Φυλλάδιο 4^o

<u>Άσκηση 1</u>

Έστω ότι d περιττός. Ένας δυαδικός (n, M, d) κώδικας υπάρχει ακριβώς τότε όταν υπάρχει ένας δυαδικός $(n+1, M, d+1)$ κώδικας.

Θεωρούμε τον (n, M, d) κώδικα C και κατασκευάζουμε τον κώδικα

$$\overline{C} = \left\{ x x_{n+1} : x = x_1 x_2 \ldots x_n \in C, \quad x_{n+1} = \bigoplus_{i=1}^{n} x_i \right\}.$$

Για κάθε $x,\, y \in C$ ισχύει $d(x, y) \geq d$.

- Εάν $d(x, y) \geq d+1$, προφανώς και $d(x x_{n+1}, y y_{n+1}) \geq d+1$.
- Εάν $d(x, y) = d$, τότε

$$\begin{aligned} d(x x_{n+1}, y y_{n+1}) &= d(x, y) + x_{n+1} \oplus y_{n+1} \\ &= d(x, y) + \left(\bigoplus_{i=1}^{n} x_i \right) \oplus \left(\bigoplus_{j=1}^{n} y_j \right) \\ &= d(x, y) + \bigoplus_{i=1}^{n} (x_i \oplus y_i) \\ &= d(x, y) + \left(\bigoplus_{k=1}^{d} 1 \right) \oplus \left(\bigoplus_{l=1}^{n-d} 0 \right) \\ &= d+1 \end{aligned}$$

Επομένως, $d_{min}(\overline{C}) = d+1$, και επειδή $|C| = |\overline{C}| = M$, ο κώδικας $\overline{C}$ είναι ένας $(n+1, M, d+1)$ κώδικας.
Για το αντίστροφο, θεωρούμε ότι υπάρχει $(n+1, M, d+1)$ κώδικας C και κατασκευάζουμε κώδικα $\overline{C}$ ως εξής: παίρνουμε δύο κωδικές λέξεις του C x, y για τις οποίες ισχύει $d(x, y) = d+1$ και αφαιρούμε από όλες τις κωδικές λέξεις του C μία από τις συντεταγμένες $i \in \{1, 2, \ldots, n+1\}$ για τις οποίες ισχύει $x_i \oplus y_i = 1$. Ο κώδικας $\overline{C}$ που προκύπτει έχει μήκος κωδικών λέξεων n, ελάχιστη απόσταση d και επιπλέον $|C| = |\overline{C}| = M$. Άρα, είναι ένας (n, M, d) κώδικας.

Άσκηση 2

Όλοι οι δυαδικοί γραμμικοί κώδικες Hamming με σταθερό n είναι ισοδύναμοι.

Ο πίνακας ελέγχου ισοτιμίας H κάθε $[n = 2^m - 1, k = n - m, 3]$ κώδικα Hamming C, περιλαμβάνει ως στήλες τα $(2^m - 1)$ μή μηδενικά διανύσματα του $\mathbb{F}_2^m$, εξ ορισμού. Επομένως, ο πίνακας ελέγχου ισοτιμίας οποιουδήποτε άλλου κώδικα Hamming μήκους n, προκύπτει από τη μετάθεση κάποιων από τις στήλες του H. Άρα, όλοι οι κώδικες Hamming μήκους n είναι ισοδύναμοι.

Άσκηση 3

Αν C_1 είναι ένας $[n, k_1, d_1]$ γραμμικός κώδικας και C_2 ένας $[n, k_2, d_2]$ γραμμικός κώδικας, σχηματίζουμε τον κώδικα

$$C = \{(y, x \oplus y) : x \in C_1, \quad y \in C_2\}$$

(i) Αν ο C_1 έχει γεννήτορα πίνακα G_1 και ο C_2 έχει γεννήτορα πίνακα τον G_2, να αποδείξετε ότι ο C είναι ένας $[2n, k_1 + k_2]$ γραμμικός κώδικας με γεννήτορα πίνακα

$$G = \begin{bmatrix} 0 & G_1 \\ G_2 & G_2 \end{bmatrix}.$$

(ii) Να αποδείξετε ότι

$$d_{min}(C) = \min\{d_1, 2d_2\}.$$

(i) Ο κώδικας C είναι γραμμικός αφού για κάθε $z_1 = (y_1, x_1 \oplus y_1)$, $z_2 = (y_2, x_2 \oplus y_2) \in C$, με x_1, $x_2 \in C_1$ και $y_1, y_2 \in C_2$, ισχύει ότι:

$$\begin{aligned} z_1 \oplus z_2 &= (y_1, x_1 \oplus y_1) \oplus (y_2, x_2 \oplus y_2) \\ &= (y_1 \oplus y_2, x_1 \oplus y_1 \oplus x_2 \oplus y_2) \\ &= (y_1 \oplus y_2, (x_1 \oplus x_2) \oplus (y_1 \oplus y_2)) \end{aligned}$$

και επομένως $z_1 \oplus z_2 \in C$, διότι $x_1 \oplus x_2 \in C_1$ και $y_1 \oplus y_2 \in C_2$, λόγω της γραμμικότητας των κωδίκων C_1, C_2.

Επίσης, οι $(k_1 + k_2)$ γραμμές του G είναι γραμμικώς ανεξάρτητες διότι θέτοντας

$$\bigoplus_{i=1}^{k_1} \lambda_i(\mathbf{0}_n, \mathbf{g_i^1}) \oplus \bigoplus_{j=1}^{k_2} \mu_j(\mathbf{g_j^2}, \mathbf{g_j^2}) = \left(\bigoplus_{j=1}^{k_2} \mu_j \mathbf{g_j^2} \ , \ \bigoplus_{i=1}^{k_1} \lambda_i \mathbf{g_i^1} \oplus \bigoplus_{j=1}^{k_2} \mu_j \mathbf{g_j^2} \right) = (\mathbf{0}_n, \mathbf{0}_n) \tag{1}$$

προκύπτει ότι θα πρέπει να ισχύουν οι σχέσεις:

$$\bigoplus_{j=1}^{k_2} \mu_j \mathbf{g_j^2} = \mathbf{0}_n \tag{2}$$

$$\bigoplus_{i=1}^{k_1} \lambda_i \mathbf{g_i^1} = \bigoplus_{j=1}^{k_2} \mu_j \mathbf{g_j^2} \tag{3}$$

όπου $\mathbf{g_i^1}$ είναι οι γραμμές του G_1 $(1 \leq i \leq k_1)$, $\mathbf{g_j^2}$ είναι οι γραμμές του G_2 $(1 \leq j \leq k_2)$ και λ_i, $\mu_j \in \mathbb{F}_2$. Μέσω της (2), η εξίσωση (3) συνεπάγεται ότι θα πρέπει και

$$\bigoplus_{i=1}^{k_1} \lambda_i \mathbf{g_i^1} = \mathbf{0}_n \tag{4}$$

Από τις (2), (4) προκύπτει ότι

$$\lambda_i = \mu_j = 0 \quad \forall i \in \{1, 2, \ldots, k_1\} \text{ και } j \in \{1, 2, \ldots, k_2\} \tag{5}$$

διότι οι γραμμές του G_1 είναι γραμμικώς ανεξάρτητες μεταξύ τους και το ίδιο ισχύει για τις γραμμές του G_2. Η σχέση (5) μας λέει ότι η εξίσωση (1) ισχύει μόνο για μηδενικά λ_i, μ_j, οπότε και οι γραμμές του G είναι γραμμικώς ανεξάρτητες.

Τέλος, ο πίνακας G παράγει τον κώδικα C, διότι για κάθε $z = (y, x \oplus y) \in C$, με $x = aG_1 \in C_1$, $y = bG_2 \in C_2$, ισχύει ότι:

$$\begin{aligned} z &= (y, x \oplus y) \\ &= (bG_2, aG_1 \oplus bG_2) \\ &= a \begin{bmatrix} \mathbf{0}_{k_1 \times n} & G_1 \end{bmatrix} \oplus b \begin{bmatrix} G_2 & G_2 \end{bmatrix} \\ &= (a, b) \begin{bmatrix} \mathbf{0}_{k_1 \times n} & G_1 \\ G_2 & G_2 \end{bmatrix} \\ &= (a, b)G \end{aligned}$$

όπου $a \in \mathbb{F}_2^{k_1}$ και $b \in \mathbb{F}_2^{k_2}$. Δηλ. κάθε κωδική λέξη του C προκύπτει ως γραμμικός συνδυασμός των $(k_1 + k_2)$ γραμμικώς ανεξαρτήτων γραμμών του G και άρα ο G παράγει τον κώδικα C. Επομένως, ο κώδικας C είναι ένας $[2n, k_1 + k_2]$ κώδικας.

(ii) Για κάθε $x \in C_1$, $y \in C_2$ ισχύει ότι

$$z = (y, x \oplus y) \in C \tag{6}$$

οπότε

$$w(z) = w(y) + w(x \oplus y) \tag{7}$$

ενώ λόγω γραμμικότητας

$$d_{min}(C) = \min\{w(z) : z \in C,\ z \neq \mathbf{0}_{2n}\} \tag{8}$$

Διακρίνουμε τις εξής περιπτώσεις για τις τιμές του $w(z)$ της (7):

- Εάν $x \neq \mathbf{0}_n$, $y = \mathbf{0}_n$, τότε $w(z) = w(x) \geq d_1$, με την ισότητα να ισχύει για κάθε x τέτοιο ώστε $w(x) = w_{min}(C_1)$.
- Εάν $x = \mathbf{0}_n$, $y \neq \mathbf{0}_n$, τότε $w(z) = 2w(y) \geq 2d_2$, με την ισότητα να ισχύει για κάθε y τέτοιο ώστε $w(y) = w_{min}(C_2)$, ενώ
- εάν $x \neq \mathbf{0}_n$, $y \neq \mathbf{0}_n$, έχουμε

  $$w(z) = w(y) + w(x \oplus y) \geq w(y) + (w(x) - w(y)) = w(x) \geq d_1 \geq \min\{d_1, 2d_2\}.$$

Επομένως για κάθε $z \neq \mathbf{0}_{2n}$, ισχύει $w(z) \geq \min\{d_1, 2d_2\}$ ενώ υπάρχουν $z \in C$ για τα οποία $w(z) = \min\{d_1, 2d_2\}$ και από την (8) $d_{min}(C) = \min\{d_1, 2d_2\}$.