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

Θεωρία Πληροφορίας

Διάλεξη 8: Κωδικοποίηση καναλιού με κυκλικούς κώδικες block

Δρ. Μιχάλης Παρασκευάς
Επίκουρος Καθηγητής

Ατζέντα

- **Κυκλικοί block κώδικες**
  - Μαθηματικό υπόβαθρο (πολυώνυμο γεννήτορας, κτλ)
  - Παράδειγμα κυκλικού block κώδικα
    - Κωδικοποίηση
    - Αποκωδικοποίηση
- **Κέρδος κωδικοποίησης καναλιού**

Κυκλικοί Κώδικες (1/2)

- Οι κυκλικοί (ή πολυωνυμικοί) κώδικες είναι ένα υποσύνολο των γραμμικών κωδίκων.
- Ορισμός: Εάν $c_i = [c_0, c_1, \dots, c_{n-2}, c_{n-1}]$ μία κωδική λέξη τότε η $c_j = [c_{n-1}, c_0, \dots, c_{n-3}, c_{n-2}]$ είναι επίσης μία κωδική λέξη.
- Ένα μήνυμα μήκους k bits: $d = [d_0, d_1, \dots, d_{k-1}]$ μπορεί να περιγραφεί με ένα πολυώνυμο $d(x) = d_0 + d_1 x^1 + d_2 x^2 + \cdots + d_{k-1} x^{k-1}$.
- Ο κώδικας ορίζεται από το πολυώνυμο γεννήτορα $g(x) = g_0 + g_1 x^1 + \cdots + g_r x^r$ με $g_0 = 1$ και $g_r = 1$.
- Μία κωδική λέξη $\mathbf{c} = [c_0, c_1, \dots, c_{n-1}]$ για το d μπορεί να περιγραφεί με την βοήθεια πολυωνύμου:

$$c(x) = Rem\left(\frac{x^r d(x)}{g(x)}\right) + x^r d(x)$$

όπου το υπόλοιπο $Rem\left(\frac{x^r d(x)}{g(x)}\right)$ είναι ένα πολυώνυμο μέχρι τάξης x^{r-1} (r bits ισοτιμίας) ονομάζεται πολυώνυμο ελέγχου ισοτιμίας τους $d(x)$.

- Όλοι οι υπολογισμοί είναι βάση του modulo-2.

Κυκλικοί Κώδικες (2/2)

- Παράδειγμα κυκλικού κώδικα (7,4) με πολυώνυμο γεννήτορα
$$g(x) = 1 + x^2 + x^3$$
- Έστω μήνυμα $\mathrm{d} = 0101$. Τότε
$$\mathrm{d}(x) = x^1 + x^3$$
$$x^3\mathrm{d}(x) = x^4 + x^6$$
$$Rem\left(\frac{x^3 d(x)}{g(x)}\right) = 1$$
$$c(x) = 1 + x^4 + x^6$$
- Συνεπώς $c = 1\ 0\ 0\ \ 0\ 1\ 0\ 1$, με τα 3 πρώτα bits να είναι τα bit ισοτιμίας και τα υπόλοιπα τα bit πληροφορίας
- Στην αποκωδικοποίηση, το λαμβανόμενο $r(x) = c(x) + e(x)$ με τα μη μηδενικά bit του $e(x)$ να υποδεικνύουν τα λάθη και το πολυώνυμο σύνδρομο να υπολογίζεται ως εξής:
$$Rem\left(\frac{c(x) + e(x)}{g(x)}\right) = Rem\left(\frac{e(x)}{g(x)}\right) = s(x)$$

- Εάν το $s(x)$ είναι μηδενικό, τότε το λαμβανόμενο σήμα είτε δεν περιέχει λάθη είτε περιέχει λάθη που δεν μπορούν να ανιχνευθούν

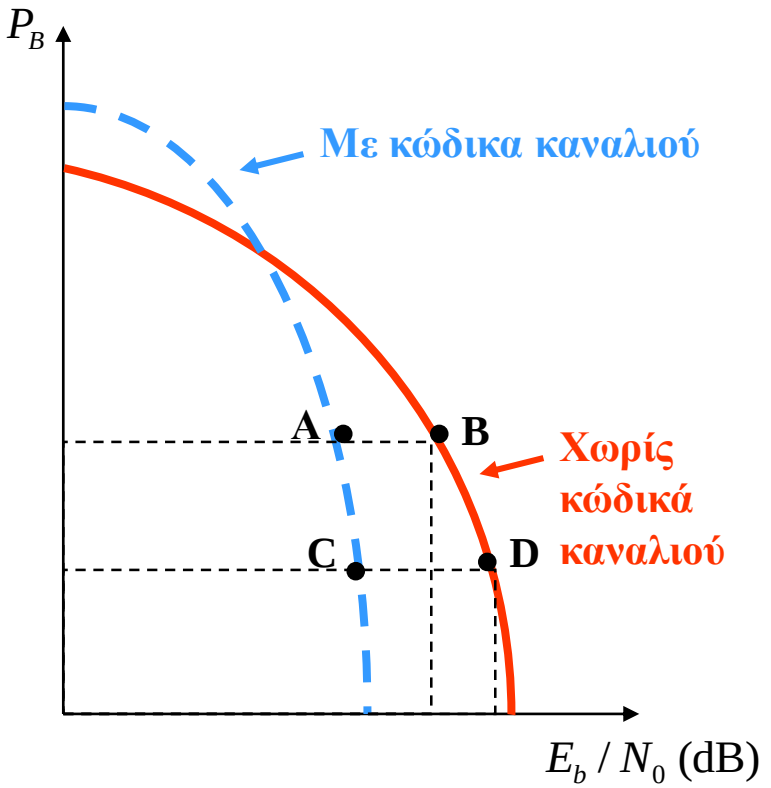
- Εάν το $s(x)$ είναι μη μηδενικό, τότε θα λάθη ανιχνεύονται και διορθώνονται

Άλλοι κώδικες FEC

- Οι BCH είναι ένα υποσύνολο κυκλικών κωδίκων με μεγάλη τιμή d_{min}, και συμβολίζονται με (n, k, d_{min}). Έχουν μεγάλη χρησιμότητα.
- Οι μη δυαδικές εκδόσεις των BCH ονομάζονται RC (Reed Solomon)
- Κώδικες Golay

Τι επιτυγχάνει η Κωδικοποίηση Καναλιού

- Απαιτεί λιγότερη ισχύ εκπομπής προκειμένου να πετύχουμε την ίδια πιθανότητα σφάλματος.
- Η μείωση αυτή της ισχύος (σε dB) ονομάζεται «Κέρδος Κωδικοποίησης».
- Ωστόσο, η μετάδοση «πλεονάζουσας πληροφορίας» μειώνει το ρυθμό μετάδοσης της «χρήσιμης» πληροφορίας.



Άσκηση 1

- Θεωρήστε τον κώδικα Hamming με $m = 3$ και πίνακα γεννήτορα

$$G = \begin{bmatrix} 1000110 \\ 0100011 \\ 0010111 \\ 0001101 \end{bmatrix}$$

  - Να υπολογιστούν τα n, k
  - Ποιος ο ρυθμός κωδικοποίησης;
  - Να υπολογιστεί το βιβλίο κωδίκων
  - Για κάθε κώδικα που προέκυψε, να υπολογιστεί η απόσταση Hamming από το λαμβανόμενο σήμα $r = [0000001]$. Ποιος είναι ο κώδικας που θα προτείνει το βιβλίο κωδίκων;

Λύση

- Αφού ο πίνακας γεννήτορας G είναι διαστάσεων $4x7$, έχουμε $n = 7$ και $k = 4$
- Ρυθμός κωδικοποίησης $R = \frac{k}{n} = \frac{4}{7}$
- Για να υπολογίσουμε το βιβλίο κωδίκων, θα πρέπει να υπολογίσουμε τα γινόμενα $d_i G$, όπου G ο πίνακας γεννήτορας και d_i όλες οι πιθανές λέξεις κλειδιά (οι οποίες είναι $2^k = 2^4 = 16$).
- Για παράδειγμα, εάν $d_i = [1010]$

$$\text{τότε } c_i = d_i G = [1010] \begin{bmatrix} 1000110 \\ 0100011 \\ 0010111 \\ 0001101 \end{bmatrix} = [1010221].$$

- Ωστόσο, στην κωδικοποίηση όλες οι πράξεις είναι modulo 2. Συνεπώς, η κωδική λέξη θα είναι $c_i = [1010001]$.

Λύση

- Μπορείτε να επαληθεύσετε το αποτέλεσμα τρέχοντας τον κώδικα matlab:

```
d=[1 0 1 0];
G=[1 0 0 0 1 1 0;0 1 0 0 0 1 1;0 0 1 0 1 1 1;0 0 0 1 1 0 1];
c=mod(d*G, 2);
```

- Ακολουθώντας την ίδια διαδικασία για όλους τους πιθανούς συνδυασμούς παίρνουμε τον παρακάτω πίνακα

Μήνυμα	Κωδική Λέξη	
0000	0000	000
0001	0001	101
0010	0010	111
0011	0011	010
0100	0100	011
0101	0101	110
0110	0110	100
0111	0111	001

Μήνυμα	Κωδική Λέξη	
1000	1000	110
1001	1001	011
1010	1010	001
1011	1011	100
1100	1100	101
1101	1101	000
1110	1110	010
1111	1111	111

Λύση

- Θυμίζουμε πώς η απόσταση Hamming δύο σημάτων είναι τα διαφορετικά bits. Συνεπώς, για το προηγούμενο βιβλίο κωδίκων, για $r = [0000001]$ έχουμε:

Κωδική Λέξη		Απόσταση Hamming
0000	000	1
0001	101	2
0010	111	3
0011	010	4
0100	011	2
0101	110	5
0110	100	4
0111	001	3

Κωδική Λέξη		Απόσταση Hamming
1000	110	4
1001	011	3
1010	001	2
1011	100	5
1100	101	3
1101	000	4
1110	010	5
1111	111	6

- Συνεπώς, ο κώδικας θα διορθώσει το λαμβανόμενο σήμα σε $r = [0000000]$.