Τμήμα Μηχανικών Πληροφορικής τ.ε.
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Ελλάδας

Θεωρία Πληροφορίας

Διάλεξη 7: Κωδικοποίηση καναλιού με γραμμικούς κώδικες block

Δρ. Μιχάλης Παρασκευάς
Επίκουρος Καθηγητής

Ατζέντα

- **Τεχνικές Διόρθωσης Λαθών**
  - Κώδικες εντοπισμού λαθών
  - Κώδικες εντοπισμού και διόρθωσης λαθών
  - Υβριδικοί κώδικες
- **Κωδικοποίηση καναλιού**
  - Ιστορική Αναδρομή
  - Βασικές έννοιες
  - Μετρικά
- **Γραμμικοί block κώδικες**
  - Μαθηματικό υπόβαθρο (πίνακας γεννήτορας, απόσταση hamming, κτλ)
  - Παράδειγμα γραμμικού block κώδικα
    - Κωδικοποίηση
    - Αποκωδικοποίηση

Τεχνικές Διόρθωσης Λαθών (1/2)

- Πρόβλημα: Κατά τη μετάδοση ψηφιακών δεδομένων, ο δέκτης λαμβάνει **λανθασμένα** δεδομένα

- Βασική ιδέα: Μπορεί ο δέκτης
  - να εντοπίσει εάν ένα μήνυμα έχει λάθος;
  - να διορθώσει ένα λανθασμένο μήνυμα;

- Λύση
  - Τεχνικές διόρθωσης λαθών

Τεχνικές Διόρθωσης Λαθών (2/2)

- Forward error-control (FEC)
  - Χρησιμοποιώντας έξτρα bit (bit ισοτιμίας) στα μεταδιδόμενα δεδομένα, μπορούμε να εντοπίσουμε και να διορθώσουμε λάθη κατά την διάρκεια της λήψης.
  - Μονόδρομη επικοινωνία

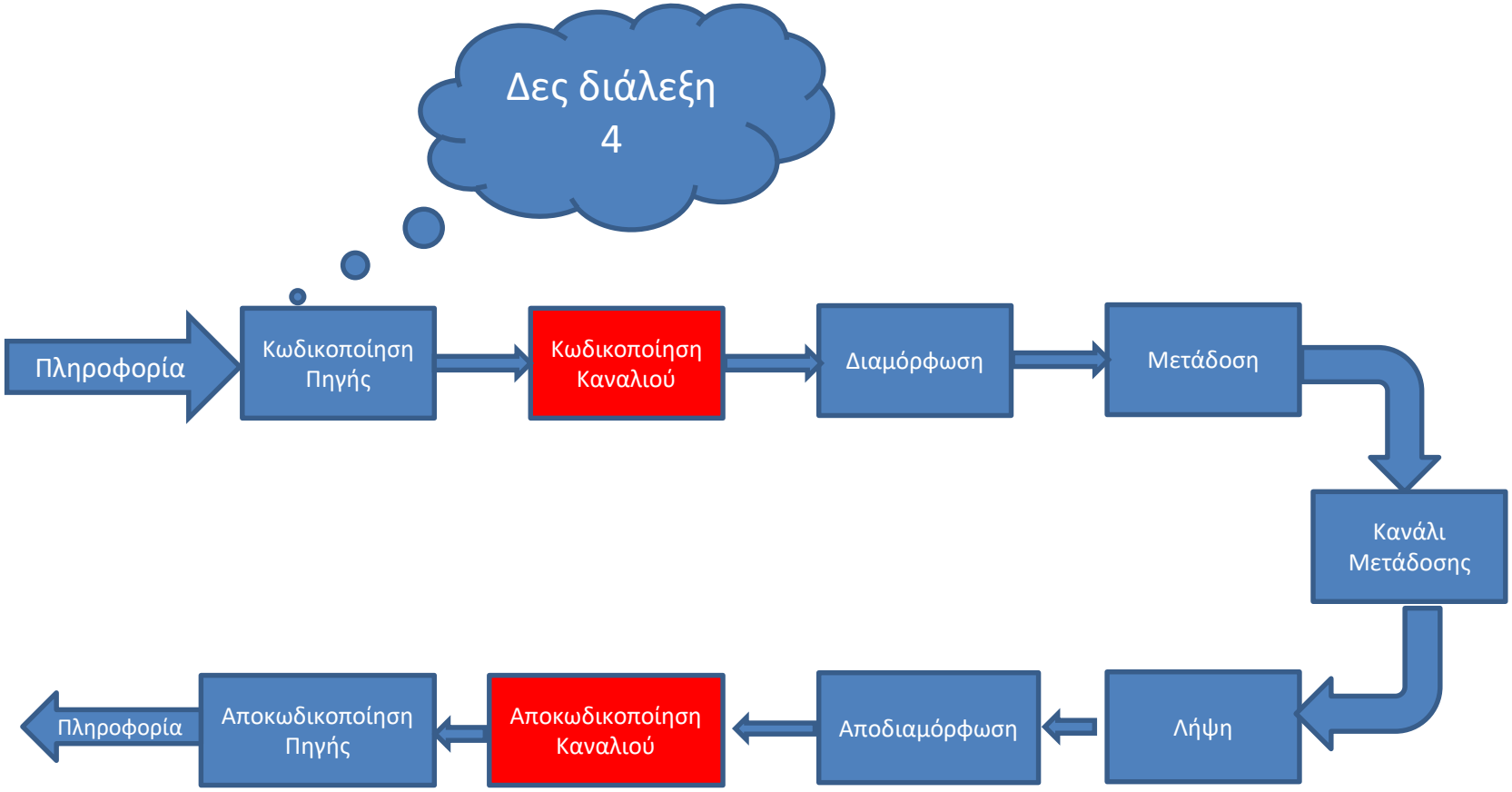
- Automatic-repeat request (ARQ)
  - Χρησιμοποιούμε έξτρα bit κυρίως για τον εντοπισμό λαθών.
  - Ο δέκτης ενημερώνει τον αποστολέα για την ορθότητα ή μη των λαμβανόμενων δεδομένων (ACK (Acknowledgement) ή NACK (Not-Acknowledgement αντίστοιχα).
  - Ο αποστολέας επαναμεταδίδει δεδομένα για τα οποία έλαβε NACK.
  - Αμφίδρομη επικοινωνία

- Υβριδική ARQ (ARQ+FEC)
  - Αμφίδρομη επικοινωνία
  - Εντοπισμός λαθών και διόρθωση

Τεχνικές Διόρθωσης Λαθών FEC: Ιστορική Αναδρομή

1948	• Ο Shannon δημοσιεύει την εργασία του για την θεωρία πληροφορίας
1954	• Ο Hamming ορίζει τους βασικούς δυαδικούς κώδικες
1959	• Κώδικες BCH
1961	• Οι Reed και Solomon προτείνουν την τεχνική ECC
1962	• Κώδικες LDPC από τον Gallager
1967	• Αποκωδικοποίηση Viterbi
1968	• Κώδικες Forney
1969	• Αλγεβρική αποκωδικοποίηση από τους Berlekamp και Messey
1975	• Πρώτες υλοποιήσεις κωδίκων RS σε μηχανές
1983	• Εμφάνιση RS κωδικών σε CD
1988	• Viterbi κώδικες υλοποιημένοι σε hardware συσκευών
1992	• Κώδικες turbo (Berrou)
1996	• Επανεμφάνιση LDPC κωδίκων
2003	• Υιοθέτηση LDPC στο DVB-S2

Κωδικοποίηση Καναλιού
Τεχνική FEC



Forward error-control (FEC)

- Η βασική ιδέα των τεχνικών FEC είναι η μετάδοση ικανού πλήθους έξτρα δεδομένων, έτσι ώστε ο δέκτης να είναι σε θέση να εντοπίσει και να διορθώσει λάθη μετάδοσης.

- Δεν απαιτείται επαναμετάδοση δεδομένων.

- Οι κυριότερες κατηγορίες FEC κωδικών είναι:
  - Κώδικες Block
  - Κυκλικοί κώδικες
  - Συνελικτικοί κώδικες
  - Turbo κώδικες

Κώδικες Block
Βασικές Έννοιες (1/2)

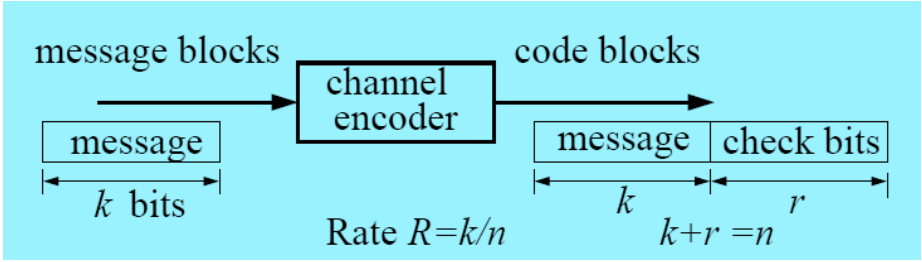
- Η πληροφορία διαιρείται σε blocks μεγέθ**ους *k***
- Σε κάθε block προστίθενται **r bits ισοτιμίας** (ή ελέγχου)
  - Συνολικό μέγεθος κάθε block

$$n = k + r$$

- Ρυθμός κώδικα:

$$R = \frac{k}{n}$$

- Ο αποκωδικοποιητής αναζητά την κωδική λέξη «πλησιέστερη» στο λαμβανόμενο μήνυμα:
  - λαμβανόμενο μήνυμα = κωδική λέξη + διάνυσμα λάθους
- Αντιστάθμιση μεταξύ:
  - Αποδοτικότητας
  - Αξιοπιστίας
  - Πολυπλοκότητας



- Στην αποκωδικοποίηση μέγιστης πιθανότητας, συγκρίνουμε το λαμβανόμενο μήνυμα με όλα τα πιθανά μεταδιδόμενα μηνύματα και επιλέγουμε αυτό με την μικρότερη **απόσταση**.

Κώδικες Block - Βασικές Έννοιες (2/2)

- Υπάρχουν συστηματικοί και μη συστηματικοί κώδικες
- Για την κατηγορία των block κωδίκων, οι συστηματικοί είναι πιο αποδοτικοί.
- Τα k bits πληροφορίας συν τα r bits ισοτιμίας σχηματίζουν την κωδική λέξη ($k + r = \mathrm{n}$)
- Όλες οι πιθανές κωδικές λέξεις σχηματίζουν το βιβλίο κωδίκων (codebook)
- Ένας συστηματικός block κώδικας συμβολίζεται με (n, k)
  - Για παράδειγμα ένας κώδικας $(17, 12)$ έχει $\mathrm{n}=17$, $\mathrm{k}=12$ και $\mathrm{r}=5$
- Στους συστηματικούς γραμμικούς block αλγόριθμους, τα r bits ισοτιμίας τοποθετούνται στο τέλος του block

Block Κώδικες - Μετρικά Σύγκρισης (Αποστάσεις)

- Απόσταση Hamming
  - Το πλήθος των bits που δύο κωδικές λέξεις διαφέρουν.
    - π.χ. Οι λέξεις 01101 και 01111 έχουν απόσταση Hamming ίση με 1 (γιατί;)

- Ευκλείδεια Απόσταση
  - Εάν $\hat{x}_1 = [a_1\, a_2\, \ldots a_n\,]$ και $\hat{x}_2 = [b_1\, b_2\, \ldots b_n\,]$ δύο κωδικές λέξεις μεγέθους n, τότε η Ευκλείδεια απόσταση ορίζεται από την σχέση: $E_{dis} = \sqrt{\sum_{i=1}^{n}(|a_i - b_i|^2)}$

- Επιλογή μετρικού:
  - Ανάλογα με το κανάλι μετάδοσης
    - Gaussian με υψηλό SNR → Ευκλείδεια Απόσταση
    - Raleigh Fading → Απόσταση Hamming

Γραμμικοί Block Κώδικες - Κωδικοποίηση

- Έστω c μία κωδική λέξη με n bits
- Έστω d ένα μήνυμα (προς κωδικοποίηση) με μήνυμα k bits, γραμμένο σε μορφή διανύσματος (π.χ. $d = [011001]$)
- Ένας γραμμικός κώδικας (n, k) ορίζεται από έναν πίνακα **γεννήτορα** $\boldsymbol{G[k \times n]}$
- Ο πίνακας **G** αναλύεται ως εξής:
  - $\boldsymbol{G = [\mathbf{I}_k | P]}$, όπου ο **P** έχει μέγεθος k × $(n - k)$ και ορίζεται από τον κώδικα (n, k) και I_k ο μοναδιαίος πίνακας τάξης k
- Κωδικοποίηση: $c = d \cdot \boldsymbol{G}$
  - Όλες οι αριθμητικές πράξεις γίνονται βάση του modulo 2
- ***Παρατήρηση***: Μία δυαδική ακολουθία των n bits έχει 2^n διαφορετικές τιμές. Ωστόσο, μόνο 2^k από αυτές είναι πιθανό να μεταδοθούν. Γιατί;

Γραμμικοί Block Κώδικες - Κωδικοποίηση - Παράδειγμα

Έστω κώδικας (6, 3) με πίνακα γεννήτορα and codebook

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

Το βιβλίο κωδίκων είναι το:

Μήνυμα	Κωδική Λέξη	
000	000	000
001	001	110
010	010	101
011	011	011
100	100	011
101	101	101
110	110	110
111	111	000

- Για παράδειγμα, για μήνυμα $d = 110$, τα bit ισοτιμίας υπολογίζονται ως εξής:
  - $c4 = 1 \cdot 0 + 1 \cdot 1 + 0 \cdot 1 = 0 + 1 + 0 = 1$
  - $c5 = 1 \cdot 1 + 1 \cdot 0 + 0 \cdot 1 = 1 + 0 + 0 = 1$
  - $c6 = 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 0 = 1 + 1 + 0 = 0$
- Οι αριθμητικές πράξεις είναι δυαδικές (*modulo-2*)
- $2^6 = 64$, αλλά μόνο $2^3 = 8$ κωδικές λέξεις είναι σωστές. Για παράδειγμα, η λέξη 111111 δεν είναι πιθανή. Άρα, εάν την λάβει ο δέκτης, θα προχωρήσει σε διόρθωση.

Γραμμικοί Block Κώδικες - Αποκωδικοποίηση

- Κάθε πίνακας γεννήτορας $\boldsymbol{G}$, μεγέθους $\boldsymbol{k \times n}$ με $\boldsymbol{G = [\mathrm{I}_k | P]}$ σχετίζεται με έναν πίνακα ισοτιμίας $\boldsymbol{H = [P^T | I_{n-k}]}$

Για το προηγούμενο παράδειγμα

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

- **Για κάθε έγκυρη κωδική λέξη $\boldsymbol{c}$**, ισχύει $\mathrm{c} \cdot \boldsymbol{H^T} = 0$

- Μία λαμβανόμενη λέξη r μπορεί να γραφεί ως

$$r = c + e$$

- Όλα τα στοιχεία είναι δυαδικά, π.χ. εάν μεταδοθεί το στοιχείο $c_i = 0$ και λάβουμε $r_i = 1$, τότε $e_i = 1$

- Ορίζουμε ως σύνδρομο λάθους s το διάνυσμα γραμμή μεγέθους $n - k$ που προκύπτει από την πράξη

$$s = rH^T = (c + e)H^T = cH^T + eH^T = eH^T$$

- Το s σχετίζεται με το διάνυσμα λάθους e και μπορεί να χρησιμοποιηθεί για να εντοπισθούν και να διορθωθούν λάθη

SOFT Αποκωδικοποίηση

ΑΛΓΟΡΙΘΜΟΣ

Για κάθε n λαμβανόμενα δείγματα:

1. Υπολογίζουμε τις Ευκλείδειες αποστάσεις ανάμεσα σε όλες τις διαμορφωμένες κωδικές λέξεις και στα δείγματα που λάβαμε.

2. Επιλέγουμε ως κωδική λέξη εκείνη με την ελάχιστη Ευκλείδεια απόσταση.

3. Εκτελούμε την αντίστροφη αντιστοίχιση για να βρούμε τη λέξη πληροφορίας.

HARD Αποκωδικοποίηση

ΑΛΓΟΡΙΘΜΟΣ

Για κάθε n λαμβανόμενα δείγματα:

1. Εκτελούμε αποδιαμόρφωση των λαμβανόμενων δειγμάτων και καταλήγουμε στα αντίστοιχα δυαδικά δεδομένα

2. Υπολογίζουμε την κωδική λέξη που είναι πλησιέστερα με βάση την απόσταση Hamming. (Συνήθως με χρήση lookup table)

3. Εκτελούμε την αντίστροφη αντιστοίχιση για να βρούμε τη λέξη πληροφορίας

Γραμμικοί Block Κώδικες
Δυνατότητα εντοπισμού λαθών και διόρθωσης

- **Βάρος** μίας κωδικής λέξης c είναι ο αριθμός των μη μηδενικών στοιχείων της c

- **Απόσταση Hamming** μεταξύ δύο κωδικών λέξεων c_1 και c_2 ορίζεται ως το πλήθος των στοιχείων όπου αυτά διαφέρουν

- **Ελάχιστη απόσταση** ενός βιβλίου κωδίκων , d_{min}, είναι η ελάχιστη απόσταση Hamming μεταξύ οποιουδήποτε ζευγαριού του βιβλίου κωδίκων

- Η ελάχιστη απόσταση distance d_{min} ενός ***γραμμικού*** block κώδικα είναι το **ελάχιστο βάρος** των μη μηδενικών κωδίκων στο βιβλίο

- **Κώδικας με d_{min} μπορεί να ανιχνεύσει μέχρι**

  $$d_{min} - 1 \text{ λάθη}$$

  και να διορθώσει

  $$\frac{d_{min}-1}{2} \text{ λάθη}$$

  σε κάθε κωδική λέξη

Γραμμικοί Block Κώδικες
Δημιουργία Hamming κωδίκων

- Για κάθε $m \geq 2$ υπάρχει ένας Hamming κώδικας με τα παρακάτω χαρακτηριστικά:
  - Μήκος Κωδικής λέξης: $n = 2m - 1$
  - Πλήθος συμβόλων πληροφορίας: $k = 2^m - m - 1$
  - Πλήθος συμβόλων ισοτιμίας $m = n - k$
  - Δυνατότητα διόρθωσης λαθών $t = 1$, αφού $d_{min} = 3$

- Ο πίνακας ελέγχου ισοτιμίας Hενός κώδικα Hamming αποτελείται από όλες τις μη μηδενικούς συνδυασμούς μήκους m ως στήλες

Γραμμικοί Block Κώδικες - Παράδειγμα Hamming κώδικα

- Για παράδειγμα, έστω $m = 3$
  - $m = 3$ bit ισοτιμίας
  - $n = 2^m - 1 = 2^3 - 1 = 7$ bit το μήκος κάθε κωδικής λέξης
  - $k = 2^m - m - 1 = 2^3 - 3 - 1 = 4$ bit πληροφορίας

- Συμβολίζουμε αυτόν τον γραμμικό κώδικα με (7, 4, 1)

- Ο πίνακας ελέγχου ισοτιμίας **H** αυτού του κώδικα είναι:

$$\mathrm{H} = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] = \left[\begin{array}{c|cccc} & 1 & 0 & 1 & 1 \\ \mathrm{I}_3 & 1 & 1 & 1 & 0 \\ & 0 & 1 & 1 & 1 \end{array}\right] = [\mathrm{I}_3 | \mathrm{P}^T]$$

- Συνεπώς ο πίνακας Γεννήτορας του κώδικα μπορεί να κατασκευαστεί ως

$$\boldsymbol{G} = [\mathrm{I}_4 | P]$$

Γραμμικοί Block Κώδικες - Παράδειγμα Hamming κώδικα