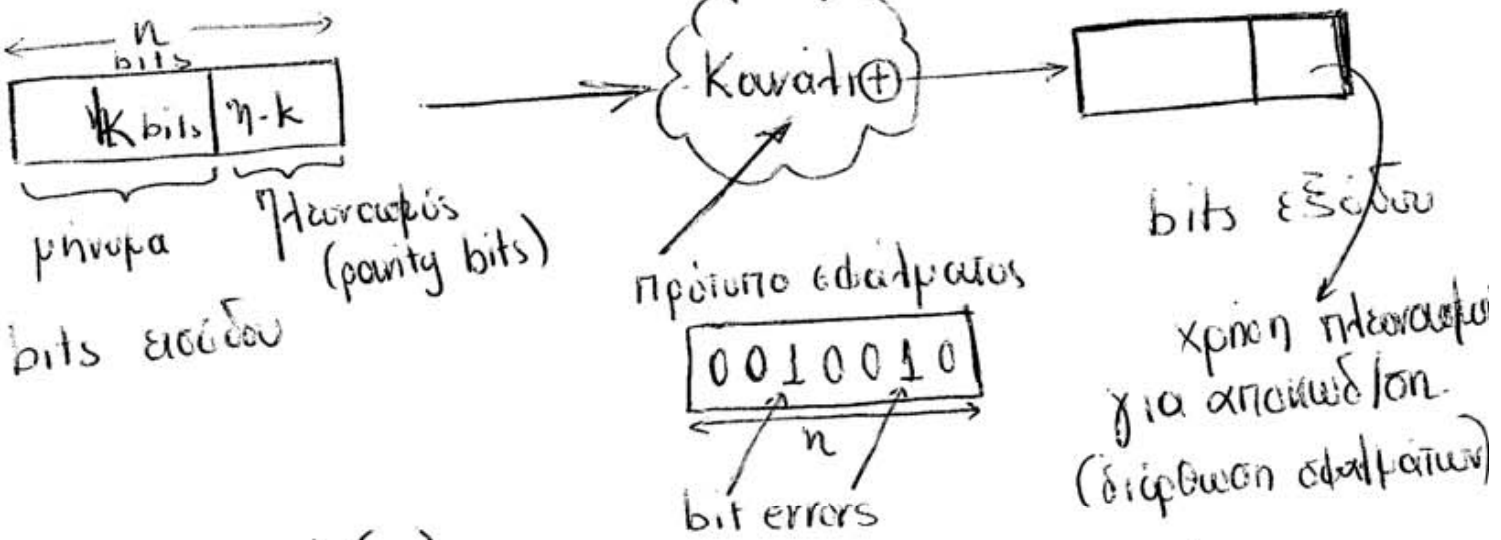
ΕΑΠ/ΠΛΗ22/ΑΘΗ.3
5η ΟΣΣ
27/04/2013

Ν.Δημητρίου

Θεωρία Κωδικοποίησης Καναλιού

Συστηματικός Κώδικας



Ορισμοί

- Βάρος Hamming $wt(x)$ (σελ 118-120) λέξης X μήκους n bits: $wt(x) = \sum_{i=1}^{n} (ones)$

  π.χ. $wt(1011001) = 4$

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

  $= wt(x+y)$

πχ $X = 1011001$

$y = 1101000$

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

διαφορετικά bits μεταξύ x, y

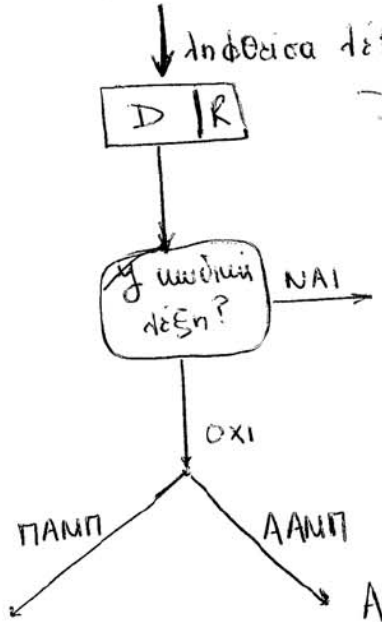
- Πιθανότητα Αποστολής λέξης x και λήψης λέξης y με απόσταση $d(x,y) = d$

Θεωρούμε τα σφάλματα bits ανεξάρτητα μεταξύ τους.

Άρα, εφόσον ο αριθμός των εσφαλμένων bits είναι ίσος με d έχουμε (υποθέτοντας p την πιθανότητα επιτυχούς μετάδοσης bit μέσω του καναλιού (αξιοπιστία)) - σελ. 117.

$\Pi(x,y) = P(n-d \text{ bits σωστά}, d \text{ bits εσφαλμένα}) = p^{n-d} \cdot (1-p)^d$

Αποκωδικοποίηση (ccl 122)



Πλήρης Αποκωδικοποίηση Μέγιστης Πιθανότητας (ΠΑΜΠ)

(1) Αν υπάρχει 1 κωδική λέξη x ώστε $d(x,y) = \min$ τότε $y \to x$

(2) Αν ∃ περισσότερες κωδικές λέξεις x_i ώστε $d(y,x_i) = \min$, αυθαίρετα διαλέγουμε μια από αυτές $y \to x_i$

Ατελής Κωδικοποίηση Μέγιστης Πιθανότητας

(1) όπως στην ΠΑΜΠ

(2) Αν ∃ περισσότερες λέξεις x_i ώστε $d(y,x_i) = \min$

ζητείται αναμετάδοση της λέξης

Θεωρήματα

(1) (4.2 σελ. 124)

Κώδικας $\mathbb{C}$ απόστασης d ανιχνεύει όλα τα σφάλματα ε με $wt(\varepsilon) < d-1$. $\exists$ ένα τουλάχιστον ε με $wt(\varepsilon) = d$ που δεν ανιχνεύει ο $\mathbb{C}$

(2) (4.3, σελ 125)

Κώδικας $\mathbb{C}$ απόστασης d διορθώνει όλα τα ε με $wt(\varepsilon) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$. $\exists$ 1 τουλάχιστον ε με $wt(\varepsilon) = 1 + \left\lfloor \frac{d-1}{2} \right\rfloor$ που δε διορθώνει ο $\mathbb{C}$

Γραμμικοί Κώδικες

$\mathbb{C}$ γραμμικός αν $\forall x,y \in \mathbb{C}$, $x+y \in \mathbb{C}$

$\Rightarrow \mathbf{0} \in \mathbb{C}$

$\Rightarrow d = \min\{wt(x)\}$ $x \in \mathbb{C}$ $x \neq 0$

- Γραμμικό αναπτύγμα υποσυνόλου S

  $C = \langle S \rangle = \{0, S,$ όλα τα αθροίσματα δέξεων του $S\}$ σελ.131

- Ορθογώνιο Συμπλήρωμα υποσυνόλου $S = \{x_1, x_2, \dots, x_n\}$

  $S^{\perp} = \{x_1', x_2', \dots, x_n'\}$ $\quad x_i \cdot x_i' = 0$ $\forall i$ $1 \le i \le n$

  ↑ βαθμωτό γινόμενο πχ $110 \cdot 101 = 11+10+01 = 1$

  Ισχύει ότι αν $C = \langle S \rangle$ τότε $C^{\perp} = S^{\perp}$

  ↓ δυϊκός κώδικας του C

- Γραμμικά Ανεξάρτητες Κωδικολέξεις σελ. 133

  $\{z_1, z_2, \dots, z_k\}$: Δεν υπάρχουν $\alpha_1, \dots, \alpha_k$ με 1 τουλάχιστον $\alpha_j \neq 0$

  ώστε $\alpha_1 z_1 + \alpha_2 z_2 + \dots + \alpha_k z_k = 0$

Αν η παραπάνω συνθήκη ισχύει (υπάρχουν $\alpha_1, \dots, \alpha_k$) τότε τα $z_1, \dots, z_k$ είναι Γραμμ. Εξαρτημένα

- Αν το σύνολο $\{z_1, .., z_k\}$ περιέχει το **0** είναι γραμμικά εξαρτημένο
- Κάθε σύνολο $S \neq \{0\}$ περιέχει ένα μέγιστης διάστασης γραμμικά ανεξάρτητο υποσύνολο.
- Β βάση του κώδικα V αν $V = \langle B \rangle$ και B γραμμικά ανεξάρτητη (σελ. 133)

Αν $S = \{0\}$ τότε βάση $= \{\}$

Για κώδικα $C = \langle S \rangle$ με n κωδικολέξεις μήκους η

υπάρχει πίνακας διαστάσεων $k \times n$ (γεννήτορας πίνακας)

για την κωδικοποίηση των μηνυμάτων μήκους k bits.

$$(\text{Μήνυμα } k \text{ bits}) \times G_{k \times n} \longrightarrow \text{κωδική λέξη μήκους } n$$

π.χ.

$$G = \left[\begin{array}{ccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \begin{array}{l} \} k=4 \text{ γραμμές} \\ \quad (\Rightarrow \text{μήκος μηνύματος} \\ \quad\quad " \quad 4 \text{ bits}) \end{array}$$

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{n=7 \text{ στήλες} \Rightarrow (\text{μήκος κωδικολέξης} = 7 \text{ bits})}$

έστω το μήνυμα 0101

Κωδικοποίηση

$$0101 \times G = (0 \times 1000111) + (1 \times 0100110) + (0 \times 0010101) +$$

$$+ (1 \times 0001011) = \overbrace{0101}^{D}\overbrace{101}^{R} \quad \text{(προσθέσαμε την 2η και 4η γραμμή του } G\text{)}$$

Κωδικολέξη

Αποκωδικοποίηση

Έλεγχος ισοτιμίας (αν η κωδικολέξη ανήκει στο C)

Υπάρχει πίνακας H διαστάσεων $n \times (n-k)$ (πίνακας ισοτιμίας) για την αποκωδικοποίηση των κωδικολέξεων μήκους n bits

Ισχύει ότι $x \cdot H = 0$ αν $x \in C$

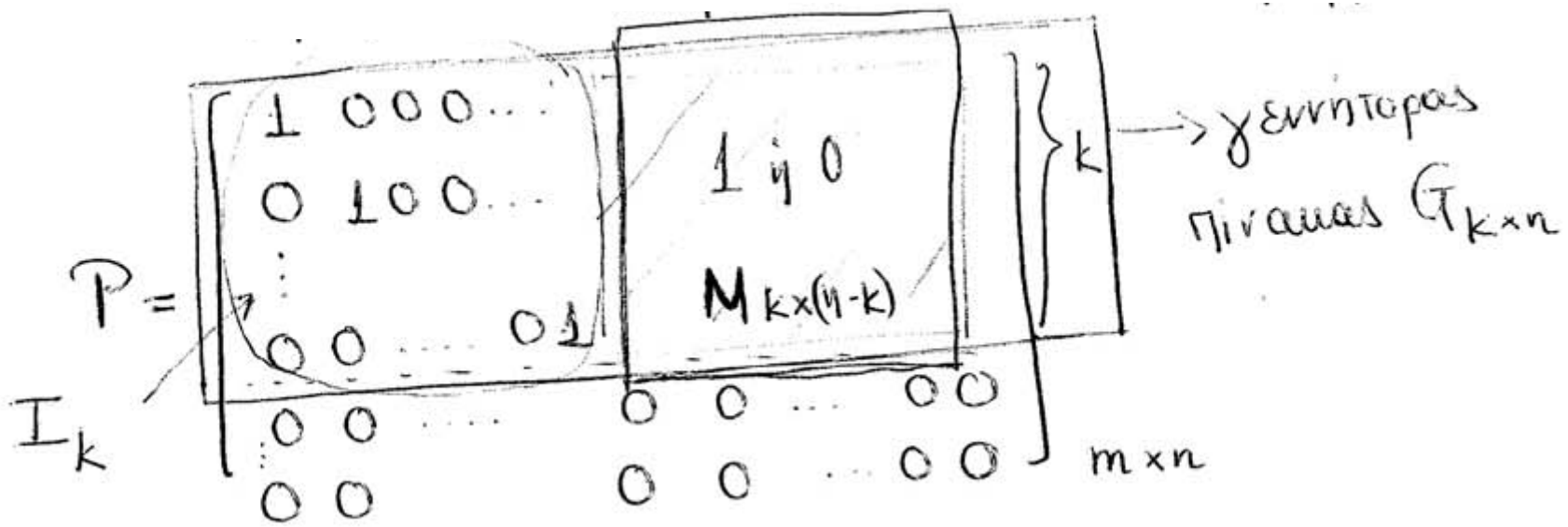
Σύνδρομο, βοηθάει στην ανίχνευση
Και πιθανόν στη διόρθωση σφαλμάτων

Εύρεση πινάκων G, H

Δίνεται κώδικας $\mathcal{C}$ ή υποσύνολο του S τ.ω. $\mathcal{C}=\langle S \rangle$.
με m κωδικές λέξεις $\{s_1, s_2, \ldots, s_m\}$ μήκους n

Σχηματίζουμε τον πίνακα $P=\begin{bmatrix} s_1 \\ s_2 \\ s_m \end{bmatrix}$ μεγέθους $m \times n$

Με αντιμετάθεση γραμμών/αντιμετάθεση γραμμής από το άθροισμά της με 1 άλλη μετασχηματίζουμε τον P σε μορφή Περιορισμένης Κλιμακωτής Διάταξης Γραμμών.



οι γραμμές του $G_{k\times n}$ είναι βάση του C

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

βάση του $C^{\perp}$: οι στήλες του H

ΓΕΣ 2003-04 Θ.6

Δίνεται το $S = \{1100011, 1010000, 1001011, 0100101, 0001101\}$

και ο κώδικας $C_4 = \langle S \rangle$ [όλοι οι γραμμικοί συνδυασμοί των S] Γραικάων

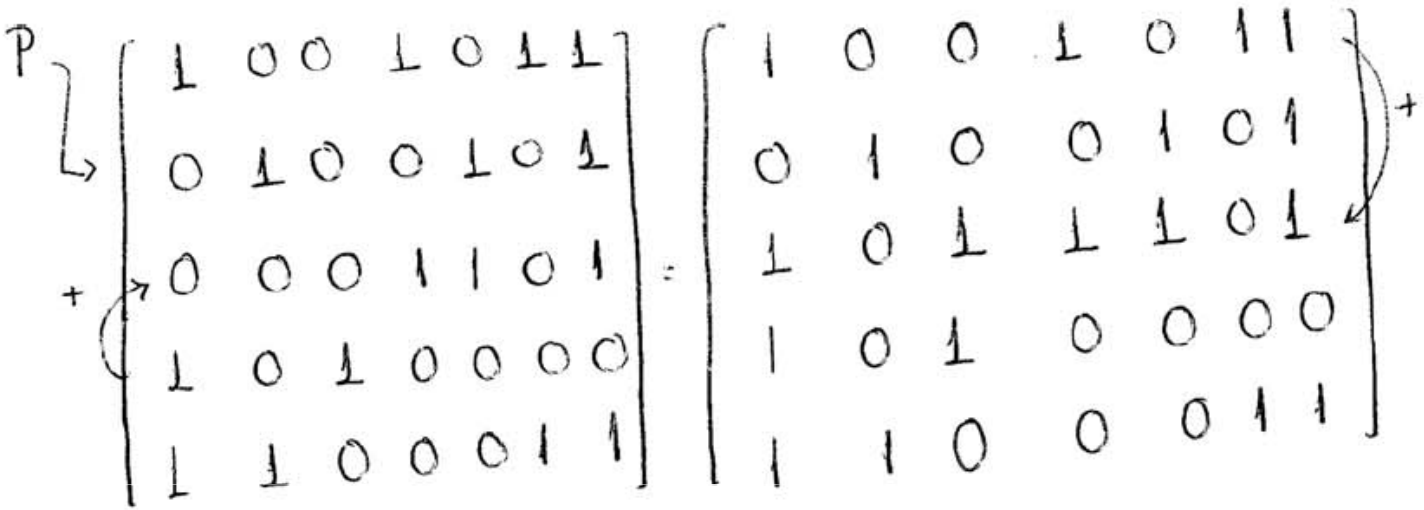
Γεννήτορας πίνακας = ?

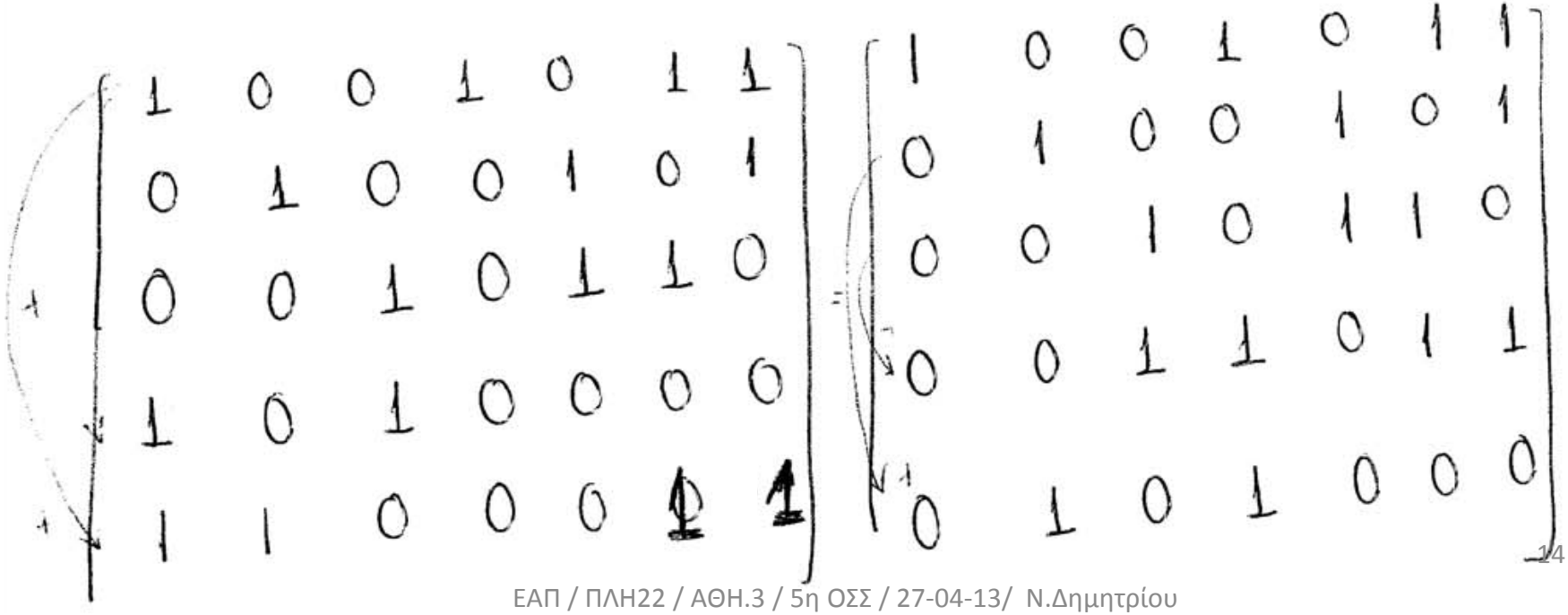
Σελ. 134-136.

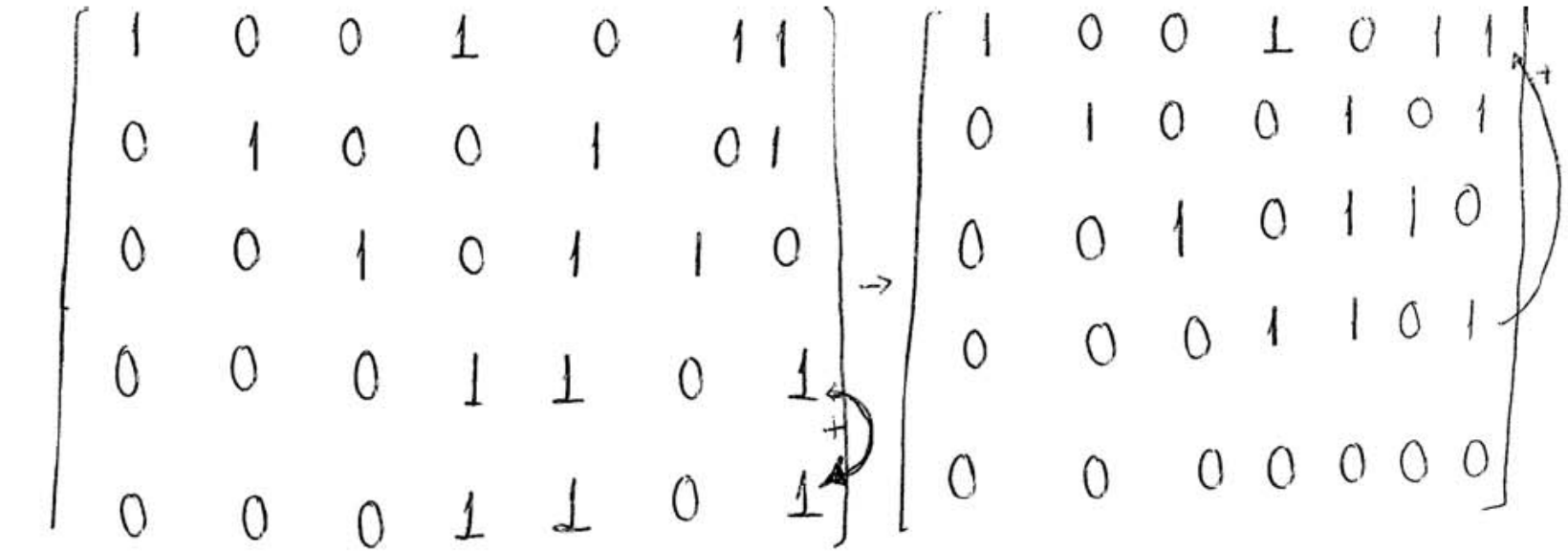
$$P = \begin{bmatrix} 1\,1\,0\,0\,0\,1\,1 & 5 \\ 1\,0\,1\,0\,0\,0\,0 & 4 \\ 1\,0\,0\,1\,0\,1\,1 & 1 \\ 0\,1\,0\,0\,1\,0\,1 & 2 \\ 0\,0\,0\,1\,1\,0\,1 & 3 \end{bmatrix}$$

Μορφή ΠΚΔΓ : Περιορισμένη κλιμακωτή Διάταξη Γραμμών

- Αντιμετάθεση γραμμών
- Αντικατάσταση γραμμής με το άθροισμά της με μια άλλη







$$\Rightarrow G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right] = [I_4 \mid M]$$

$$\mathcal{C}(n, k, d) \longrightarrow n = 7, \quad k = 4$$

- n: αριθμός bits κωδικολέξεων
- k: διάσταση διανυσματικού χώρου / αριθμός bits μηνυμάτων
- d: απόσταση κώδικα

Εύρεση Απόστασης

1) Αν γνωρίζουμε τον κώδικα (Προσοχή! το αναπτύγμα $G<S>$ δηλ όλες τις κωδικολέξεις)

τότε $d = \min[wt(X_i)]$ $X_i \in C$

2) Αν γνωρίζουμε τον S α) είτε υπολογίζουμε το $C = <S>$ (με όλα τα δυνατά αθροίσματα των λέξεων του S)

β) είτε υπολογίζουμε την απόσταση από τη βάση-πίνακα G ή τον πίνακα H

$$H = \begin{bmatrix} M \\ \hline I_3 \end{bmatrix} = \left[\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$$

$d = 2$

Ο κώδικας είναι απόστασης d αν κάθε υποσύνολο $d-1$ γραμμοανεξάρτητη γραμμ. ανεξάρτητο και υπάρχει ένα τουλάχιστον υποσύνολο d γραμμών γραμμ. εξαρτημένο (με μηδενικό άθροισμα)

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

Αθροίζοντας 2 στοιχεία της βάσης, η κωδική λέξη που παράγεται έχει απόσταση τουλάχιστον 2. (λόγω του μοναδιαίου πίνακα). Αν υπάρχουν 2 όμοια στοιχεία του M, η απόσταση του κώδικα είναι ίση με 2.

βαση του $C^{\perp}$: οι στηλες του $H = \{1111100, 1010010, 0101001\}$ *

Κωδικοποίηση μηνυμάτων $A = 0011$ $B = 1001$

$u_A = A \cdot G = 0011 \cdot G = 0011011$ (αθροισμα 3ης & 4ης γραμμης G)

$u_B = B \cdot G = 1001 \cdot G = 1001011$ (-"- 1ης & 4ης -"- G)

Η κωδική λέξη 1101110 αναλύεται ως → data $\overbrace{1101}^{k}$ (4 bits)
→ parity $\underbrace{110}_{n-k}$ (3 bits)

Το πλήθος των συνομάδων του $\mathcal{C}$ είναι $2^{n-k} = 2^{7-4} = 2^3 = 8$

Η συνομάδα $\mathcal{C} + 1111011$ θα βρεθεί αφού πρώτα προσδιοριστεί το αναπτύγμα του κώδικα (είτε από τη βάση είτε από το S)

Τότε προσθέτουμε σε κάθε κωδικολέξη την 1111011 και λαμβάνουμε τη συνομάδα $C + 1111011$

Αποκωδικοποίηση με βοήθεια συνοράδων.

1. Λήψη λέξης y

Υπολογισμός της συνοράδας $C+y \rightarrow$ (δυνατά πρότυπα σφάλματος για τη λέξη y)

Αν $y \in C$, τότε $C+y \rightarrow \{0, \dots\}$

Αν $y \notin C$, τότε $C+y \Rightarrow \{\varepsilon_1, \varepsilon_2, \dots\}$

ο δέκτης επιλέγει το πρότυπο σφάλματος με το μικρότερο βάρος. Αν υπάρχουν περισσότερα του 1 πρότυπα ελαχίστου βάρους τότε:

α. ΠΑΜΠ : επιλέγουμε ένα τυχαία / αυθαίρετα

β. ΑΑΜΠ : ο δέκτης ζητάει επανεκπομπή.

Η λέξη που έχει μεταδοθεί είναι η $x = y + \varepsilon$

Για μεγάλο αριθμό πιθανών λέξεων η παραπάνω διαδικασία είναι πολύπλοκη, οπότε χρησιμοποιείται η μέθοδος με τον πίνακα ελέγχου ισοτιμίας και την τυπική Διάταξη Αποκωδικοποίησης.

Παράδειγμα 4.20

$C = \{0000, 1010, 1101, 0111\}$

Απόσταση κώδικα: $d = \min\{wt(x_i)\} = 2$.

Ικανότητα διόρθωσης $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$ σφαλμάτων.

Εύρεση ΠΚΔΓ:

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

$$\rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \rightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$ ΠΚΔΓ

Αρα, $G = \left[\begin{array}{cc:cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{array}\right]$

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

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

Κατασκευάζουμε τον εξής πίνακα:

Οδηγός Συνδράδας (Λοιμφάζουμε πρότυπα ελαχίστου βάρους)

μήκους $n = 4$ bits	γ. Η ($n-k$ bits)
0 0 0 0	0 0
0 0 0 1	0 1
0 0 1 0	1 0
0 1 0 0	1 1
1 0 0 0	1 0

Τα σύνδρομα συμπτώσεων

Στην ΠΑΜΠ επιλέγουμε έναν από τους 2 οδηγούς

Στην ΑΑΜΠ αφήνουμε τη θέση του οδηγού μονή

Άρα, για ΠΑΜΠ

οδηγός Συνοριάδας	y H
0 0 0 0	0 0
0 0 0 1	0 1
0 0 1 0	1 0
0 1 0 0	1 1

για ΑΑΜΠ

οδηγός Συνοριάδας	y H
0 0 0 0	0 0
0 0 0 1	0 1
~~0 0 1 0~~	1 0
0 1 0 0	1 1

Προσοχή! Αν είχαμε δυνατότητα διόρθωσης ενός σφάλματος, τότε οι πίνακες ΠΑΜΠ & ΑΑΜΠ συμπίπτουν