανοτήτων.
  2. Συγχώνευσε τα δύο σύμβολα με τις μικρότερες πιθανότητες και δημιούργησε νέο «σύμβολο» .
  3. Ανάθεσε στα δύο σύμβολα «0» και «1».
  4. Ταξινόμησε εκ νέου τη λίστα των συμβόλων.
  5. Επανέλαβε τα παραπάνω μέχρι όλα τα σύμβολα συγχωνευτούν σε ένα τελικό σύμβολο.

Αλγόριθμος Κωδικοποίησης Huffman

- Δυαδικό δέντρο:
  - ρίζα: το τελικό σύνθετο σύμβολο
  - φύλλα: τα αρχικά σύμβολα
  - ενδιάμεσοι κόμβοι: σύνθετα σύμβολα
- Αποκωδικοποίηση → ανάθεση bits σε σύμβολα εισόδου
- Βήματα αποκωδικοποίησης:
  1. Ξεκίνα από τη ρίζα του δέντρου και κινήσου προς ένα φύλλο ακολουθώντας το bit που συναντάται κάθε φορά.
  2. Όταν φτάσεις σε κάποιο φύλλο έχεις αποκωδικοποιήσει ένα σύμβολο.
  3. Επανέλαβε για όλα τα σύμβολα (φύλλα).

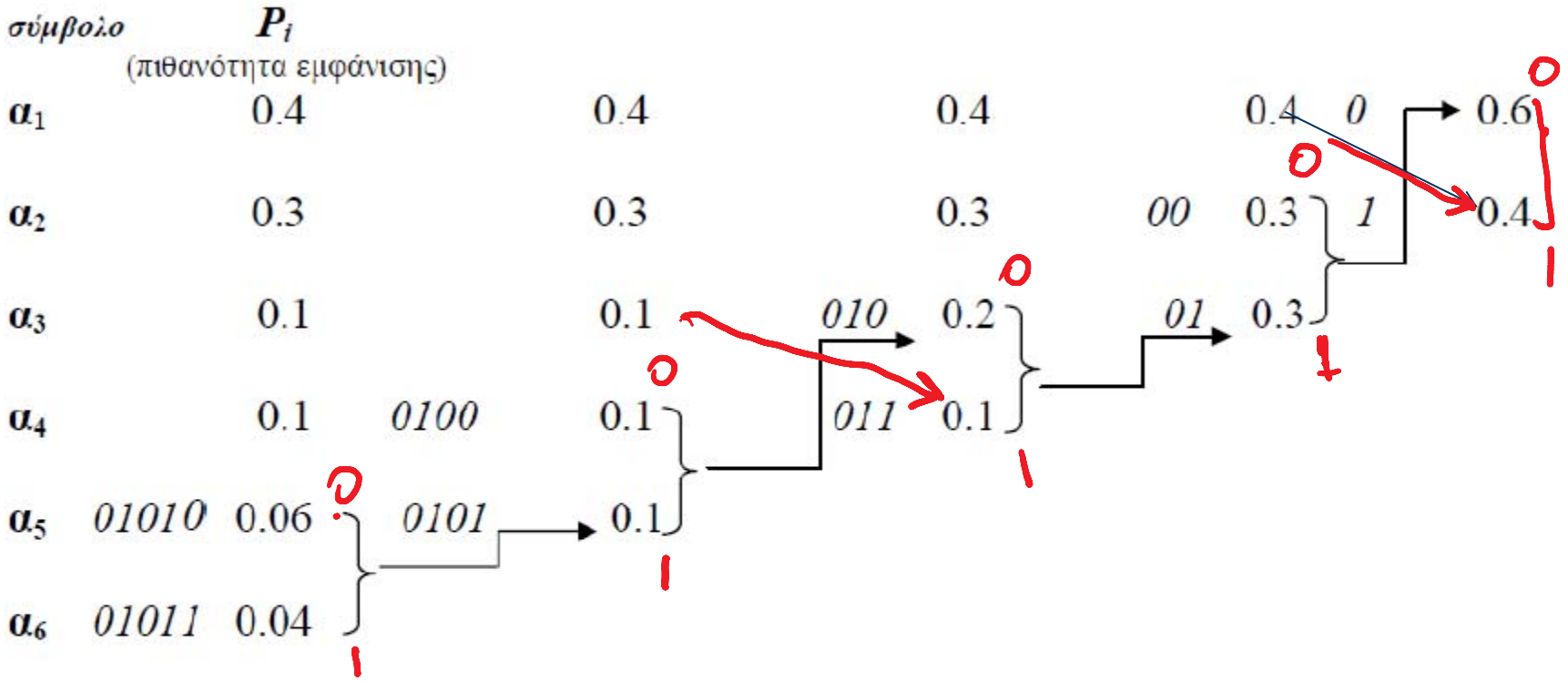
παράδειγμα



- Προθεματική αντιστοίχιση:
  - s_0: 1
  - s_1: 00
  - s_2: 01
- Μονοσήμαντη και άμεση αποκωδικοποίηση

1	0	1	0	0	0	1	1	0	0
s_0		s_2		s_1		s_2		s_0	s_1

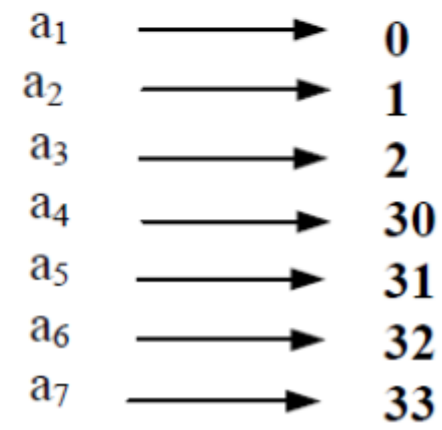
Παράδειγμα



$\alpha_1 \rightarrow 1$
$\alpha_2 \rightarrow 00$
$\alpha_3 \rightarrow 011$
$\alpha_4 \rightarrow 0100$
$\alpha_5 \rightarrow 01010$
$\alpha_6 \rightarrow 01011$

Παράδειγμα- τετραδικό σύστημα

σύμβολο		P_i (πιθανότητα εμφάνισης)		
a_1		0.5	*0*	0.5
a_2		0.25	*1*	0.25
a_3		0.15	*2*	0.15
a_4	*30*	0.05	*3*	0.1
a_5	*31*	0.03		
a_6	*32*	0.015		
a_7	*33*	0.005		



Σχόλια

- **Παρατηρήσεις**
- Η διαδικασία κωδικοποίησηςHuffman δεν είναι μοναδική.
- Σημεία που μπορούν να υλοποιηθούν με διαφορετικό τρόπο:
- Αν δυο σύμβολα έχουν την ίδια πιθανότητα εμφάνισης υπάρχουν δυο τρόποι διάταξης τους.
- Η ανάθεση 0 και 1 μπορεί να γίνει από πάνω προς τα κάτω ή από κάτω προς τα πάνω.
- Διαφορετικές υλοποιήσεις οδηγούν σε σύμβολα με διαφορετικό κώδικα ή ακόμα και διαφορετικό μήκος κώδικα.
- **Το μέσο μήκος κώδικα διατηρείται σταθερό** και είναι Βέλτιστο

- **Μειονεκτήματα**
- Οι κώδικες Huffman παρουσιάζουν ισχυρή εξάρτηση από τη στατιστική της πηγής.Η εκτίμηση της στατιστικής της πηγής απαιτεί χρονοβόρες διαδικασίες.
- Ο κώδικας μπορεί να είναι μη αποδοτικός επειδή είναι σχεδιασμένος για μπλοκ μήκους ενός συμβόλου π.χ. για μεγάλο p_{max} απαιτείται ιδανικό μήκος κωδικής λέξης μικρότερο από ένα, κάτι που δεν είναι εφικτό.

Παραδείγματα κωδίκων Fano

Κωδικοποίηση Fano							
α/α i	Σύμβολο s_i	Πιθανότητα P_i	1η Διαίρεση	2η Διαίρεση	3η Διαίρεση	Κωδικολέξη $c(s_i)$	Μήκος Κωδικολέξης l_i
1	s_1	0.4	0.4 } 0	0.4 } 0		0 0	2
2	s_2	0.2	0.2 }	0.2 } 1		0 1	2
3	s_3	0.2	0.2 }	0.2 0		1 0	2
4	s_4	0.1	0.1 } 1	0.1 } 1	0.1 } 0	1 1 0	3
5	s_5	0.1	0.1 }	0.1 }	0.1 } 1	1 1 1	3

$$\overline{L} = \sum_{i=1}^{5} P_i \ell_i = 0.4 \times 2 + 0.2 \times 2 + 0.2 \times 2 + 0.1 \times 3 + 0.1 \times 3 = 2.2\,\text{bit}$$

Η απόδοση του κώδικα είναι

$$\eta = \frac{H(\mathscr{L})}{\overline{L}} = \frac{2.12}{2.2} \approx 96.4\%$$

Το μέσο μήκος των κωδικολέξεων διαφέρει λιγότερο από 0.1 bit από την εντροπία της πηγής

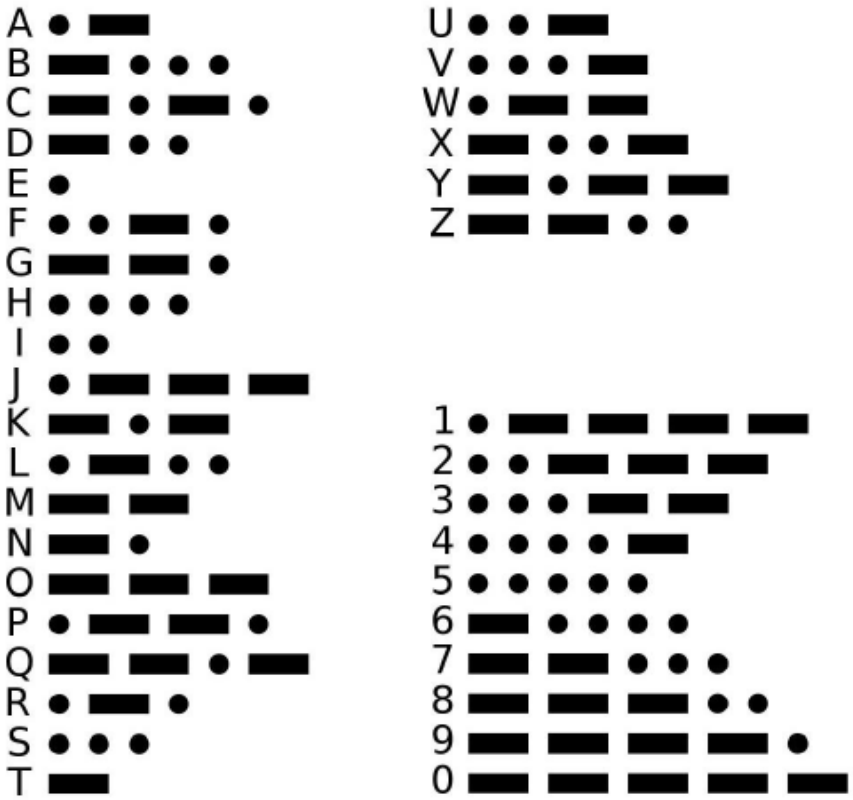
Κώδικας Morse

Γράμμα	Συχνότητα
E	11.16%
A	8.50%
R	7.58%
I	7.54%
O	7.16%
T	6.95%
N	6.65%
S	5.74%
L	5.49%
C	4.54%
U	3.63%
D	3.38%
P	3.17%

Γράμμα	Συχνότητα
M	3.01%
H	3.00%
G	2.47%
B	2.07%
F	1.81%
Y	1.78%
W	1.29%
K	1.10%
V	1.01%
X	0.29%
Z	0.27%
J	0.20%
Q	0.20%

International Morse Code

1. A dash is equal to three dots.
2. The space between parts of the same letter is equal to one dot.
3. The space between two letters is equal to three dots.
4. The space between two words is equal to seven dots.



Αλγόριθμος Κωδικοποίησης Lempel-Ziv

- Ξεπερνά τα προβλήματα του αλγορίθμου Huffman.
- Ανήκει στην κατηγορία των καθολικών (universal) αλγορίθμων
- μη εξάρτηση από την στατιστική της πηγής
- Όταν εφαρμοστεί σε Αγγλικό κείμενο επιτυγχάνει συμπίεση 55% σε σύγκριση με το 43% του Huffman.
- συμπίεση εικόνων (αρχεία GIF) – rar και gzip

Ο αλγόριθμος Lempel-Ziv ανήκει στην κατηγορία των καθολικών (universal) αλγορίθμων κωδικοποίησης πηγής, δηλαδή αλγορίθμων, που είναι ανεξάρτητοι από τη στατιστική της πηγής. Ο αλγόριθμος αυτός είναι ένα σχήμα κωδικοποίησης από μπλοκ μεταβλητού μήκους σε σταθερού μήκους.

Ασκηση

Έστω πηγή πληροφορίας η οποία παράγει τα ακόλουθα σύμβολα που κωδικοποιούνται από κάποιο κώδικα πηγής με τα παρακάτω μήκη:

Σύμβολο	x_1	x_2	x_3	x_4	x_5
Πιθανότητα	0.06	0.3	0.6	0.01	0.03
Μήκος κωδικής λέξης	3	2	2	3	1

Να υπολογιστεί η εντροπία της πηγής και ο πλεονασμός της. Πόσο είναι το μέσο μήκος του συγκεκριμένου κώδικα και ο πλεονασμός του; Εισάγει σφάλματα;

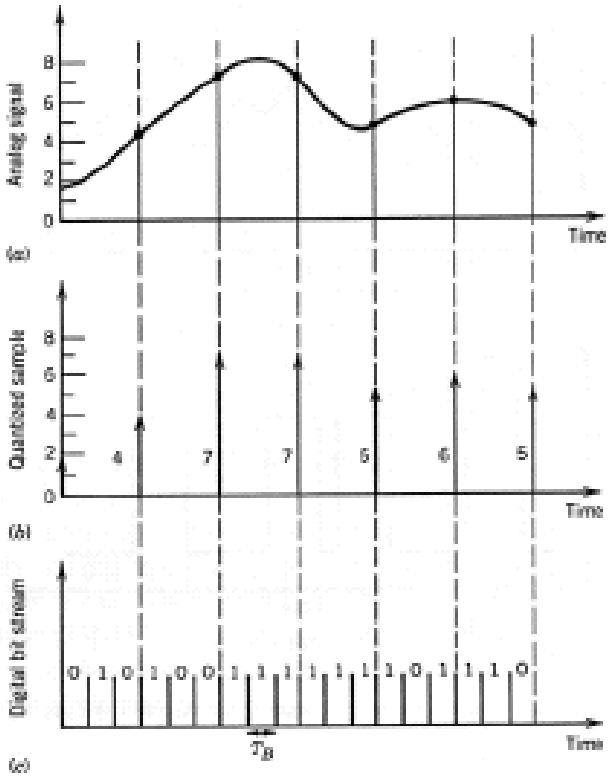
(Απ: $H=1.425$ bits/symbol, $H_{max}=\log_2 5=2.32$ bits/symbol → $\pi=0,39$,
$E[L]=2.04$ bits/symbol > H → $\pi_c=0.30$)

Επειδή $E(L)=\bar{L} > H$ ο κώδικας δεν εξάγει σφάλματα (Θ. Shannon)

PCM

- Η PCM είναι μια κλασσική τεχνική κωδικοποίησης με δεκαετίες εφαρμογής σε συστήματα τηλεπικοινωνιών.
- Θεωρείται σήμερα απαρχαιωμένη και αντικαθίσταται σταδιακά με πιο σύνθετες τεχνικές που βασίζονται στις παραπάνω δυνατότητες που προσφέρει η σύγχρονη τεχνολογία. Είναι όμως μια απλή υλοποίηση του θεωρήματος δειγματοληψίας και την διαχωρίζουμε σε ομοιόμορφη και μη-ομοιόμορφη PCM ανάλογα εάν έχουμε ομοιόμορφη ή μη-ομοιόμορφη κβάντιση

PCM



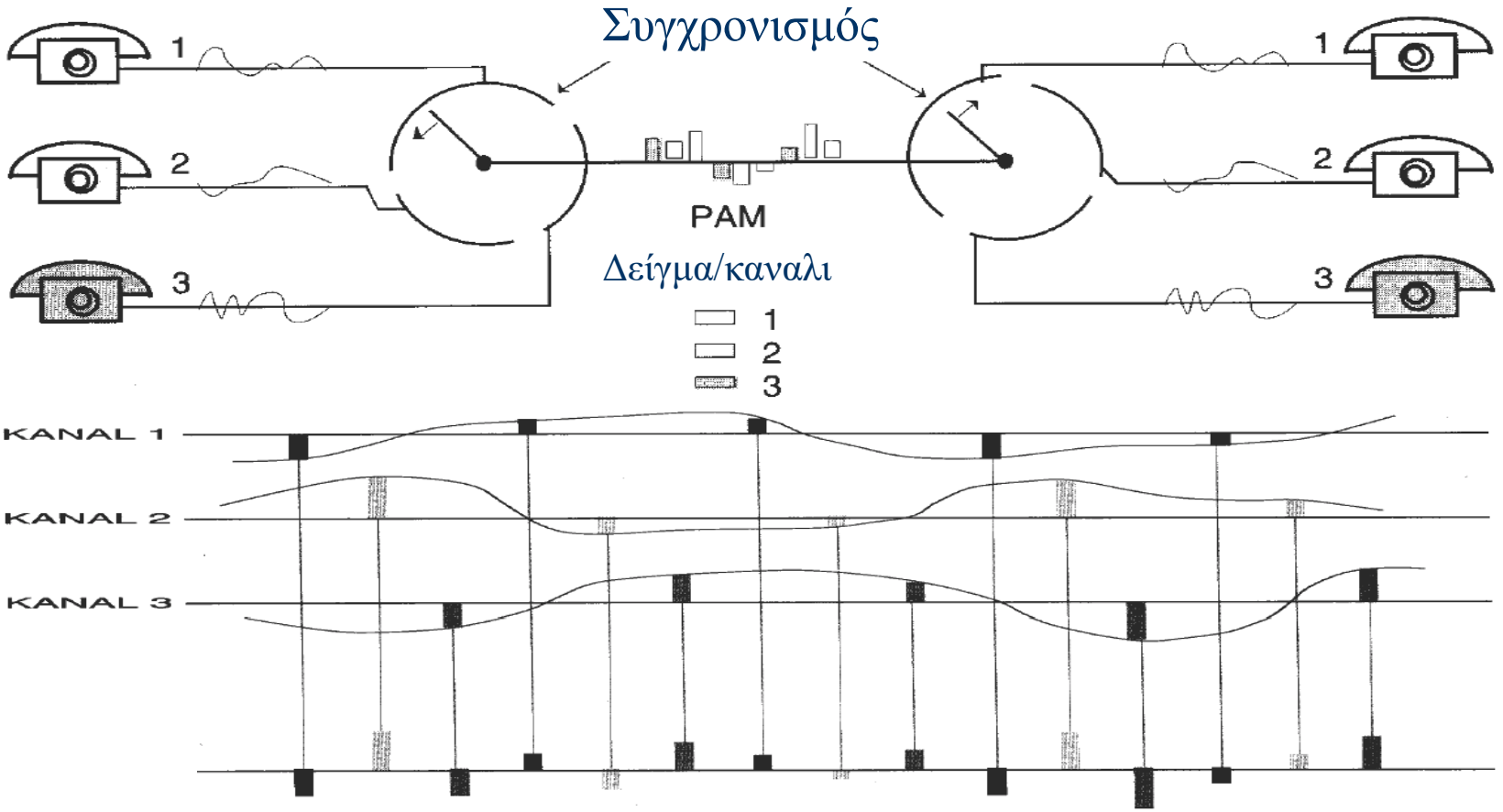
- ✓ Υπάρχουνε μία σειρά από τρόπους μετατροπής αναλογικού σήματος σε ψηφιακό. Στην τηλεφωνία (π.χ. κινητά) χρησιμοποιείται το PCM (Pulse Code Modulation)
- ✓ **Pulse-code modulation (παλμοκωδική διαμόρφωση) (PCM) (παρουσία/απουσία παλμού)**
- ✓ PCM: είναι η συνηθέστερη τεχνική μετάδοσης αναλογικού ως ψηφιακό σήμα
- ✓ προκύπτει ρυθμός bit:

$$R_b > (2\,\Delta f)\,\log_2(M)$$

- ✓ M σταθμες κβάντισης (M=256)

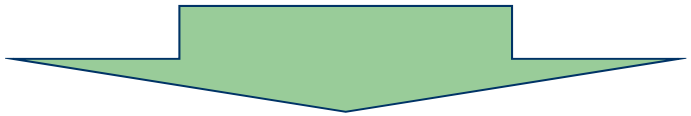
[π.χ: τηλεφωνία Δf = 4 kHz, R_b = 64 kbit/s]

Σύστημα PCM


Συγχρονισμός
1
2
3
PAM
Δείγμα/καναλι
1
2
3
KANAL 1
KANAL 2
KANAL 3

Εύρος Ζώνης PCM

- Σήμα αναλογικό, εύρους ζώνης *W*



- Ελάχιστος ρυθμός δειγματοληψίας: *2W δείγματα/sec*
- Συνήθως χρησιμοποιείται υπερδειγματοληψία
  - $f_s > 2W$ *δείγματα/sec*
- Χρησιμοποιούνται *n bits/δείγμα*
  - Οπότε για να μεταδώσω ρυθμό συμβόλων: $f_s n$ *bits/sec*

- Για τη μετάδοση σε βασική ζώνη ενός σήματος με ρυθμό μετάδοσης Rs παλμοί(bits ή symbols)/sec,

.....απαιτείται εύρος ζώνης μεγαλύτερο ή ίσο από Rs/2

Εύρος Ζώνης PCM (2)

- απαιτείται εύρος ζώνης

$$BW_{PCM} \geq \frac{nf_s}{2}$$

- Για δειγματοληψία σε ρυθμό Nyquist

$$BW_{PCM} \geq nW$$

- Συμπέρασμα:
  - το σύστημα PCM αυξάνει το εύρος ζώνης του αρχικού σήματος *n φορές*
  - *$n = \log_2 M$, M ο αριθμός των σταθμών κβάντισης*

Παράδειγμα

Θέλουμε να μεταδώσουμε δεδομένα μέσω τηλεφωνικής dial-up σύνδεσης με $BW = 3kHz$, $S/N = 13dB$ με ρυθμό $1200bps$ και $BER \leq 10^{-4}$. Διαθέτουμε ένα QPSK modem που μπορεί νε λειτουργήσει με ταχύτητα σηματοδοσίας $n \cdot 1200bps$ (όπου n=1,2,3) με $P_e = 2^n \cdot 10^4$ αντίστοιχα. Είναι αυτό εφικτό;

Αντί να στέλνω "1" στέλνω "111" και αντίγια "0" → "000"
Άρα ο ρυθμός μετάδοσης γίνεται $R_b = 3 \cdot 1200 bps$

Η χωρητικότητα του καναλιού μας είναι: $C = B \log\left(1 + \frac{S}{N}\right) \Rightarrow C = 13Kbps$
και $R_b < C$ άρα εφικτή η μετάδοση.

η πιθανότητα σφάλματος γίνεται:

$P_e = P(2$ ή περισσότερα bits τ?ς κωδικής λέξ?ς είναι εσφαλμένα$) =$

$= \binom{3}{2} P_c^2 (1 - P_c) + \binom{3}{3} P_c^3 = 3P_c^2 - 2P_c^3$ και επειδή $P_c = 2^3 \cdot 10^{-4}$

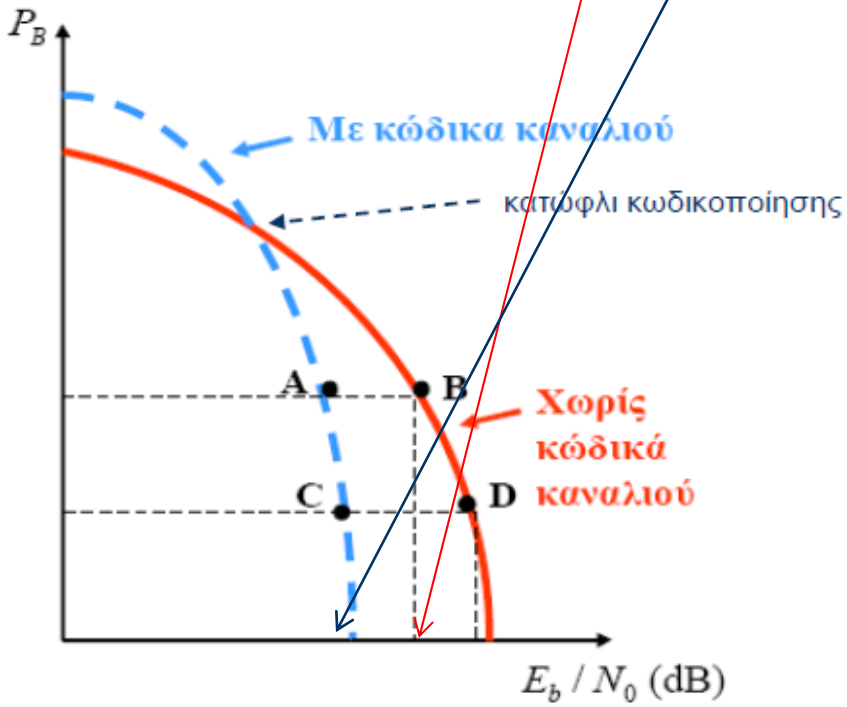
$$\boxed{P_e = 2 \cdot 10^{-6}}$$

Κωδικοποίηση καναλιού

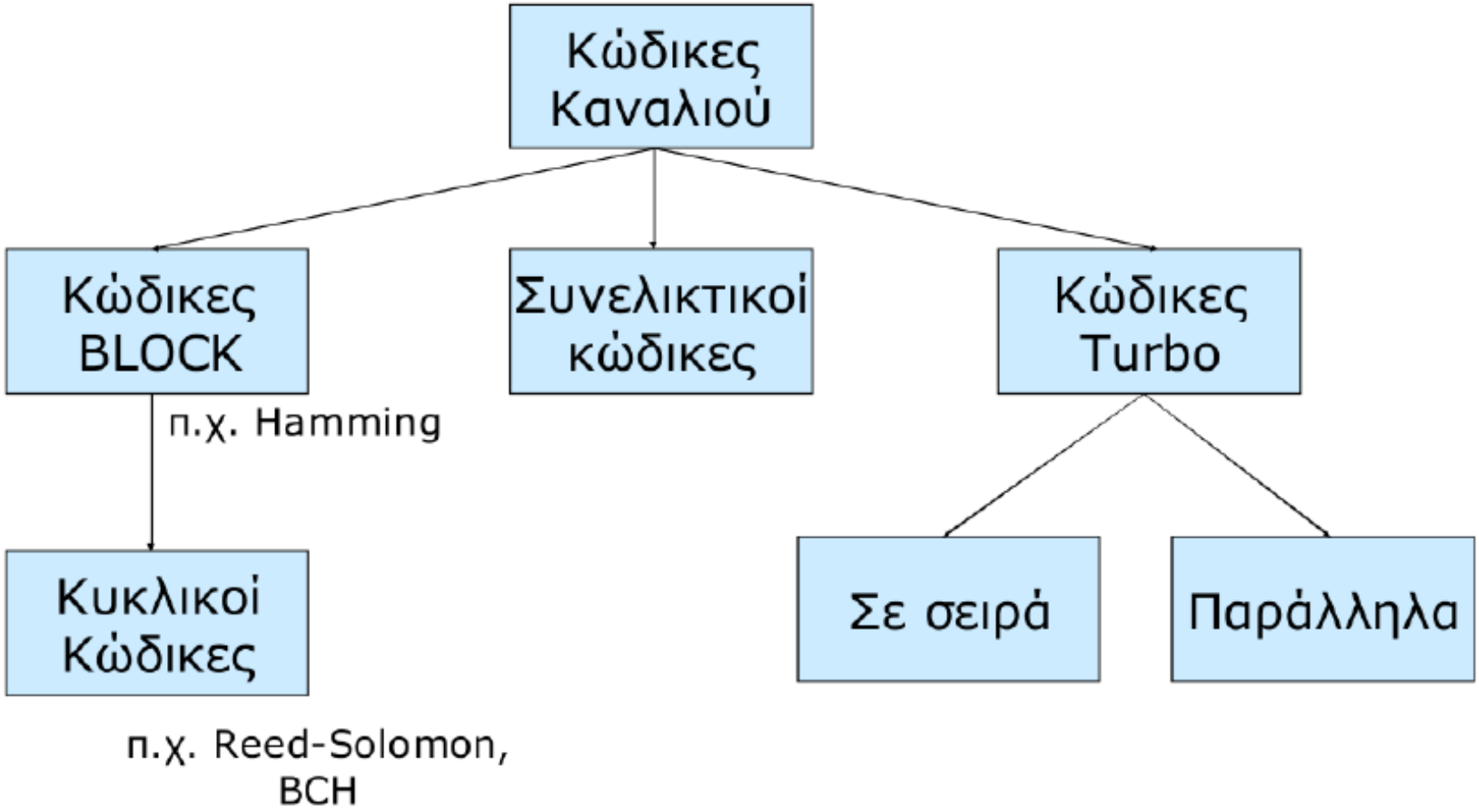
- Κανάλι μετάδοσης → εισαγωγή παραμόρφωσης → μείωση αξιοπιστίας και ποιότητας επικοινωνίας.
- Τεχνική αύξησης αξιοπιστίας → κωδικοποίηση καναλιού.
- Κωδικοποίηση καναλιού → εισαγωγή ελεγχόμενου πλεονασμού (με «δομημένο» τρόπο ώστε να αντιμετωπίζονται αποδοτικότερα οι παραμορφώσεις που εισάγει το κανάλι)
  - αποδοτική μετάδοση πληροφορίας
  - ανίχνευση και διόρθωση σφαλμάτων
- Αποκωδικοποίηση καναλιού: αντίστροφή διαδικασία ανάκτησης της αρχικής πληροφορίας γνωρίζοντας τη μέθοδο κωδικοποίησης καναλιού, ώστε να ελαχιστοποιηθεί η πιθανότητα σφάλματος.

Κέρδος ΚωδικοποίησηςΚαναλιού

- Κέρδος κωδικοποίησης (coding gain): η μείωση σε E_b/N_0 που επιτυγχάνεται με τη χρήση κωδικοποίησης καναλιού για επίτευξη ίδιας πιθανότητας σφάλματος → $CG = (E_b/N_0)_u / (E_b/N_0)_c$
- Μετάδοση ίδιου ρυθμού πληροφορίας → αύξηση ρυθμού μετάδοσης κωδικοποιημένου μηνύματος.



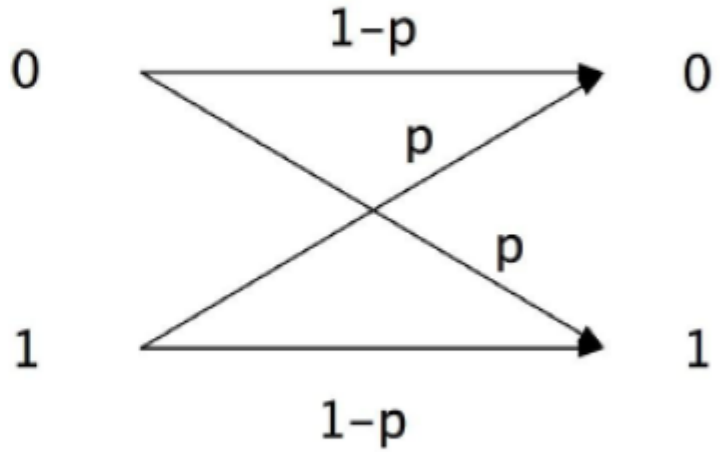
ΚατηγορίεςΚωδίκων Καναλιού



Κώδικας Ελέγχου Απλής Ισοτιμίας

- Μετάδοση 4 συμβόλων σε δυαδικό συμμετρικό κανάλι (Binary Symmetric Channel - BSC).

Δυαδική Αναπαράσταση	Κωδικές Λέξεις
00	000
01	011
10	101
11	110



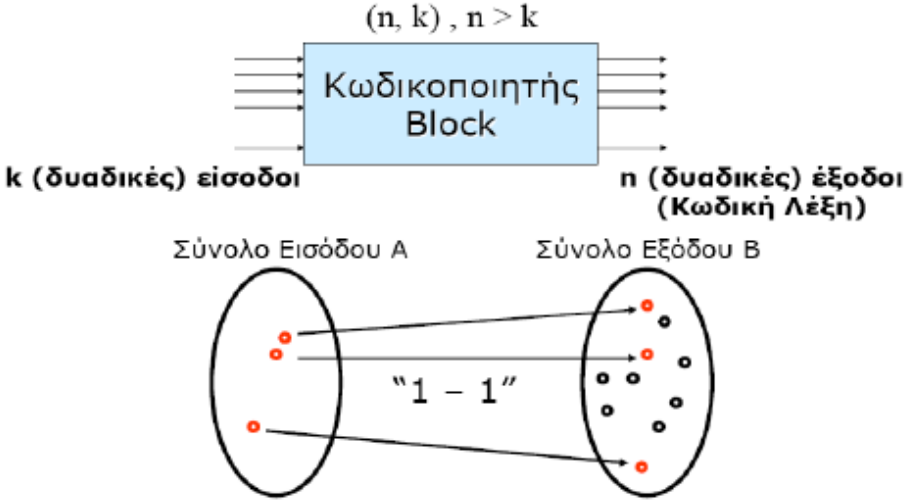
- Σφάλματα: 100, 111, 001, 010

Γραμμικοί Κώδικες Block

- Κώδικες block: μετατροπή ακολουθιών k bits πηγής (blocks) σε ακολουθίες μήκους $n > k$ bits που εξαρτώνται μόνο από το εκάστοτε block εισόδου.
- Γραμμικοί κώδικες: κάθε γραμμικός συνδυασμός (modulo-2 $\oplus$ άθροισμα) δύο κωδικών λέξεων είναι επίσης κωδική λέξη του.
- Ένας γραμμικός κώδικας block $C(n,k)$ αποτελείται (συνήθως) από $M=2^k$ κωδικές λέξεις $\boldsymbol{c}_i$ μήκους n, δηλαδή $C=\{\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_M\}$.
- Κωδικός ρυθμός: $r_c = k / n$
- Για τη διατήρηση ίδιου ρυθμού πληροφορίας:

$$(\textit{ρυθμός εισόδου}) = r_c \times (\textit{ρυθμός εξόδου})$$

- Ο αποκωδικοποιητής αναζητά την κωδική λέξη που είναι πλησιέστερη στο λαμβανόμενο block.



Γεννήτορας & Πίνακας Ελέγχου Ισοτιμίας

- Για έναν γραμμικό κώδικα block (n,k) ορίζεται ο γεννήτορας πίνακας (generation matrix) $\boldsymbol{G}$ διαστάσεων k x n για τον οποίο ισχύει ότι για μια λέξη πληροφορίας $\boldsymbol{u}$, η κωδικοποιημένη λέξη παράγεται ως:

$$\boldsymbol{v} = \boldsymbol{u} \cdot \boldsymbol{G}$$

- Επομένως, οποιοσδήποτε γραμμικός συνδυασμός γραμμών του γεννήτορα είναι μια κωδική λέξη.

- Σημείωση: για την δυαδική περίπτωση τα αθροίσματα είναι modulo-2 ⊕ (XOR).

- Ορίζεται ο πίνακας ελέγχου ισοτιμίας (parity check matrix) $\boldsymbol{H}$ διαστάσεων (n-k) x n για τον οποίο ισχύει ότι για κάθε κωδική λέξη ικανοποιούνται οι παρακάτω σχέσεις

$$\boldsymbol{v} \cdot \boldsymbol{H}^{\mathrm{T}} = \boldsymbol{0} \qquad \boldsymbol{G} \cdot \boldsymbol{H}^{\mathrm{T}} = \boldsymbol{0}$$

Παράδειγμα

- Γραμμικός κώδικας block, n=7 k=4
- Παράγεται από τον Πίνακα γεννήτορα

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

- Έστω λέξη πληροφορίας $u=(1\quad 1\quad 0\quad 1)$
- Τότε

$$v=u\cdot G=(1\quad 1\quad 0\quad 1)\cdot\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&1&0&0&1&0\\1&0&1&0&0&0&1\end{pmatrix}=(0\quad 0\quad 0\quad 1\quad 1\quad 0\quad 1)$$

Βάρος και Απόσταση Hamming

- Βάρος Hamming (ή απλά βάρος κωδικής λέξης) $w(v)$: το πλήθος των μη μηδενικών συνιστωσών (ψηφίων) της κωδικής λέξης v.
- Απόσταση Hamming $d(v_1, v_2)$ δύο κωδικών λέξεων: το πλήθος των συνιστωσών στις οποίες διαφέρουν οι κωδικές λέξεις v_1 και v_2.
- Ελάχιστο βάρος κώδικα w_{min}: το ελάχιστο των βαρών των κωδικών λέξεων εκτός της κωδικής λέξης με όλο μηδενικά.
- Ελάχιστη απόσταση κώδικα d_{min}: η ελάχιστη απόσταση Hamming μεταξύ δύο οποιονδήποτε διαφορετικών κωδικών λέξεων.
- Σε οποιονδήποτε γραμμικό κώδικα αποδεικνύεται ότι $d_{min} = w_{min}$.

Παράδειγμα : Οι λέξεις 01101 και 01111 έχουν απόσταση Hamming ίση με 1

Απόσταση Hamming

- Η σημασία της απόστασης Hamming είναι ότι αν δύο λέξεις απέχουν *d* bits, τότε αρκούν *d* σφάλματα για να μετατρέψουν τη μια στην άλλη.
- Συνήθως και τα 2^m μηνύματα είναι έγκυρα, όχι όμως όλες οι 2^n κωδικές λέξεις. Αυτές επιλέγονται με τρόπο που να μεγιστοποιεί την απόσταση Hamming
- Η απόσταση Hamming μεταξύ των κωδικών λέξεων προσδιορίζει την ικανότητα εντοπισμού σφαλμάτων και την ικανότητα διόρθωσης σφαλμάτων ενός κώδικα
- Αν έχω απόσταση *d*+1 μπορώ να ανιχνεύσω *d* απλά σφάλματα γιατί τα *d* σφάλματα δεν αρκούν να μετατρέψουν μια λέξη σε μια άλλη έγκυρη κωδική λέξη. Άρα το λάθος θα φανεί.
- Για να διορθώσω *d* σφάλματα πρέπει η απόσταση να είναι 2*d*+1 γιατί τότε ακόμα κι αν συμβούν *d* σφάλματα η αρχική κωδική λέξη θα είναι κοντύτερα σε αυτή με τα σφάλματα οπότε ο δέκτης μπορεί να την αντικαταστήσει.

Ικανότητα Ανίχνευσης & Διόρθωσης

- Ένας γραμμικός κώδικας block μπορεί να ανιχνεύσει $t_d = d_{\min} - 1$ σφάλματα.
- Μπορεί να διορθώσει $t_c = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$ σφάλματα.

- Για μια λαμβανόμενη λέξη $\boldsymbol{r}$, ορίζεται το σύνδρομο της ως

$$\boldsymbol{S} = \boldsymbol{r} \cdot \boldsymbol{H}^{\mathrm{T}}$$

- Αν το σύνδρομο δεν είναι μηδενικό, η $\boldsymbol{r}$ δεν αντιστοιχεί σε κωδική λέξη, άρα περιέχει σφάλματα.
- Αν η λαμβανόμενη λέξη γραφεί ως άθροισμα της μεταδιδόμενης λέξης και του σφάλματος ($\boldsymbol{r} = \boldsymbol{v} \oplus \boldsymbol{e}$) τότε ισχύει

$$\boldsymbol{S} = \boldsymbol{e} \cdot \boldsymbol{H}^{\mathrm{T}}$$

Απόσταση Hamming

Έστω δύο κωδικές λέξεις, οι 10001001 και 10110001. Είναι δυνατόν να πούμε σε πόσα bit διαφέρουν αν τις κάνουμε XOR και μετρήσουμε τα "1" στο αποτέλεσμα:

```
10001001
10110001
--------
00111000
```

Αυτή η διαφορά τους ονομάζεται απόσταση Hamming των δύο λέξεων

- ας θεωρήσουμε έναν κώδικα με μόνο τέσσερις έγκυρες κωδικές λέξεις: 0000000000, 0000011111, 1111100000 και 1111111111
- Αυτός ο κώδικας έχει απόσταση 5, που σημαίνει ότι μπορεί να διορθώνει διπλά σφάλματα. Εαν ληφθεί η κωδική λέξη 0000000111, ο δέκτης γνωρίζει ότι η πρωτότυπη πρέπει να ήταν 0000011111. Εαν, ωστόσο, ένα τριπλό σφάλμα αλλάζει το 0000000000 σε 0000000111, το σφάλμα δεν θα διορθωθεί σωστά

Χρήσεις Κωδίκων Καναλιού

- Hamming
  - ECC μνήμες
- Reed Solomon
  - CDs, DVDs, Blue-ray Disks, δορυφορικές επικοινωνίες, DSL
- Turbo
  - Δορυφορικές επικοινωνίες, 3G, 4G, WiMAX
- LDPC (low-density parity-check)
  - DVB-S2, WiMAX, IEEE 802.11