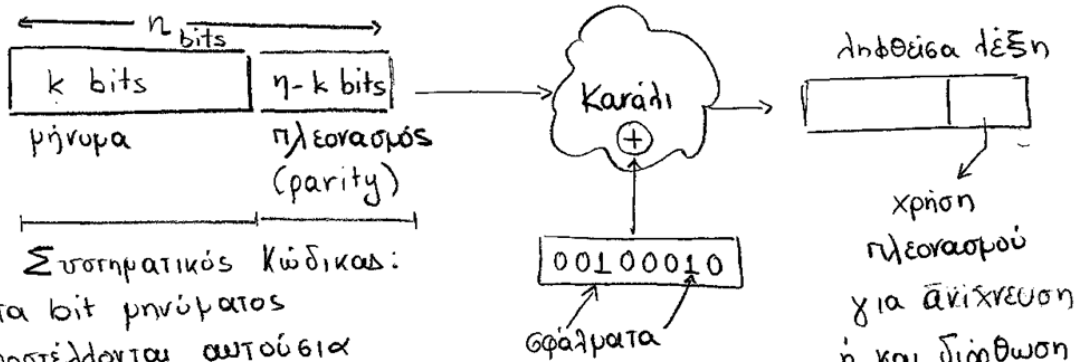
Κώδικας Διόρθωσης Σφαλμάτων (Block Code)



Ρυθμός πληροφορίας: $r = \frac{k}{\eta}$

Βάρος Hamming λέξης x μήκους n bits

$$wt(x) = \sum_{i=1}^{n} (ones) \quad \text{π.χ. } wt(1011001) = 4$$

Απόσταση 2 λέξεων x, y

$$d(x,y) = \sum_{i=1}^{n} (\text{διαφορετικά bits στις αντίστοιχες θέσεις}) =$$

$$= wt(x + y) \quad (+ : \text{XOR})$$

βλ. αρχείο PLH22_OSS4_slides διαφάνειες 47-57

π.χ. $x = 1011001$

$y = 1101000$

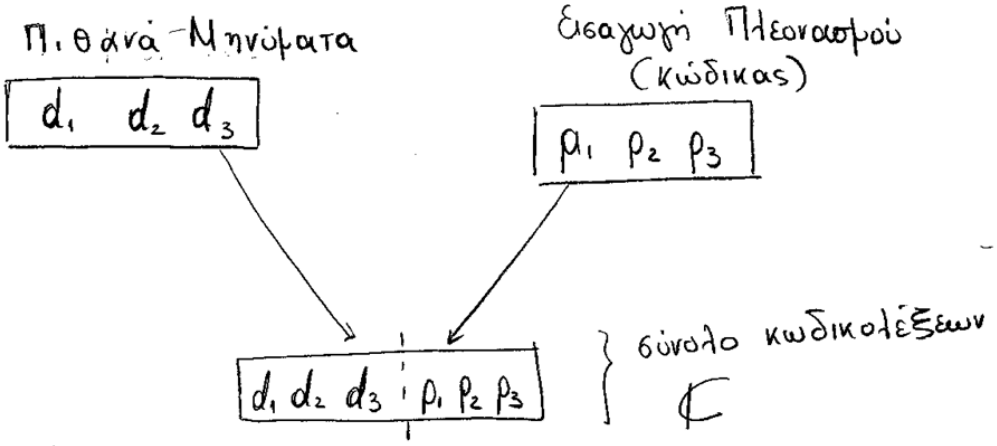
$x+y = 0110001 \rightarrow wt(x+y) = d(x,y) = 3$

διαφορετικά bits μεταξύ x, y

Πιθανότητα αποστολής λέξης x (η bits) και λήψης λέξης y με απόσταση $d(x,y) = d$ [δηλ. να συμβούν d λάθη]

Αν πιθανότητα επιτυχούς μετάδοσης 1 bit: p

τότε $P(d \text{ bits εσφαλμένα}, \eta-d \text{ bits σωστά}) = p^{\eta-d}(1-p)^{d}$ ⇐ Αξιοπιστία



Αν τα ψηφία πλεονασμού προκύπτουν ως γραμμικοί συνδυασμοί των ψηφίων μηνύματος ο κώδικας είναι γραμμικός.

Ιδιότητες γραμμικών κωδίκων

1) $\forall\, x, y \in \mathcal{C}$, $x+y \in \mathcal{C}$

2) $\mathbf{0} = \underbrace{000\ldots0}_{n \text{ bits}} \in \mathcal{C}$

3) Απόσταση κώδικα: (γενικά) η ελάχιστη απόσταση μεταξύ δύο κωδικολέξεων του

Αν $\mathcal{C}$ γραμμικός: Απόσταση = ελάχιστο των βαρών των κωδικολέξεων του $\mathcal{C}$

Μηνύματα

	d_1 d_2	Ελάχιστη απόσταση: 1
m_1	0 0	
m_2	0 1	Αρκεί 1 σφάλμα για
m_3	1 0	να ληφθεί λάθος μήνυμα
m_4	1 1	

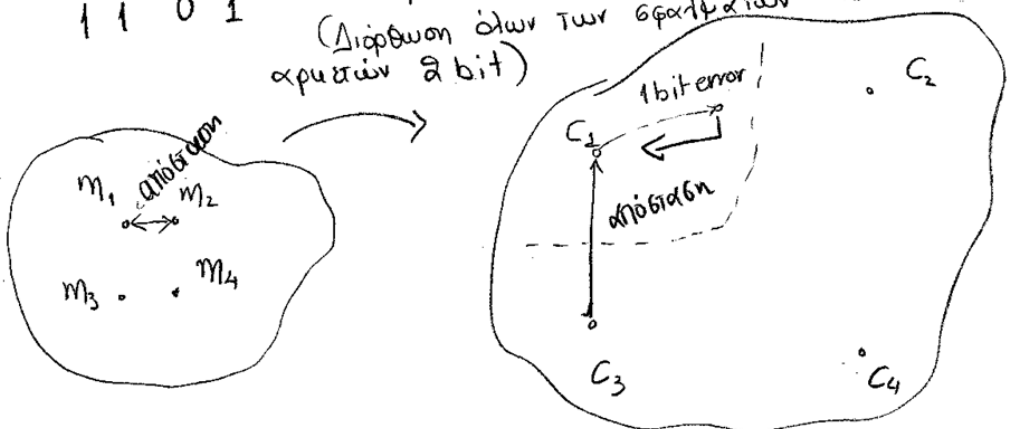
Έστω κώδικας με 2 parity bits

$$p_1 = d_1 + d_2$$

$$p_2 = d_1$$

	d_1 d_2 p_1 p_2	Ελάχιστη απόσταση: 2
C_1	0 0 0 0	
C_2	0 1 1 0	"Αυξάνει" η απόσταση
C_3	1 0 1 1	μεταξύ 2 κωδικολέξεων
C_4	1 1 0 1	αρα αυξάνει η αξιοπιστία

(Διόρθωση όλων των σφαλμάτων 1 bit και αρκετών 2 bit)



Κωδικοποίηση: Αύξηση Πλεονασμού → { Αύξηση Αξιοπιστίας / Κόστος σε εύρος ζώνης

Παράδειγμα (Συνέχεια)

C_1 0 0 0 0

C_2 0 1 1 0

C_3 1 0 1 1

C_4 1 1 0 1

- Αποστολή 00 → (κωδ/ση) '0000' λήψη '0000'

  Σύγκριση με κώδικα → C_1

  Απόφαση: λανθασμένα λέξη '0000' → C_1 → m_1 → '00' (αποκωδικοποίηση)

- Αποστολή 11 → (κωδ/ση) '1101' λήψη '1100' (↑ bit error)

  Σύγκριση με κώδικα → καμμία λέξη

  ελάχιστη απόσταση από C_4

  Απόφαση: λανθασμένα λέξη : '1101' → C_4 → m_4 → '11' (αποκωδικοποίηση)

  (Αποκωδικοποίηση μέγιστης πιθανότητας) διόρθωση

- → Αποστολή 01 → (ΑΜΠ) '0110' λήψη '1111' (bit errors)

  1111 ∉ Φ

  ελάχιστη απόσταση { C_4, C_3 } → ? → Π (πλήρης) ΑΜΠ (Τυχαία Επιλογή C_4)

  Α (ατελής) ΑΜΠ (αίτηση επανεκπομπής)

Θεωρήματα

Κώδικας $\mathcal{C}$ απόστασης d

$\Rightarrow$ Ανιχνεύει όλα τα σφάλματα ε με $wt(\varepsilon) < d-1$

$\Rightarrow$ Δεν ανιχνεύει ένα τουλάχιστον σφάλμα ε με $wt(\varepsilon) = d$

$\Rightarrow$ Διορθώνει όλα τα σφάλματα ε με

$$wt(\varepsilon) \leq \left\lfloor \frac{d-1}{2} \right\rfloor \leftarrow \text{ακέραιο μέρος}$$

$\Rightarrow$ Δεν διορθώνει ένα τουλάχιστον σφάλμα ε με

$$wt(\varepsilon) = 1 + \left\lfloor \frac{d-1}{2} \right\rfloor$$

Κατασκευή Κωδίκων.

- Αν ο κώδικας $\mathcal{C}$ ορίζεται ως ανάπτυγμα ενός συνόλου κωδικολέξεων S, $\mathcal{C} = \langle S \rangle$ τότε
  - ο $\mathcal{C}$ περιλαμβάνει:
    - → Το **0**
    - → όλα τα στοιχεία του S
    - → όλους τους γραμμικούς συνδυασμούς των στοιχείων του S
- Βάση Κώδικα $\mathcal{C}$: είναι ένα σύνολο κωδικολέξεων B για το οποίο ισχύουν τα εξής
  - → $\mathcal{C} = \langle B \rangle$
  - → Τα στοιχεία του B είναι γραμμικά ανεξάρτητα (κανένα δεν προκύπτει ως γραμμικός συνδυασμός των υπολοίπων)

Γεννήτορας Πίνακας G

Πίνακας Διαστάσεων $k \times \eta$ για

κωδικοποίηση μηνυμάτων k bits σε κωδικολέξεις η bits

Μήνυμα (k bits) × G ⟶ κωδική λέξη

π.χ.

$$G = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$$

k = 4 γραμμές ⇒ μήκος μηνυμάτων 4 bits

η = 7 στήλες ⇒ μήκος κωδικολέξης 7 bits

Έστω μήνυμα 0101

βλ. αρχείο PLH22_OSS4_slides διαφάνειες 66-80-

Κωδικοποίηση

$0101 \cdot G = 0 \times (1000111) + 1 \times (0100110) + 0 \times (0010101) + 1 \times (0001011) =$ κωδικολέξη 0101101

(αλλό γινόμενο, XOR)

μήνυμα: 0101 — πλεονασμός: 101

Στην ουσία προσθέτουμε τη 2η και 4η γραμμή του G

Αποκωδικοποίηση

Έλεγχος ισοτιμίας

Κατασκευάζεται πίνακας ισοτιμίας H $\eta \times (\eta - k)$

Αν η λαθεισα κωδικολέξη × ανήκει στον κώδικα τότε

$\times \cdot H = 0 \leftarrow$ σύνδρομο

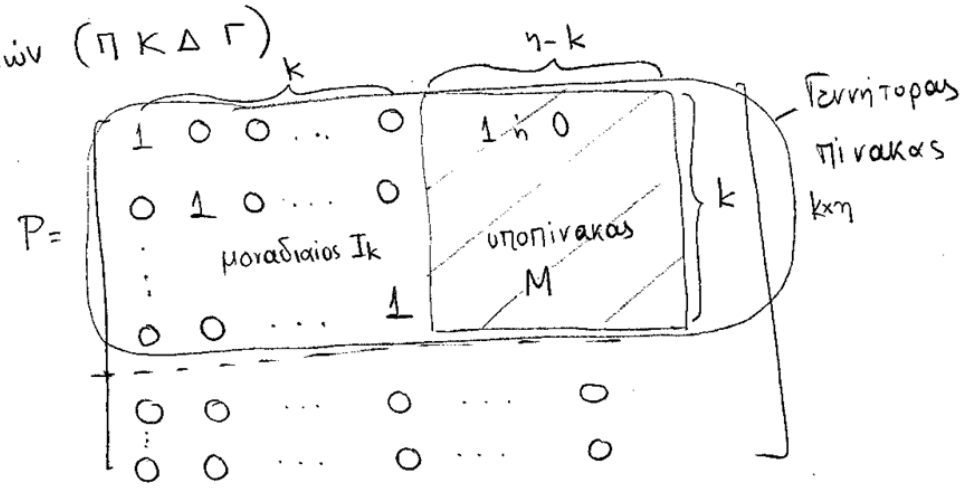
Αν το σύνδρομο είναι μη μηδενικό, χρησιμοποιείται για την ανίχνευση και πιθανή διόρθωση σφαλμάτων.

Εύρεση Πινάκων G, H

Αν δίνεται ο κώδικας $\mathbb{C}$ ή κάποιο υποσύνολό του S του οποίου το ανάπτυγμα δίνει τον $\mathbb{C}$, $\mathbb{C} = \langle S \rangle$ με τη μορφή συνόλου κωδικολέξεων $\{S_1, S_2, \ldots, S_m\}$:

→ Σχηματίζουμε τον πίνακα $P = \begin{bmatrix} S_1 \\ S_2 \\ \vdots \\ S_m \end{bmatrix}$

Με αντιμετάθεση γραμμών ή αντικατάσταση γραμμής από το άθροισμά της με άλλη γραμμή μετασχηματίζουμε τον P σε μορφή Περιορισμένης Κλιμακωτής Διάταξης Γραμμών (ΠΚΔΓ)



∴ Γραμμές του G: βάση του $\mathbb{C}$

Κατασκευή πίνακα ισοτιμίας

$$H = \begin{bmatrix} M_{k\times(n-k)} \\ \hline I_{n-k} \end{bmatrix}_{n\times(n-k)}$$

Από τον H προκύπτει και η βάση του δυϊκού κώδικα $\mathcal{C}^{\perp}$ (Σημείωση: Αν $\mathcal{C}=\{\alpha_1,\alpha_2,\dots,\alpha_n\}$ τότε ο κώδικας $\mathcal{C}'=\{\beta_1,\dots,\beta_m\}$ είναι δυϊκός του $\mathcal{C}$ δηλ. $\mathcal{C}'=\mathcal{C}^{\perp}$ εφόσον

$\forall i,j$ ισχύει $\alpha_i\cdot\beta_j=0$, $i=1,\dots,n$, $j=1,\dots,m$

Οι στήλες του H δίνουν μια βάση για τον $\mathcal{C}^{\perp}$

Εύρεση Απόστασης Κώδικα

1) Αν γνωρίζουμε όλες τις κωδικολέξεις ⇒ ελάχιστο βάρος

2) Αν γνωρίζουμε ένα υποσύνολο S τέτοιο ώστε $\mathcal{C}=\langle S\rangle$
   ↳ είτε υπολογίζουμε το πλήρες ανάπτυγμα $\langle S\rangle$ και εφαρμόζουμε το βήμα 1)
   ↳ είτε προσδιορίζουμε τους G, H και πηγαίνουμε στο βήμα 3

3) Όριο Singleton: $d \leq n-k$ για γραμμικούς κώδικες (n, k)

Α. Θέτουμε $d_0 = 2$.

Β. Παρατηρούμε στον G αν υπάρχουν d_0 γραμμές των οποίων τα μέρη ισοτιμίας να αθροίζονται σε 000... Αν υπάρχουν τότε απόσταση $d = d_0$. Αν όχι, τότε θέτουμε $d_0 = d_0 + 1$ και επαναλαμβάνουμε το (Β) μέχρι $d_0 = n-k$.

Όριο συστηματικό ακολουθείται με τις γραμμές του πίνακα H.

π.χ. $H = \begin{bmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 1\,1\,0 \\ 1\,0\,1 \\ 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix}$ →

$$G = \underbrace{\left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right]}_{n=7} \Big\} k=4$$

$d \leq n-k = 3$

Όμως υπάρχουν { 2 γραμμές του G με κοινό μέρος ισοτιμίας ή 2 όμοιες γραμμές του H } που αθροίζονται σε '000'

Άρα $d = 2$.

Μέθοδοι Αποκωδικοποίησης

Ⓐ Μέθοδος Συνοράδων κώδικα $\mathbb{C}(n,k)$

Συνοράδα κώδικα $\mathbb{C}$ για το στοιχείο x: το σύνολο $\mathbb{C}+x$.

Πλήθος διαφορετικών συνοράδων: 2^{n-k}

1. Λήψη λέξης y
2. Υπολογισμός συνοράδας $\mathbb{C}+y$
3. Αν $y \in \mathbb{C}$ τότε $0 \in \mathbb{C}+y$
4. Αν $y \notin \mathbb{C}$ τότε επιλέγουμε το στοιχείο του $\mathbb{C}+y$ με το μικρότερο βάρος $\Rightarrow$ πρότυπο σφάλματος ε
5. Διόρθωση λέξης: $y' = y + \varepsilon$

Αν περισσότερα του 1 δυνατά πρότυπα σφάλματος ελαχίστου βάρους $\Rightarrow$
- ΠΑΝΠ τυχαία επιλογή ενός
- ΑΑΝΠ αίτηση για επανεκπομπή

βλ. αρχείο PLH22_OSS4_slides διαφάνειες 82-91

(Β) Με τυπική Διάταξη Αποκωδικοποίησης .ΤΔΑ. "

1. Υπολογισμός πίνακα H

2. Για πρότυπα σφάλματος ελάχιστου βάρους E_i υπολογίζουμε τα γινόμενα (σύνδρομα) $E_i H$ και τα βάζουμε σε πίνακα

πρότυπο σφάλματος	σύνδρομο

3. Για τη ληφθείσα λέξη y υπολογίζουμε το γινόμενο yH

4. Αν $yH = 0$ $y \in C$

5. Αν $yH \neq 0$ αναζητούμε το μη μηδενικό σύνδρομο yH στον ανωτέρω πίνακα και το αντιστοιχίζουμε στο σχετικό πρότυπο σφάλματος E_i

6. Διόρθωση λέξης $y' = y + E_i$

7. Αν περισσότερα πρότυπα σφάλματος αντιστοιχούν στο σύνδρομο, ισχύουν οι προαναφερθείσες επιλογές ΠΑΜΠ, ΑΑΜΠ

11

Θέμα 4 Ενδεικτικές Ασκήσεις

Λέξη Πληροφορίας $d_1\ d_2$	Κωδικολέξη $d_1\ d_2\ p_1 p_2 p_3$
00	00000
01	01101
10	10111
11	11010

? Συστηματικός κώδικας

Όλες οι κωδικολέξεις περιέχουν στα πρώτα 2 ψηφία τους τις αντίστοιχες λέξεις πληροφορίας

$p_1 = a_1 d_1 + a_2 d_2$

2η γραμμή $p_1 = 1, \quad d_1 = 0 \quad d_2 = 1$

$\Rightarrow 1 = a_2$

3η γραμμή $p_1 = 1, \quad d_1 = 1, \quad d_2 = 0$ → $p_1 = d_1 + d_2$

$\Rightarrow 1 = a_1$

$p_2 = d_1$

$p_3 = d_1 + d_2$

ο κώδικας είναι γραμμικός $\quad \eta = 5$

$k = 2$

12

Εύρεση G

$$G = \left[\begin{array}{cc|ccc} d_1 & d_2 & p_1 & p_2 & p_3 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right]$$

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Απόσταση Κώδικα $d \leq n-k = 3$ (όριο Singleton)

$d = 3$ (ελάχιστο βάρος κώδικα - που μας δίνεται)

Ικανότητα διόρθωσης λαθών $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$. bit error

Τυπική Διάταξη αποκωδικοποίησης (ΤΔΑ)

Πρότυπο ελαχίστου βάρους (x) / Πρότυπο σφάλματος	Σύνδρομο $x \cdot H$
1 0 0 0 0	1 1 1
0 1 0 0 0	1 0 1
0 0 1 0 0	1 0 0
0 0 0 1 0	0 1 0
0 0 0 0 1	0 0 1
0 0 0 1 1 / ή 1 0 1 0 0	0 1 1
0 0 1 1 0 / ή 1 0 0 0 1	1 1 0

ΠΑΜΠ: Επιλογή ενός προτύπου

ΑΑΜΠ: Κενό πρότυπο, αίτηση επανεκπομπής

Παράδειγμα Αποκωδικοποίησης

Λήψη λέξης $y = 0\ 0\ 0\ 0\ 1 \notin C$

→ Μέθοδος με συνοράδες

Εύρεση $C + 0,0001 = \{\underline{00001}, 01100, 10110, 11011\}$

πρότυπο σφάλματος ελαχίστου βάρους

Άρα διορθωμένη λέξη $y' = y + 00001 = \underline{00000}$

→ Μέθοδος με ΤΔΑ.

Εύρεση συνδρόμου $yH = 00001 \cdot H = \underline{001}$

Από πίνακα ΤΔΑ πρότυπο σφάλματος → 00001.

άρα $y' = y + 00001 = 00000$

Με βάση τον πίνακα ΤΔΑ και υποθέτοντας ΠΑΜΠ.

ο κώδικας διορθώνει:

→ 5 σφάλματα 1 bit

→ 2 σφάλματα 2 bit

Πιθανότητα σφάλματος

$P_F = 1 - P(\text{καμένα σφάλμα}) - P(\text{σφάλματα 1bit}) - P(\text{2 σφάλματα 2 bit}) = 1 - (1-\varepsilon)^5 - 5\varepsilon(1-\varepsilon)^4 - 2\varepsilon^2(1-\varepsilon)^3$

βλ. αρχείο PLH22_OSS4_slides διαφάνειες 109-114

Κώδικας Hamming:

Χαρακτηριστικά:

→ Μήκος της μορφής $n = 2^r - 1 \quad r \geq 2$

→ Πίνακας ελέγχου ισοτιμίας H με όλες τις μη μηδενικές λέξεις μήκους r

→ Διάσταση $k = n - r = 2^r - 1 - r$

→ Απόσταση $d = 3$

→ Ικανότητα διόρθωσης 1 σφάλματος $\left(\left\lfloor \frac{d-1}{2} \right\rfloor = 1\right)$

→ Στην ΤΔΑ ο πίνακας συνδρόμων περιλαμβάνει όλες τις γραμμές του H [όλες τις δυνατές λέξεις μήκους r]

· Όριο Hamming.

Αν έχουμε κώδικα C με πλήθος κωδικών λέξεων $|C|$ μήκος κωδικολέξης n και απόσταση $d = 2t+1$ ή $d = 2t+2$ τότε ισχύει ότι $|C| \cdot \left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t}\right] \leq 2^n$

$$\therefore \binom{n}{i} = \frac{n!}{i!(n-i)!}$$

Τέλειοι κώδικες

Αν $d = 2t+1$ και ισχύει η ανωτέρω σχέση με το σύμβολο της ισότητας, ο κώδικας είναι <u>τέλειος</u>

15

Παράδειγμα κώδικα Hamming

$$H = \left[\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$$ ← όλες οι μη μηδενικές δυνατές δέξεις 3 bit

$n = 7$

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

$k = 4$

$d \leq 7 - 4 = 3$ (όριο Singleton)

$d = 3$ (ιδιότητα Hamming)

Πλήθος κωδικολέξεων

$$|C| = 2^k = 2^4$$

Υπολογισμός ορίου Hamming $\quad d = 2 \cdot 1 + 1$, $t = 1$

$$|C| \cdot \left[\binom{n}{0} + \binom{n}{t}\right] =$$

$$= 2^4 \cdot \left[\binom{7}{0} + \binom{7}{1}\right] = 2^4 \cdot \left[\frac{7!}{0!\,7!} + \frac{7!}{1!\cdot 6!}\right] =$$

$$= 2^4 \left[1 + 7\right] = 2^4 \cdot 8 = 2^4 \cdot 2^3 = 2^7 = 2^n.$$

Άρα, τέλειος κώδικας

Πρόσθετα παραδείγματα

βλ. αρχείο PLH22_OSS4_slides διαφάνειες 92-107-

ΘΕΜΑ 2/ΓΕ5/2012-13

Στόχος της άσκησης *είναι η εξοικείωση με έννοιες και αλγόριθμους που εφαρμόζονται σε γραμμικούς κώδικες ελέγχου σφάλματος.*

Σχετικές ασκήσεις: *Θ3/ΓΕ5/2011-12, Θ4/ΓΕ5/2010-11, Θ4/ΓΕ5/2009-10, Θ5/ΕΞ2009Α και Θ5/ΕΞ2010Β*

Δίνεται κώδικας Hamming μήκους 7 με πίνακα ισοτιμίας τον ακόλουθο:

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_2 \\ 0 & 1 & 1 \\ 1 & \alpha_3 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Ζητούνται τα ακόλουθα:
(α) Να προσδιοριστούν τα α_1, α_2, α_3,

(β). Να βρεθεί ο γεννήτορας πίνακας G.

(γ). Δείξτε ότι η λέξη

$$s = [1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0]$$

δεν είναι κωδική λέξη του κώδικα.

(δ). Να σχηματίσετε την Τυπική Διάταξη Αποκωδικοποίησης (ΤΔΑ) για ΠΑΜΠ και ΑΑΜΠ

(ε).Να βρεθούν το σύνδρομο και το πρότυπο σφάλματος που αντιστοιχούν στη ληφθείσα λέξη $r = [1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1]$

η οποία αποκωδικοποιείται στη συνέχεια στην κωδική λέξη

$$z = [0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1]$$

Ενδεικτική Μεθοδολογία: *Να υπολογίσετε πρώτα τους άγνωστους συντελεστές και έπειτα τον πίνακα G σύμφωνα με τον ορισμό του. Τα υπόλοιπα μεγέθη είναι εφαρμογές των ορισμών τους και της σχετικής θεωρίας.*

ΑΠΑΝΤΗΣΗ

α). Επειδή ο κώδικας είναι Hamming μήκους n=7, ο πίνακας ελέγχου ισοτιμίας Η πρέπει να απαρτίζεται από όλες τις δυνατές μη μηδενικές λέξεις μήκους r=3 (βλ. τον ορισμό κώδικα Hamming, σελ. 151 βιβλίου, Ορισμός 4.6) αφού ισχύει

$$n = 2^r - 1 = 7$$

Επομένως η απόστασή του είναι d=3 και η διάστασή του είναι k=4.

Α! τρόπος.

Με απλή παρατήρηση των γραμμών του Η βλέπουμε ότι οι παραμετρικές γραμμές αντιστοιχούν στις λέξεις 101 και 110 οπότε, λόγω και της θέσης των παραμέτρων α_1, α_2, α_3 στις παραμετρικές λέξεις θα έχουμε:

α_1=0, α_2=1, α_3=1.

Β! τρόπος

Για να υπολογίσω τους άγνωστους συντελεστές του πίνακα θα χρησιμοποιήσω τον κανόνα υπολογισμού της απόστασης του με τη χρήση *του πίνακα ελέγχου ισοτιμίας, δηλαδή τον ελάχιστο αριθμό γραμμών του πίνακα των οποίων το άθροισμα είναι 0.*

Βήμα 1ο

Χρησιμοποιώ τις γραμμές 3η, 4η, 7η

$$\begin{bmatrix}1 & \alpha_3 & 0\end{bmatrix}+\begin{bmatrix}1 & 1 & 1\end{bmatrix}+\begin{bmatrix}0 & 0 & 1\end{bmatrix}=\begin{bmatrix}0 & 0 & 0\end{bmatrix}$$

$$\alpha_3 = 1$$

Επομένως ο πίνακας ισοτιμίας του κώδικα διαμορφώνεται ως

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_2 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Βήμα 2ο

Χρησιμοποιώ τις γραμμές 1η, 2η, 3η

$$[1 \quad \alpha_1 \quad \alpha_2] + [0 \quad 1 \quad 1] + [\mathbf{1} \quad \mathbf{1} \quad 0] = [0 \quad 0 \quad 0]$$

$$[1+0+1 \quad \alpha_1 + 1 + \mathbf{1} \quad \alpha_2 + 1 + 0] = [0 \quad 0 \quad 0]$$

$$\boldsymbol{\alpha_1 = 0 \quad \alpha_2 = 1}$$

Τελικά ο πίνακας ισοτιμίας του κώδικα διαμορφώνεται ως

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

β). Όπως γνωρίζω δεδομένου ότι ο πίνακας ισοτιμίας Η είναι 7x3 και της μορφής $H = \begin{bmatrix} M \\ I \end{bmatrix}$ με

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Ο γεννήτορας πίνακας $G = [I \quad M]$ διάστασης 4x7 θα δίνεται ως

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

γ). Γνωρίζω ότι για να ανήκει η λέξη **s** στον κώδικα, θα πρέπει να ισχύει $s \cdot H = 0$ («Θεωρία Πληροφορίας», σελ. 145) και επομένως

$$s \cdot H = [1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0] \cdot \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0 \quad 1 \quad 0]$$

Αφού το παραπάνω κριτήριο δεν ισχύει, η λέξη s δεν ανήκει στον κώδικα C.

δ). Για το σχηματισμό της ΤΔΑ, πρέπει να βρούμε για κάθε συνομάδα το σύνδρομό της και το πρότυπο σφάλματος ελάχιστου βάρους, δηλαδή τον οδηγό της συνομάδας.

Δεν είναι όμως απαραίτητο να προσδιορίσουμε κάθε συνομάδα, αρκεί να δοκιμάσουμε τις λέξεις με μικρό βάρος για να οδηγηθούμε στο ζητούμενο.

Πρώτα εξετάζουμε τις λέξεις βάρους 1, δηλαδή τις λέξεις *0000001, 0000010, 0000100, 0001000, 0010000, 0100000 και 1000000:*

$$\begin{aligned}
[0\ 0\ 0\ 0\ 0\ 0\ 1] \cdot H &= [0\ 0\ 1] \\
[0\ 0\ 0\ 0\ 0\ 1\ 0] \cdot H &= [0\ 1\ 0] \\
[0\ 0\ 0\ 0\ 1\ 0\ 0] \cdot H &= [1\ 0\ 0] \\
[0\ 0\ 0\ 1\ 0\ 0\ 0] \cdot H &= [1\ 1\ 1] \\
[0\ 0\ 1\ 0\ 0\ 0\ 0] \cdot H &= [1\ 1\ 0] \\
[0\ 1\ 0\ 0\ 0\ 0\ 0] \cdot H &= [0\ 1\ 1] \\
[1\ 0\ 0\ 0\ 0\ 0\ 0] \cdot H &= [1\ 0\ 1]
\end{aligned}$$

Παρατηρούμε ότι έχουμε λάβει όλα τα δυνατά σύνδρομα αφού το σύνδρομο [0 0 0] συμπεριλαμβάνεται πάντα και επομένως

ΤΔΑ ΓΙΑ ΠΑΜΠ		**ΤΔΑ ΓΙΑ ΑΑΜΠ**	
[0 0 0 0 0 0 1]	[0 0 1]	[0 0 0 0 0 0 1]	[0 0 1]
[0 0 0 0 0 1 0]	[0 1 0]	[0 0 0 0 0 1 0]	[0 1 0]
[0 0 0 0 1 0 0]	[1 0 0]	[0 0 0 0 1 0 0]	[1 0 0]
[0 0 0 1 0 0 0]	[1 1 1]	[0 0 0 1 0 0 0]	[1 1 1]
[0 0 1 0 0 0 0]	[1 1 0]	[0 0 1 0 0 0 0]	[1 1 0]
[0 1 0 0 0 0 0]	[0 1 1]	[0 1 0 0 0 0 0]	[0 1 1]
[1 0 0 0 0 0 0]	[1 0 1]	[1 0 0 0 0 0 0]	[1 0 1]
[0 0 0 0 0 0 0]	[0 0 0]	[0 0 0 0 0 0 0]	[0 0 0]

Παρατηρούμε ότι για κώδικες Hamming οι Τυπικές Διατάξεις Αποκωδικοποίησης (ΤΔΑ) για ΠΑΜΠ και ΑΑΜΠ "συμπίπτουν"

ε). Για να προσδιορίσουμε το πρότυπο σφάλματος που χρησιμοποιήθηκε στην αποκωδικοποίηση, θα εφαρμόσω τον τύπο της σελ. 143 του βιβλίου «Θεωρία Πληροφορίας και Κωδικοποίησης»

$$\varepsilon = r + z$$
$$\varepsilon = [1\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1] + [0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 1] = [1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0]$$

Το πρότυπο αυτό σφάλματος αντιστοιχεί στο σύνδρομο [1 0 1] όπως προσδιορίζεται και από την ΤΔΑ στο προηγούμενο ερώτημα.

ΘΕΜΑ 4 /ΓΕ5/2009-10

Στόχος της άσκησης *είναι η εξοικείωση με έννοιες και αλγόριθμους που εφαρμόζονται σε γραμμικούς κώδικες ελέγχου σφάλματος. Σχετικές ασκήσεις: Θ3/ΓΕ5/2008-9.*

Θεωρούμε τον δυαδικό κώδικα ο οποίος προκύπτει από τις παρακάτω σχέσεις

1) $x_0 = u_1 \oplus u_2 \oplus u_3$,
2) $x_1 = u_0 \oplus u_1 \oplus u_2$,
3) $x_2 = u_0 \oplus u_1 \oplus u_3$,
4) $x_3 = u_0 \oplus u_2 \oplus u_3$,
5) $x_4 = u_0$,
6) $x_5 = u_1$,
7) $x_6 = u_2$,
8) $x_7 = u_3$

Τα x_i, i=0,1,…,7 είναι τα ψηφία του κώδικα που προκύπτουν από την κωδικοποίηση 4 bits πληροφορίας u_j, j=0,1,2,3

(α) Είναι ο κώδικας συστηματικός; Είναι ο κώδικας γραμμικός; Εάν ναι, ποια είναι η διάστασή του και ποιος ο ρυθμός του κώδικα;

(β) Βρείτε το γεννήτορα πίνακα G καθώς και τον πίνακα ισοτιμίας H.

(γ) Βρείτε την ελάχιστη απόσταση d_{min}, του κώδικα. Πόσα λάθη ανιχνεύει και πόσα διορθώνει;

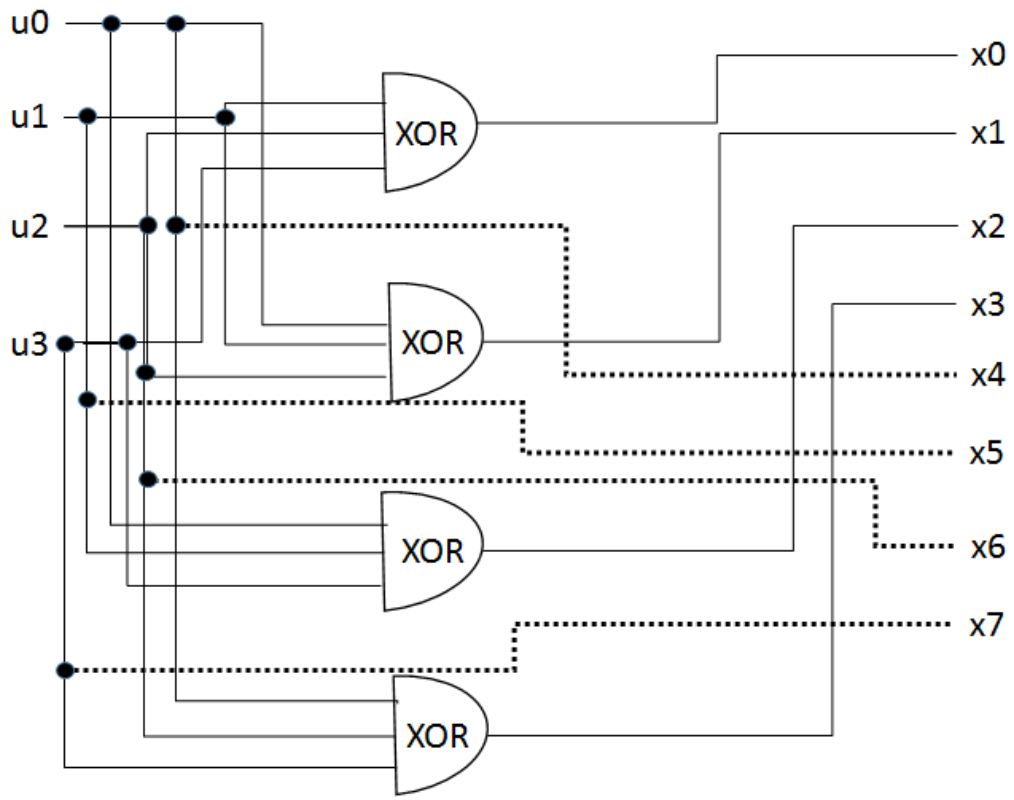
(δ) Βρείτε το δυϊκό κώδικα $C^{\perp}$. Τι παρατηρείτε σε σχέση με τον κώδικα C;

{Υπόδειξη: Για να βρείτε πώς συνδέονται οι δύο κώδικες αρκεί να δημιουργήσετε τις κωδικές λέξεις μέσω των γεννητόρων πινάκων και να τις συγκρίνετε μεταξύ τους.}

Ενδεικτική Μεθοδολογία: *Για την απάντηση του πρώτου ερωτήματος εξετάζουμε αν πληρούνται οι αντίστοιχες ιδιότητες. Για τον προσδιορισμό του γεννήτορα πίνακα λαμβάνουμε υπόψη αν ο κώδικας είναι συστηματικός και δημιουργούμε μια βάση, δηλαδή ένα γραμμικώς ανεξάρτητο υποσύνολο του κώδικα. Για την απάντηση του ερωτήματος 4, λάβετε υπόψη ότι οι στήλες του πίνακα ισοτιμίας Η του κώδικα C αποτελούν βάση του δυϊκού κώδικα* $C^{\perp}$.

Απάντηση

1. Ο κώδικας είναι συστηματικός δεδομένου ότι τα ψηφία πληροφορίας $\mathbf{u_0 - u_3}$ περνούν αυτούσια στον αποκωδικοποιητή αφού καταλαμβάνουν αντίστοιχα τα ψηφία $\mathbf{x_4 - x_7}$ της κάθε κωδικής λέξης. Ο κώδικας είναι γραμμικός γιατί όλες οι εξισώσεις από τις οποίες ορίζεται είναι γραμμικές. Η διάσταση του κώδικα είναι k=4 δεδομένου ότι κωδικοποιούμε 4 ψηφία πληροφορίας και ο κώδικας είναι συστηματικός οπότε οι γραμμές του γεννήτορα πίνακα είναι γραμμικώς ανεξάρτητες. Τέλος ο ρυθμός του κώδικα είναι k/n=4/8=1/2.Παρακάτω παρατίθεται ενδεικτικά το διάγραμμα του κώδικα (δεν ζητείται από την εκφώνηση)



2. Ο γεννήτορας πίνακας G θα είναι της μορφής [M I] καθότι τα ψηφία πληροφορίας καταλαμβάνουν τις 4 τελευταίες θέσεις της κάθε κωδικής λέξης. Για το λόγο αυτό μπορούμε να δημιουργήσουμε τον γεννήτορα πίνακα με γραμμικώς ανεξάρτητα διανύσματα βάσης δημιουργώντας τον μοναδιαίο πίνακα I_{4x4} στο τέλος του G και χρησιμοποιώντας τις σχέσεις της άσκησης για να βρούμε τον M_{4x4}. Έτσι έχουμε,

$$G = [M \quad I] = \begin{bmatrix} & 1 & 0 & 0 & 0 \\ M & 0 & 1 & 0 & 0 \\ & 0 & 0 & 1 & 0 \\ & 0 & 0 & 0 & 1 \end{bmatrix} \overset{\Sigma\chi\acute{\epsilon}\sigma\epsilon\iota\varsigma\ x_0 - x_3}{=} \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Άρα ο πίνακας ισοτιμίας Η που προκύπτει είναι

$$H = \begin{bmatrix} I \\ M \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

3. Η ελάχιστη απόσταση d_{min} του κώδικα θα προκύψει από τον πίνακα ισοτιμίας Η.

Παρατηρούμε ότι $d_{min} > 2$ διότι δεν υπάρχουν δύο ίδιες γραμμές στον πίνακα Η. Επίσης παρατηρούμε ότι $d_{min} > 3$ διότι . Όλες οι γραμμές του Η έχουν περιττό αριθμό '1'. Παρατηρούμε λοιπόν ότι $d_{min} = 4$ διότι μπορούν να βρεθούν 4 γραμμές του Η που το άθροισμά τους να είναι 0, π.χ. η $1^η$, $2^η$, $3^η$ και $6^η$ γραμμή ή $2^η$, $3^η$, $4^η$ και $5^η$ γραμμή κ.ο.κ.

Έτσι λοιπόν ο κώδικας ανιχνεύει 3 λάθη και διορθώνει 1 λάθος.

4. Γνωρίζουμε ότι οι στήλες του πίνακα ισοτιμίας Η του κώδικα C αποτελούν τα διανύσματα βάσης του δυϊκού κώδικα $C^{\perp}$ και άρα δημιουργούν τον γεννήτορα πίνακα $G^{\perp}$ του δυϊκού κώδικα $C^{\perp}$.

Δηλαδή έχουμε ότι

$$G^{\perp} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} I & M \end{bmatrix}$$

Χρησιμοποιώντας τους δύο γεννήτορες πίνακες μπορούμε να δούμε ότι δημιουργούν τον ίδιο κώδικα. Δηλαδή ο κώδικας C και ο δυϊκός του κώδικας είναι ίδιοι. Ένας κώδικας που ταυτίζεται με τον δυϊκό του λέγεται αυτοδυϊκός.