ΘΕΩΡΙΑ ΠΛΗΡΟΦΟΡΙΑΣ

Κεφάλαιο 10 : Κωδικοποίηση καναλιού

Πανεπιστήμιο Αιγαίου, Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Περιεχόμενα Ομιλίας

- Απόσταση και βάρος Hamming
- Τεχνικές και κώδικες ανίχνευσης & διόρθωσης σφαλμάτων
- Γραμμικοί κώδικες
- Κώδικες δομής (block)
- Κώδικες Hamming
- Κώδικες LDPC
- Κυκλικοί κώδικες
- Κώδικες BCH
- Συνελικτικοί κώδικες
- Κώδικες Turbo

Τί είναι ο κώδικας καναλιού;

- Κώδικας καναλιού είναι κάθε μέθοδος κωδικοποίησης ψηφιακής πληροφορίας που διευκολύνει τη μετάδοσή της από αναλογικά και ψηφιακά μέσα μετάδοσης.
- Εισάγεται πλεονάζουσα πληροφορία με ελεγχόμενο και συστηματικό τρόπο.
- Τα bits αυτά δε μεταφέρουν πληροφορία , αλλά δίνουν τη δυνατότητα στον αποκωδικοποιητή να ανιχνεύει ή και να διορθώνει λάθη.

Γιατί χρειαζόμαστε την κωδικοποίηση καναλιού;

- Αφαίρεση από το αποστελλόμενο σήμα συνεχούς συνιστώσας τάσης, λόγω αδυναμίας μετάδοσής της.
- Ενημέρωση δέκτη για τη χρονική στιγμή που ξεκινά η μετάδοση και τη διάρκειά της.
- Βέλτιστη χρήση του εύρους ζώνης του συγκεκριμένου καναλιού επικοινωνίας.
- Ανάγκη τρόπου εντοπισμού και διόρθωσης λαθών κατά τη μετάδοση της πληροφορίας.
- Ανάγκη μείωση παραμόρφωσης.
- Μείωση πιθανότητας παρουσίασης διαφωνίας (crosstalk).

Βασικές Έννοιες

Αξιοπιστία καναλιού

- Είναι ο πραγματικός αριθμός με $0 \leq p \leq 1$

όπου *p* είναι η πιθανότητα της ορθής μεταφοράς ενός δυαδικού ψηφίου μέσω του καναλιού.

- Ένα κανάλι χαρακτηρίζεται πιο αξιόπιστο από ένα άλλο αν η πιθανότητα *p*, δηλαδή η αξιοπιστία του, είναι πιο υψηλή.

Ρυθμός πληροφορίας

- Είναι το ποσοστό της κωδικής λέξης που μεταφέρει το μήνυμα.
- Ο ρυθμός πληροφορίας ενός δυαδικού κώδικα *C* μήκους *n* είναι :

και παίρνει τιμές από 0 ως 1. $R = \frac{\log_2 |C|}{n}$

Απόσταση και Βάρος

Βάρος Hamming

Το **βάρος Hamming** μιας λέξης μήκους n ψηφίων είναι το πλήθος των ψηφίων της λέξης που είναι ίσα με «1».

Απόσταση Hamming

Η **απόσταση Hamming** μεταξύ δύο λέξεων και του ίδιου μήκους είναι το πλήθος των θέσεων στις οποίες οι δύο λέξεις εμφανίζουν ασυμφωνία του δυαδικού ψηφίου.

- Για παράδειγμα, οι κωδικές λέξεις 11000010 και 10010010 έχουν απόσταση Hamming 2,

Απόσταση Hamming

- Η ελάχιστη απόσταση Hamming μεταξύ των «λέξεων» του αποτελεί χαρακτηριστικό του (απόσταση Hamming του κώδικα)

Έστω d_{ham} η απόσταση Hamming ενός κώδικα

- Ικανότητα ανίχνευσης σφαλμάτων:

$$d_{ham} - 1$$

- Ικανότητα διόρθωσης σφαλμάτων:

$$\left\lfloor \frac{d_{ham} - 1}{2} \right\rfloor$$

Τεχνικές και κώδικες ανίχνευσης & διόρθωσης σφαλμάτων

- Automatic Repeat Request (ARQ)
  - Ο δέκτης εκτελεί ανίχνευση των σφαλμάτων και ζητά από τον πομπό επανεκπομπή των δεδομένων
  - Αυξημένη πολυπλοκότητα, αφού απαιτεί την ύπαρξη ενός καναλιού ανάδρασης, που δεν είναι πάντα διαθέσιμο, καθιστώντας την έτσι μη πρακτική για αρκετές εφαρμογές.
- Forward Error Correction (FEC)
  - Ο δέκτης σε περίπτωση ανίχνευσης σφάλματος προβαίνει και στη διόρθωσή του ακολουθώντας τους κανόνες κωδικοποίησης.
  - Η τεχνική αυτή, αν και δυσκολότερη στην εφαρμογή από την ARQ, δεν απαιτεί δίαυλο ανάδρασης.

Κώδικας ελέγχου απλής ισοτιμίας

- Ο απλούστερος κώδικας ανίχνευσης σφάλματος είναι ο κώδικας ελέγχου απλής ισοτιμίας (simple parity check code), C(n, n-1, 2), q=2.
- Ένα bit ισοτιμίας προστίθεται στο μήνυμα.
- Αυτός ο κώδικας είναι ικανός να ανιχνεύει ένα μεμονωμένο σφάλμα.
- Για παράδειγμα ο κώδικας

C={0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111},

έχει παραμέτρους C(4,3,2).

Κώδικας απλής επανάληψης

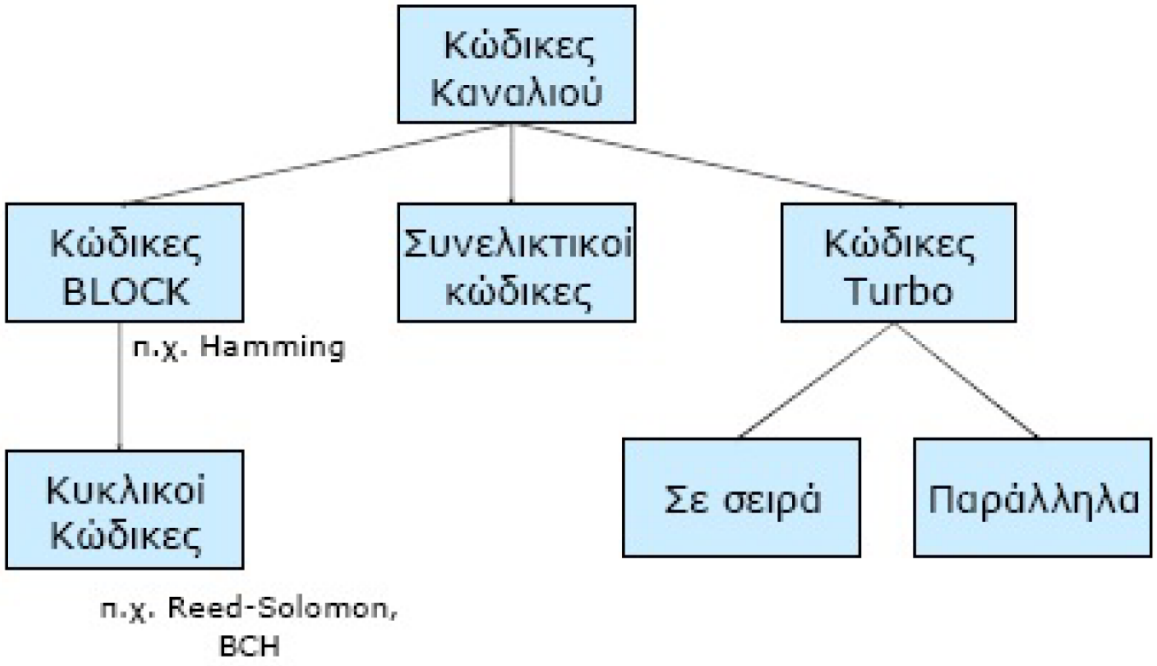
- Ο απλούστερος κώδικας διόρθωσης σφάλματος είναι ο κώδικας απλής επανάληψης (simple repetition code), C(n, 1, n), q=2.
- Αυτός ο κώδικας αποτελείται από δύο μόνο κωδικές λέξεις, η μια με όλα τα ψηφία της 0 και η άλλη με όλα 1.
- Το μήνυμα είναι ίσο με ένα bit, αν είναι 0 τότε μεταδίδεται η κωδική λέξη που αποτελείται μόνο από μηδενικά.
- Για παράδειγμα ο κώδικας C={00000, 11111} έχει παραμέτρους C(5,1,5) και μπορεί να διορθώσει 2 σφάλματα ή να ανιχνεύσει 4.
- Ο ρυθμός του είναι χαμηλός: R=1/5.

Δι-διάστατο parity ή Ορθογώνιοι κώδικες

1	0	0	1	1	1	0	0
0	0	0	1	1	1	1	0
0	0	1	1	0	0	1	1
1	0	0	1	0	0	1	1
0	1	1	1	1	1	0	1
1	0	1	0	1	1	1	1
0	0	1	1	0	0	1	1
1	1	0	0	0	0	1	1

- Τα σύμβολα του μηνύματος είναι τα μη χρωματισμένα και σχηματίζουν ορθογώνιο.
- Τα χρωματισμένα με γκρι bits στην αριστερή στήλη είναι bits ισοτιμίας ορισμένα με τέτοιο τρόπο ώστε το άθροισμα της αντίστοιχης γραμμής να έχει άρτια ισοτιμία.
- Ομοίως, τα χρωματισμένα με γκρι bits στην τελευταία γραμμή είναι ορισμένα με τέτοιο τρόπο ώστε το άθροισμα κάθε στήλης να έχει άρτια ισοτιμία.
- Ο ορθογώνιος κώδικας μπορεί να διορθώσει ένα λάθος οπουδήποτε κι αν εμφανιστεί στον πίνακα.

Κατηγορίες κωδίκων καναλιού



Γραμμικοί κώδικες

- Όλοι οι κώδικες στους οποίους αναφερόμαστε είναι δυαδικοί.

$$F = GF(2) = \{0,1\}$$

- Τα στοιχεία του *F* καλούνται bits.
- Το *F* δηλώνει το διάνυσμα των n-διαστάσεων που αποτελείται από όλα τα δυαδικά διανύσματα μήκους n
- Οι κώδικες με κώδικές λέξεις m που έχουν το ίδιο μήκος κωδικής λέξης n λέγονται ομοιόμορφοι δυαδικοί κώδικες (uniform binary codes).
- Αυτοί είναι κατά κανόνα γραμμικοί κώδικες εκτός αν ορίζονται διαφορετικά.
- Ένας γραμμικός κώδικας C είναι ένα γραμμικό υποσύνολο του *F* και έχει ίσα ψηφία ίσα με n.
- Ισοδύναμα, ένας (δυαδικός) κώδικας είναι γραμμικός αν το άθροισμα των οποιωνδήποτε κωδικών λέξεων είναι επίσης μια κωδική λέξη.

Γραμμικοί Κώδικες

- Ένας (n, M, d) κώδικας
  - Μια ομάδα από M δυαδικά διανύσματα (κωδικές λέξεις)
  - Μήκους n
  - Όπου κάθε δύο κωδικές λέξεις διαφέρουν κατά d θέσεις
- Στους μπλόκ κώδικες
  - Ένα μπλόκ από k bits πληροφορίας ακολουθείται από c bits ψηφία ισοτιμίας

Γραμμικοί Κώδικες

- Παράδειγμα
- 0 0 0 0 0
- 1 1 1 1 1
- Ο παραπάνω είναι ένας (5, 2, 5) γραμμικός κώδικας όπου
- n = 5 μήκος λέξης
- M = 2 αριθμός λέξεων στον κώδικα
- d = 5 απόσταση

Γραμμικοί Κώδικες

- Παράδειγμα
- 0 0 0 0 0
- 1 1 1 1 1
- 1+4 = 5
- k + c = n = 5 σύμβολα ψηφία
- k|c Block κώδικας (χωριστά τα k με τα c σύμβολα)

Απόδοση $R = \frac{\log_2}{n} = \frac{1}{5} = 0.2$

Γραμμικοί Κώδικες

- Παράδειγμα
- 0 0 0
- 0 1 1
- 1 0 1
- 1 1 0

- Παράδειγμα

0 0 0 0 0 0 0

1 1 1 0 1 0 0

0 1 1 1 0 1 0

0 0 1 1 1 0 1

1 0 0 1 1 1 0

0 1 0 0 1 1 1

1 0 1 0 0 1 1

1 1 0 1 0 0 1

Γραμμικοί Κώδικες

- Παράδειγμα

0 0 0 0 0 0 0 0	1 1 1 1 1 1 1 1
1 1 0 0 0 0 0 0	0 0 1 1 1 1 1 1
1 0 1 0 0 0 0 0	0 1 0 1 1 1 1 1
1 0 0 1 0 0 0 0	0 1 1 0 1 1 1 1
1 0 0 0 1 0 0 0	0 1 1 1 0 1 1 1
1 0 0 0 0 1 0 0	0 1 1 1 1 0 1 1
1 0 0 0 0 0 1 0	0 1 1 1 1 1 0 1
1 0 0 0 0 0 0 1	0 1 1 1 1 1 1 0

Γραμμικοί κώδικες

- Παράδειγμα

0 0 0 0 0 0 0 0	1 1 1 1 1 1 1 1
1 1 0 0 0 0 0 0	0 0 1 1 1 1 1 1
1 0 1 0 0 0 0 0	0 1 0 1 1 1 1 1
1 0 0 1 0 0 0 0	0 1 1 0 1 1 1 1
1 0 0 0 1 0 0 0	0 1 1 1 0 1 1 1
1 0 0 0 0 1 0 0	0 1 1 1 1 0 1 1
1 0 0 0 0 0 1 0	0 1 1 1 1 1 0 1
1 0 0 0 0 0 0 1	0 1 1 1 1 1 1 0

- Είναι ένας (8, 16, 2) όχι και τόσο καλός κώδικας
- Η μία λέξη προστιθέμενη στην άλλη δεν δίνει μία τρίτη λέξη, δηλαδή δεν είναι κυκλικός κώδικας.
- Έτσι, αυτός ο κώδικας δεν είναι γραμμικός.

Γεννήτορας πίνακας κώδικα

- Αν πάρουμε ένα μέγιστο σύνολο από γραμμικά ανεξάρτητες κωδικές λέξεις από τον C, $x^{(1)}, \ldots, x^{(k)}$
- Τότε ο C εμπεριέχει όλους τους γραμμικούς συνδυασμούς:

$$a_1 X^{(1)} + a_k X^{(k)}, a_1 \in F$$

- Ο $k \times n$ δυαδικός πίνακας

$$G = \begin{bmatrix} x^{(1)} \\ \vdots \\ x^{(k)} \end{bmatrix}$$

καλείται γεννητριακή (generator) μήτρα ή γεννήτορας πίνακας του κώδικα.

Ο κώδικας είναι ο γραμμικός χώρος του G.

Κώδικες block

- Οι κώδικες block καθορίζονται από 3 βασικές παραμέτρους:
  - Το μήκος της ομάδας
  - Το μήκος του μηνύματος *k*
  - Την ελάχιστη απόσταση κώδικα d_{min} και συμβολίζονται ως
    - $C(n,k,d_{min})$.
  - Block *k bits* πληροφορίας αντιστοιχούνται σε *n bits (n>k)* και παρακάτω ορίζεται ο ρυθμός R του κώδικα.

$$R = \frac{k}{n} \qquad 0 \leq R \leq 1$$

  - Το μέγεθος πλεονάζουσας πληροφορίας μετράται από το λόγο n/k.

Κώδικες block

- Ένας κώδικας μπλοκ παράγεται από ένα σύνολο k γραμμικώς ανεξάρτητων n-διάστατων διανυσμάτων $g_0, g_1, \ldots, g_{k-1}$
- Οι κωδικές λέξεις αποτελούν γραμμικό συνδυασμό αυτών των διανυσμάτων. Συνεπώς, η κωδική λέξη ενός μηνύματος μπορεί να αναπαρασταθεί με τη μορφή :

$$c = (c_0, c_1, \ldots, c_{k-1}) \qquad v = c_0 \cdot g_0 + c_1 \cdot g_1 + \ldots + c_{k-1} \cdot g_{k-1}$$

- Τα διανύσματα αποτελούν τις γραμμές του γεννήτορα πίνακα

$$G = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & \cdots & g_{0,k-1} \\ g_{10} & g_{11} & \cdots & g_{1,k-1} \\ g_{20} & g_{21} & \cdots & g_{2,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix}$$

- Έτσι, η κωδική λέξη v για το μήνυμα c γράφεται $v = c \cdot G = c_0 \cdot g_0 + c_1 \cdot g_1 + \ldots + c_{k-1} \cdot g_{k-1}$
- Με το γεννήτορα πίνακα είμαστε σε θέση να υπολογίσουμε τις διακριτές κωδικές λέξεις που αντιστοιχούν σε όλες τις δυνατές ακολουθίες «0» και «1» ενός μπλοκ

Γραμμικοί μπλοκ κώδικες

- Στους κώδικες μπλοκ (*block code*) για κάθε k bit μιας λέξης δεδομένων που εισάγεται στον κωδικοποιητή, εξάγεται μία κωδικολέξη μήκους n bit

- Οι κώδικες μπλοκ, των οποίων οι λέξεις δεδομένων τοποθετούνται στην αρχή (ή στο τέλος) των κωδικολέξεων αναλλοίωτες, ονομάζονται συστηματικοί (*systematic*)
- Ένας κώδικας μπλοκ ονομάζεται γραμμικός (*linear*) όταν το αποτέλεσμα της πρόσθεσης, με αριθμητική modulo-2, οποιονδήποτε δύο κωδικολέξεων είναι μια άλλη κωδικολέξη του κώδικα

Γραμμικοί μπλοκ κώδικες (κωδικοποίηση)

- Έστω $\mathbf{d} = [d1, d2, \ldots, dk]$ παριστάνει το διάνυσμα της λέξης δεδομένων και $\mathbf{c} = [c1, c2, \ldots, cn]$ παριστάνει το διάνυσμα της αντίστοιχης κωδικολέξης
- Ένας συστηματικός γραμμικός κώδικας μπλοκ γράφεται

$$
\begin{aligned}
c_1 &= d_1 \\
c_2 &= d_2 \\
&\vdots \\
c_k &= d_k
\end{aligned}
$$

k Bit
Λέξη Δεδομένων

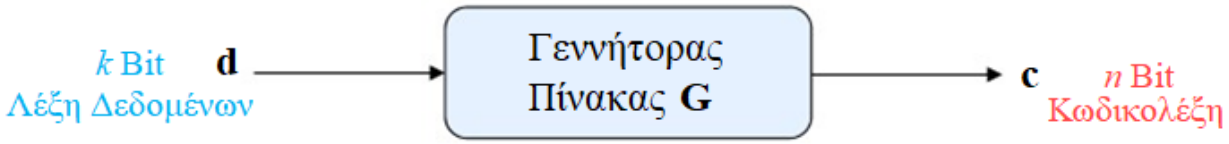
$$
\begin{aligned}
c_{k+1} &= p_{11}\, d_1 \oplus p_{12}\, d_2 \oplus \cdots \oplus p_{1k}\, d_k \\
c_{k+2} &= p_{21}\, d_1 \oplus p_{22}\, d_2 \oplus \cdots \oplus p_{2k}\, d_k \\
&\vdots \\
c_n &= p_{m1}\, d_1 \oplus p_{m2}\, d_2 \oplus \cdots \oplus p_{mk}\, d_k
\end{aligned}
$$

m = n - k
Bit Ελέγχου

Γραμμικοί μπλοκ κώδικες (κωδικοποίηση)

- Κάθε κωδικολέξη ενός συστηματικού γραμμικού κώδικα μπλοκ σχηματίζεται βάσει του γεννήτορα πίνακα (generator matrix) **G** ως εξής

$$\mathbf{c} = \mathbf{d}\,\mathbf{G}$$



- Ο γεννήτορας πίνακας είναι διάστασης $k \times n$ έχει την εξής δομή

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & \cdots & 0 & p_{11} & p_{21} & \cdots & p_{m1} \\ 0 & 1 & \cdots & 0 & p_{12} & p_{22} & \cdots & p_{m2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & p_{1k} & p_{2k} & \cdots & p_{mk} \end{bmatrix} = [\mathbf{I}_k\ \mathbf{P}]$$

- Ο **P** είναι ο πίνακας συντελεστών με τιμές $\{0, 1\}$

Γραμμικοί μπλοκ κώδικες (κωδικοποίηση)

- Δηλαδή, κάθε το διάνυσμα κάθε κωδικολέξης γράφεται ως συνδυασμός του διανύσματος της λέξης δεδομένων και του διανύσματος των bit ελέγχου

$$\mathbf{c} = \mathbf{d}\,\mathbf{G} \Leftrightarrow \mathbf{c} = \mathbf{d}\,[\mathbf{I}_k \;\; \mathbf{P}] \Leftrightarrow \mathbf{c} = [\mathbf{d} \;\; \mathbf{d}\,\mathbf{P}] \Leftrightarrow \mathbf{c} = [\mathbf{d} \;\; \mathbf{c}_p]$$

- Δεδομένου της γραμμικότητας του κώδικα, από την πρόσθεση, με αριθμητική modulo-2, οποιονδήποτε δύο κωδικολέξεων προκύπτει μια έγκυρη κωδικολέξη του κώδικα
- Η ελάχιστη απόσταση Hamming ενός γραμμικού κώδικα μπλοκ προκύπτει αφού υπολογιστούν οι αποστάσεις Hamming μεταξύ όλων των κωδικολέξεων του κώδικα
- Συνεπώς, η ελάχιστη απόσταση Hamming ενός γραμμικού κώδικα μπλοκ προκύπτει από την κωδικολέξη με το ελάχιστο βάρος Hamming (πλην της κωδικολέξης του μηδενικού διανύσματος)

Παράδειγμα

- Παράδειγμα: Έστω ο γεννήτορας πίνακας ενός κώδικα μπλοκ

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

- Η διάσταση του πίνακα **G** είναι k×n = 3×6, δηλαδή ο κώδικάς μπλοκ είναι ο (n, k) = (6, 3)
- Ο κώδικας ικανοποιεί το όριο Hamming αφού

$$n \leq 2^m - 1 \Leftrightarrow 6 \leq 2^3 - 1 = 7$$

- Με πολλαπλασιασμό της κάθε λέξης δεδομένων **d** με τον **G** προκύπτουν οι αντίστοιχες κωδικολέξεις **c**
- Παρατηρούμε ότι ο κώδικας μπλοκ είναι συστηματικός, αφού τα 3 πρώτα bit της κάθε κωδικολέξης είναι η λέξη δεδομένων

Λέξη Δεδομένων	
000	000000
001	001110
010	010011
011	011101
100	100101
101	101011
110	110110
111	111000

Παράδειγμα

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

- Επιπλέον, παρατηρούμε ότι ο κώδικας μπλοκ είναι γραμμικός, αφού κάθε αποτέλεσμα πρόσθεσης 2 οποιονδήποτε κωδικολέξεων παράγει μία από τις κωδικολέξεις του κώδικα, πχ `001110` ⊕ `010011` = `011101`, `001110` ⊕ `101011` = `100101`

Λέξη Δεδομένων	
000	000000
001	001110
010	010011
011	011101
100	100101
101	101011
110	110110
111	111000

- Εφόσον ο κώδικας μπλοκ είναι γραμμικός, για να βρούμε την ελάχιστη απόσταση Hamming, αρκεί να βρούμε την κωδικολέξη με το ελάχιστο βάρος και αυτό είναι $d_{min} = 3$
- Άρα, ο κώδικας (6, 3) μπορεί να διορθώσει έως 1 λάθος

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = 1$$

- Επίσης, ο συγκεκριμένος (6, 3) μπορεί να ανιχνεύσει έως 2 λάθη

$$t' = d_{\min} - 1 = 2$$

Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

- Ας ορίσουμε τον πίνακα

$$\mathbf{H} = \underbrace{\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1k} \\ p_{21} & p_{22} & \cdots & p_{2k} \\ \vdots & \vdots & \cdots & \vdots \\ p_{m1} & p_{m2} & \cdots & p_{mk} \end{bmatrix}}_{\mathbf{P}^{\mathsf{T}}\ (m \times k)} \underbrace{\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}}_{\mathbf{I}_m\ (m \times m)} = [\mathbf{P}^{\mathsf{T}}\ \mathbf{I}_m]$$

- Υπολογίζοντας το γινόμενο $\mathbf{HG}^{\mathsf{T}}$ προκύπτει η παρακάτω ιδιότητα

$$\mathbf{H}\,\mathbf{G}^{\mathsf{T}} = [\mathbf{P}^{\mathsf{T}}\ \mathbf{I}_m]\,[\mathbf{I}_k\ \mathbf{P}]^{\mathsf{T}} = [\mathbf{P}^{\mathsf{T}}\ \mathbf{I}_m] \begin{bmatrix} \mathbf{I}_k \\ \mathbf{P}^{\mathsf{T}} \end{bmatrix} = \mathbf{P}^{\mathsf{T}}\,\mathbf{I}_k \oplus \mathbf{I}_m\,\mathbf{P}^{\mathsf{T}} = \mathbf{P}^{\mathsf{T}} + \mathbf{P}^{\mathsf{T}} = \mathbf{0}$$

- Ισοδύναμα, εφαρμόζοντας και στα δύο μέλη τον ανάστροφο πίνακα επιπλέον προκύπτει

$$\mathbf{H}\,\mathbf{G}^{\mathsf{T}} = \mathbf{0} \Leftrightarrow (\mathbf{H}\,\mathbf{G}^{\mathsf{T}})^{\mathsf{T}} = \mathbf{0}^{\mathsf{T}} \Leftrightarrow (\mathbf{G}^{\mathsf{T}})^{\mathsf{T}}\,\mathbf{H}^{\mathsf{T}} = \mathbf{0} \Leftrightarrow \mathbf{G}\,\mathbf{H}^{\mathsf{T}} = \mathbf{0}$$

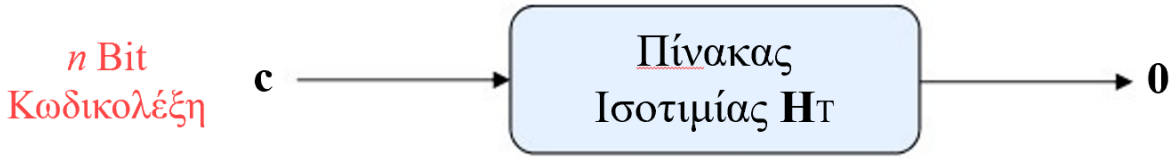
Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

- Αν στην εξίσωση $\mathbf{G}\mathbf{H}^{\mathsf{T}} = \mathbf{0}$ πολλαπλασιάσουμε και τα δύο μέλη με **d** προκύπτει:

$$\mathbf{G}\,\mathbf{H}^{\mathsf{T}} = 0 \Leftrightarrow \underbrace{\mathbf{d}\,\mathbf{G}}_{\mathbf{c}}\,\mathbf{H}^{\mathsf{T}} = \mathbf{d}\,0 \Leftrightarrow \mathbf{c}\,\mathbf{H}^{\mathsf{T}} = 0$$

- Ο πίνακας **H** (διάστασης $m \times n$) ονομάζεται πίνακας ελέγχου ισοτιμίας (*parity check matrix*)

- Η παραπάνω εξίσωση ισχύει για κάθε έγκυρη κωδικολέξη του κώδικα



Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

- Αν **r** είναι η κωδικολέξη που λαμβάνει ο δέκτης, τότε αυτή γράφεται ως αποτέλεσμα άθροισης μεταξύ μιας έγκυρης κωδικολέξης **c** και ενός διανύσματος σφάλματος **e** = [e_1, e_2, …, e_n], δηλαδή

$$\mathbf{r} = \mathbf{c} \oplus \mathbf{e}$$

- Πολλαπλασιάζοντας το **r** με τον $\mathbf{H}^T$ έχουμε το διάνυσμα **s**, το οποίο ονομάζεται σύνδρομο (syndrome) και σχετίζεται με το διάνυσμα σφάλματος ως εξής

$$\mathbf{s} = \mathbf{r}\mathbf{H}^T = [\mathbf{c} \oplus \mathbf{e}]\mathbf{H}^T = \underbrace{\mathbf{c}\mathbf{H}^T}_{\mathbf{0}} \oplus \mathbf{e}\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$$

- Προφανώς, αν δεν έχει συμβεί σφάλμα **e** = **0**, το σύνδρομο είναι το μηδενικό διάνυσμα **s** = **0**

Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

- Η διαδικασία αποκωδικοποίησης μπορεί να γίνει ως εξής:
  - Υπολογισμός συνδρόμου $\mathbf{s} = \mathbf{r}\mathbf{H}^T$
  - Αν $\mathbf{s} = \mathbf{0}$, τότε δεν έχει συμβεί σφάλμα, δηλαδή $\mathbf{c}_i = \mathbf{r}$
  - Αν $\mathbf{s} \neq \mathbf{0}$, τότε έχει συμβεί κάποιο σφάλμα και η έγκυρη κωδικολέξη
    βρίσκεται βάσει της ελάχιστης απόσταση Hamming dmin{**r**, $\mathbf{c}_i$}
- Ο παραπάνω τρόπος αποκωδικοποίησης απαιτεί να υπάρχουν αποθηκευμένες σε μνήμη όλες οι έγκυρες κωδικολέξεις **c**i, ώστε να συγκριθούν με το **r**
- Η απαίτηση σε μνήμη n 2k bit είναι υπερβολικά μεγάλη, ενώ απαιτούνται n πύλες XOR 2 εισόδων, όπου για κάθε **r** που λαμβάνεται θα πρέπει να εκτελέσει 2k λογικές πράξεις

Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

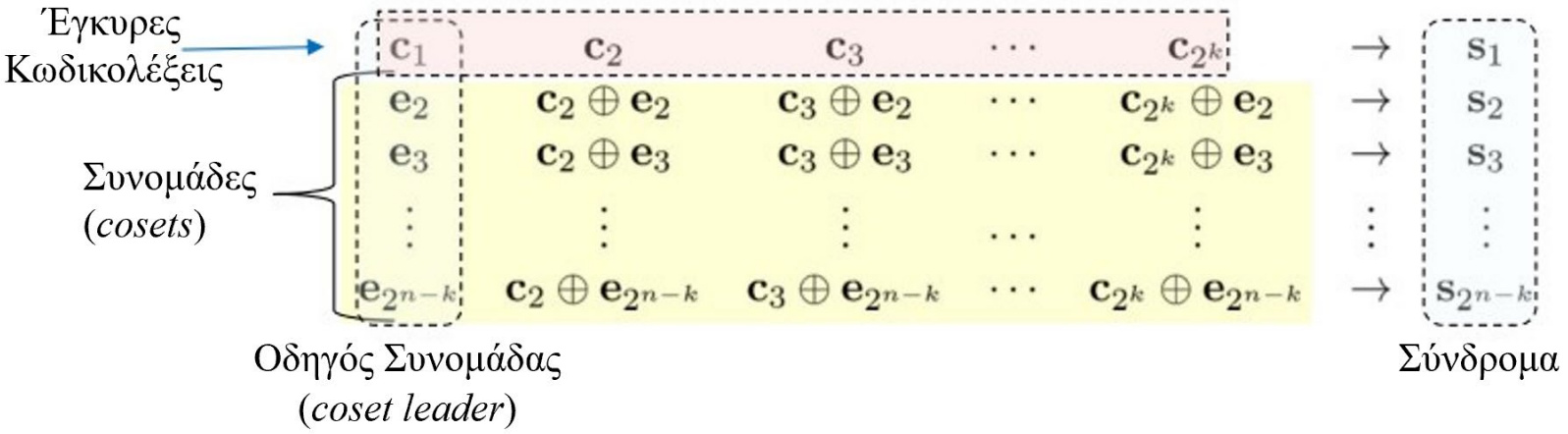
- Πιο αποδοτική είναι η αποκωδικοποίηση με χρήση του πίνακα τυπικής διάταξης (standard array)
- Αναλυτικότερα, η εξίσωση για το σύνδρομο $\mathbf{s} = \mathbf{e}\,\mathbf{H}^{\mathrm{T}} = \mathbf{e}\,[\mathbf{P}^{\mathrm{T}}\ \mathbf{I}_m]^{\mathrm{T}} = \mathbf{e}\left[\left(\mathbf{P}^{\mathrm{T}}\right)^{\mathrm{T}}\ \mathbf{I}_m\right] = \mathbf{e}\left[\mathbf{P}\ \mathbf{I}_m\right]$ γράφεται

$$[s_1, s_2, \ldots, s_m] = [e_1, e_2, \ldots, e_n] \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ p_{k1} & p_{k2} & \cdots & p_{km} \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \} \mathbf{P} \\ \\ \\ \\ \} \mathbf{I}_m \end{matrix}$$

- Πρόκειται για σύστημα m εξισώσεων με n αγνώστους και άρα έχει πολλές λύσεις ως προς **e**
- Ειδικότερα, υπάρχουν 2^{n-k} δυνατές διαφορετικές λύσεις
- Ο πίνακας τυπικής διάταξης ενός κώδικα μπλοκ συνοψίζει σε στήλες ανά έγκυρη κωδικολέξη το σύνολο των μη έγκυρων κωδικολέξεων που ο κώδικας μπορεί να διορθώσει

Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

- Η κάθε γραμμή περιλαμβάνει κωδικολέξεις με το ίδιο σφάλμα και αντιστοιχεί στο ίδιο σύνδρομο, ενώ διαφορετικές γραμμές έχουν διαφορετικά σύνδρομα
- Στην 1η στήλη βρίσκεται η κωδικολέξη $\mathbf{c}_1 = \mathbf{0}$ και οπωσδήποτε $\mathbf{s}_1 = \mathbf{0}$



Γραμμικοί μπλοκ κώδικες (απόκωδικοποίηση)

- Άρα τελικά
  - Υπολογισμός συνδρόμου $\mathbf{s} = \mathbf{r}\mathbf{H}^T$
  - Αν $\mathbf{s} = \mathbf{0}$, τότε δεν έχει συμβεί σφάλμα, δηλαδή $\mathbf{c}_i = \mathbf{r}$
  - Αν $\mathbf{s} \neq \mathbf{0}$, τότε έχει συμβεί κάποιο σφάλμα
  - το σφάλμα προκύπτει από τη γραμμή που αντιστοιχίζει το σύνδρομο με το σφάλμα **e**
  - Η κωδική λέξη υπολογίζεται: $\mathbf{c} = \mathbf{e} \oplus \mathbf{r}$