# Φυλλάδιο $2^o$

**Άσκηση 1**

Στην Άσκηση 3 του πρώτου φυλλαδίου ο $(11, 24, 5)$ κώδικας $C$ που κατασκευάσατε είναι γραμμικός.

Για να είναι ο κώδικας $C$ γραμμικός, θα πρέπει να είναι διανυσματικός υπόχωρος του $\mathbb{F}_2^{11}$. Επομένως θα πρέπει να ισχύει:

(i) $\forall\ x,\ y \in C \Rightarrow x \oplus y \in C$

(ii) $\forall \lambda \in \mathbb{F}_2,\ x \in C \Rightarrow \lambda x \in C$.

Ο *incidence* πίνακας $A = [a_{ij}]$ της άσκησης ήταν ο εξής:

| | $bl_1$ | $bl_2$ | $bl_3$ | $bl_4$ | $bl_5$ | $bl_6$ | $bl_7$ | $bl_8$ | $bl_9$ | $bl_{10}$ | $bl_{11}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 2 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 3 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 4 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 5 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| 6 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 7 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 8 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
| 9 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| 10 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 11 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |

ενώ ο κώδικας $C$ περιλαμβάνει επιπλέον τις γραμμές του πίνακα $B = [b_{ij}] = [1 \oplus a_{ij}]$, το μηδενικό $1 \times 11$ διάνυσμα $\mathbf{0}$ καθώς και το συμπληρωματικό του διάνυσμα $\mathbf{1}$. Παρατηρούμε ότι για τις 2 πρώτες γραμμές $a_1$, $a_2$ του πίνακα $A$, ισχύει:

$$a_1 \oplus a_2 = (11011001001) \notin A$$

αφού $w(a_1 \oplus a_2) = 6$. Επιπλέον $a_1 \oplus a_2 \notin B$, ενώ προφανώς $a_1 \oplus a_2 \neq \mathbf{0}$ και $a_1 \oplus a_2 \neq \mathbf{1}$. Επομένως $a_1 \oplus a_2 \notin C$ και εφόσον δεν ισχύει η απαίτηση $(i)$, ο κώδικας $C$ δεν είναι διανυσματικός υπόχωρος του $\mathbb{F}_2^{11}$. Άρα δεν είναι γραμμικός.

**Άσκηση 2**

Να αποδείξετε ότι το σύνολο $E_n$ (δες και Άσκηση 2 του φυλλαδίου 1) είναι διανυσματικός υπόχωρος του $\mathbb{F}_2^n$. Πόσο είναι η διάσταση του $E_n$; Να βρείτε μια βάση του $E_n$.

Για να είναι το $E_n$ διανυσματικός υπόχωρος του $\mathbb{F}_2^n$ θα πρέπει

(i) $\forall \lambda \in \mathbb{F}_2,\ x \in E_n \Rightarrow \lambda x \in E_n$

(ii) $\forall\ x,\ y \in E_n \Rightarrow x \oplus y \in E_n\ x \in E_n \Rightarrow \lambda x \in E_n$.

(i) Εάν $\mathbf{0}$ είναι το μηδενικό διάνυσμα του $\mathbb{F}_2^n$ ισχύει

- $0 \cdot x = \mathbf{0}$, $w(\mathbf{0}) = 0$ άρτιος και $\mathbf{0} \in E_n$
- $1 \cdot x = x \in E_n$

(ii) Έστω $x, y \in E_n$. Τότε $x = \overline{x}x_n$, $y = \overline{y}y_n$ για κάποια $\overline{x}, \overline{y} \in \mathbb{F}_2^{n-1}$ και $x_n = \bigoplus_{i=1}^{n-1} x_i$, $y_n = \bigoplus_{i=1}^{n-1} y_i$.

Γνωρίζουμε επίσης πως ισχύει γενικότερα $\forall\ u,\ v \in \mathbb{F}_2^k$

$$d(u, v) = w(u) + w(v) - 2w(u \cap v) \tag{1}$$

όπου $u \cap v = \{u_i, v_i : u_i = v_i,\ i \in \{1, 2, \ldots, k\}\}$. Για να ισχύει ότι το $x \oplus y \in E_n$ θα πρέπει ο $w(x \oplus y)$ να είναι άρτιος. Ισχύει

$$\begin{aligned} w(x \oplus y) &= \sum_{i=1}^{n-1} x_i \oplus y_i + \left(\bigoplus_{i=1}^{n-1} x_i\right) \oplus \left(\bigoplus_{i=1}^{n-1} y_i\right) \\ &= d(\overline{x}, \overline{y}) + \left(\bigoplus_{i=1}^{n-1} x_i\right) \oplus \left(\bigoplus_{i=1}^{n-1} y_i\right) \end{aligned} \tag{2}$$

Από την (1) ισχύει ότι

$$d(\overline{x}, \overline{y}) = w(\overline{x}) + w(\overline{y}) - 2w(\overline{x} \cap \overline{y}) \tag{3}$$

Διακρίνουμε τις εξής περιπτώσεις:

- Εάν $w(\overline{x})$ περιττός και $w(\overline{y})$ άρτιος τότε $\bigoplus_{i=1}^{n-1} x_i = 1$, $\bigoplus_{i=1}^{n-1} y_i = 0$ ενώ από την (3) $d(\overline{x}, \overline{y})$ περιττός, γεγονός που συνεπάγεται από τη (2) ότι $w(x \oplus y)$ άρτιος. Το ίδιο συμπεραίνουμε εάν $w(\overline{x})$ άρτιος και $w(\overline{y})$ περιττός.

- Όμοια, εάν $w(\overline{x})$ άρτιος και $w(\overline{y})$ άρτιος η (2) δίνει ότι $w(x \oplus y)$ άρτιος.

Άρα σε κάθε περίπτωση, εάν $x,\ y \in E_n$, τότε $x \oplus y \in E_n$.

Εφόσον πληρούνται οι (i), (ii), το $E_n$ είναι διανυσματικός υπόχωρος του $\mathbb{F}_2^n$.
Διάσταση και βάση του χώρου $E_n$: Για κάθε $x = (x_1, x_2, \ldots, x_{n-1}, x_n) \in E_n$, ισχύει ότι

$$\begin{aligned} x &= (x_1, x_2, \ldots, x_{n-1}, \bigoplus_{i=1}^{n-1}) \\ &= x_1(1, 0, \ldots, 0, 1) \oplus x_2(0, 1, \ldots, 0, 1) \oplus \cdots \oplus x_{n-1}(0, 0, \ldots, 1, 1) \\ &= x_1(\mathbf{e_1}, 1) \oplus x_2(\mathbf{e_2}, 1) \oplus \cdots \oplus x_{n-1}(\mathbf{e_{n-1}}, 1) \\ &= \bigoplus_{i=1}^{n-1} x_i(\mathbf{e_i}, 1) \end{aligned} \tag{4}$$

όπου $\mathbf{e_i}$ $(1 \leq i \leq n-1)$, είναι τα $n-1$ γραμμικώς ανεξάρτητα διανύσματα της ορθοκανονικής βάσης του $\mathbb{F}_2^{n-1}$. Παρατηρούμε επίσης πως και τα διανύσματα $(\mathbf{e_i}, 1)$ $(1 \leq i \leq n-1)$, είναι γραμμικώς ανεξάρτητα διανύσματα του $E_n$. Επομένως από την (4) συμπεραίνουμε ότι κάθε $x \in E_n$ γράφεται ως γραμμικός συνδυασμός των $n-1$ γραμμικώς ανεξαρτήτων διανυσμάτων $(\mathbf{e_i}, 1)$. Δηλ. η διάσταση του χώρου $E_n$ είναι $n-1$ και μια βάση του αποτελούν τα διανύσματα $(\mathbf{e_i}, 1)$, $(1 \leq i \leq n-1)$.

**Άσκηση 3**

Ποιές είναι οι παράμετροι $[n, k, d]$ του γραμμικού κώδικα $E_n$· Να γράψετε τον πίνακα γεννήτορα αυτού σε κανονική μορφή.

Το μήκος των κωδικών λέξεων είναι $n$, οπότε η πρώτη παράμετρος είναι $n$. Από το γεγονός ότι έχουμε $n-1$ ψηφία εισόδου ισχύει $k = n-1$. Τέλος,

$$d_{min}(E_n) = \min\{w(x) : x \in E_n, x \neq \mathbf{0}\} = 2$$

όπου $\mathbf{0}$ είναι το μηδενικό διάνυσμα του $E_n$. Άρα $d = 2$.
Από την (4), ο γεννήτορας πίνακας $G$ του $E_n$ θα μπορούσε να έχει ως γραμμές τα $n-1$ γραμμικώς ανεξάρτητα διανύσματα $(\mathbf{e_i}, 1)$, $(1 \leq i \leq n-1)$:

$$G = \begin{bmatrix} \mathbf{e_1} & 1 \\ \mathbf{e_2} & 1 \\ \vdots & \vdots \\ \mathbf{e_{n-1}} & 1 \end{bmatrix}$$

Ο πίνακας $G$ έχει διαστάσεις $(n-1) \times n$ και είναι σε κανονική μορφή.

**΄Ασκηση 4**

Δίνεται ο γραμμικός $[6,3]$ κώδικας ως προς το σώμα $\mathbb{F}_3$, με γεννήτορα πίνακα

$$G = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 & 1 \end{bmatrix}$$

Να γράψετε τον $G$ στην κανονική του μορφή.

Με αντιμετάθεση της 1ης και 4ης στήλης του $G$, προκύπτει ο ισοδύναμος πίνακας $G_1$:

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 0 & 0 & 2 & 1 & 1 & 1 \end{bmatrix}$$

Με αντιμετάθεση της 3ης και 4ης στήλης του $G_1$, προκύπτει ο ισοδύναμος πίνακας $G_2$:

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 2 & 1 & 1 \end{bmatrix}$$

ο οποίος είναι σε κανονική μορφή και αποτελεί την κανονική μορφή του $G$.

**΄Ασκηση 5**

Αν ο $C$ είναι δυαδικός γραμμικός κώδικας, τότε ο κώδικας που προκύπτει προσθέτοντας στο τέλος κάθε κωδικής λέξης το σύμβολο ελέγχου ισοτιμίας είναι επίσης γραμμικός.

Θεωρούμε τον κώδικα

$$\overline{C} = \left\{ x_1 x_2 \dots x_n x_{n+1} : x = x_1 x_2 \dots x_n \in C \text{ και } x_{n+1} = \bigoplus_{i=1}^{n} \right\}$$

Θεωρούμε δύο κωδικές λέξεις του κώδικα $C$, $x$, $y$. Το ότι ο $C$ είναι γραμμικός συνεπάγεται ότι ισχύουν οι σχέσεις

(i) $0 \cdot x = \mathbf{0}_n \in C$ όπου $\mathbf{0}_n$ είναι το μηδενικό διάνυσμα του $\mathbb{F}_2^n$.

(ii) $x \oplus y \in C$.

Για τις αντίστοιχες κωδικές λέξεις $xx_{n+1}$, $yy_{n+1}$ του κώδικα $\overline{C}$ ισχύουν τα εξής:

- $0 \cdot xx_{n+1} = \mathbf{0}_{n+1} \in \overline{C}$, εφόσον από την (i), $\mathbf{0}_n \in C$ και $\bigoplus_{i=1}^{n} 0 = 0$ και

- αν θέσουμε $z = x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$ θα έχουμε:

$$\begin{aligned} xx_{n+1} \oplus yy_{n+1} &= \left(x_1, x_2, \ldots, x_n, \bigoplus_{i=1}^{n} x_i\right) \oplus \left(y_1, y_2, \ldots, y_n, \bigoplus_{i=1}^{n} y_i\right) \\ &= \left(x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n, \left(\bigoplus_{i=1}^{n} x_i\right) \oplus \left(\bigoplus_{i=1}^{n} y_i\right)\right) \\ &= (x \oplus y, \bigoplus_{i=1}^{n}(x_i \oplus y_i)) \\ &= (z, \bigoplus_{i=1}^{n}(x_i \oplus y_i)) \end{aligned}$$

οπότε $xx_{n+1} \oplus yy_{n+1} \in \overline{C}$, διότι από τη (ii), $z \in C$ και $\bigoplus_{i=1}^{n}(x_i \oplus y_i) = \bigoplus_{i=1}^{n} z_i$.

Επομένως ισχύουν οι (i),(ii) και για τον $\overline{C}$, οπότε ο κώδικας $\overline{C}$ είναι γραμμικός.

**Άσκηση 7**

Να βρείτε ένα γεννήτορα πίνακα για ένα δυαδικό $[8, 4, 4]$ κώδικα.

Γνωρίζουμε πως ο πίνακας ισοτιμίας $H$ εγγυάται ότι ο κώδικας θα έχει $d_{min} = 4$, εάν ο ελάχιστος αριθμός των γραμμικώς εξαρτημένων στηλών του $mld(H)$ είναι ίσος με 4. Επομένως, αρκεί να κατασκευάσουμε τον $4 \times 8$ πίνακα $H$, έτσι ώστε οι στήλες του ανα τρεις να είναι γραμμικά ανεξάρτητες.
Ξεκινάμε την κατασκευή του $H$, θεωρώντας ως 1η στήλη του, μία από τις $2^4 - 1 = 15$ μή μηδενικές τετράδες του $\mathbb{F}_2^4$, έστω τη $(1, 0, 0, 0)^T$ και ως 2η μία από τις υπόλοιπες 14, έστω τη $(0, 1, 0, 0)^T$. Συμβολίζοντας ως $H_s$ το σύνολο των ήδη επιλεγμένων τετράδων θα έχουμε

$$H_s = \{(1, 0, 0, 0)^T, (0, 1, 0, 0)^T\}$$

ενώ εάν ως $H_{us}$ συμβολίσουμε το σύνολο των προς επιλογή τετράδων ισχύει

$$H_{us} = \mathbb{F}_2^4 - H_s - H_r$$

όπου $H_r$ είναι το σύνολο των τετράδων που απορρίπτονται κάθε φορά όπως θα δούμε αμέσως πιο κάτω. Για την ώρα

$$H_r = \{(0, 0, 0, 0)^T\}.$$

Κάθε φορά που επιλέγουμε μια στήλη του $H_s$ την αφαιρούμε από το $H_{us}$. Για να συνεχίσουμε πρέπει να αφαιρέσουμε (απορρίψουμε) από το σύνολο των προς επιλογή

τετράδων, εκείνες που προκύπτουν από το γραμμικό συνδυασμό των 2 στηλών που έχουν ήδη επιλεγεί, αφού απαιτείται οι στήλες του $H$ να είναι ανα τρείς γραμμικά ανεξάρτητες (δηλ. καμία από τις τρείς να μή γράφεται ως γραμμικός συνδυασμός των δύο άλλων). Η τετράδα που αφαιρείται είναι η $(1,1,0,0)^T$. Συμβολίζοντας, όπως είπαμε, ως $H_r$ το σύνολο των τετράδων που κάθε φορά απορρίπτονται έχουμε ότι

$$H_r = \{(0,0,0,0)^T, (1,1,0,0)^T\}.$$

Συνεχίζουμε επιλέγοντας μία από τις τετράδες του $H_{us}$, έστω τη $(0,0,1,0)^T$. Οπότε

$$H_s = \{(1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T\}$$

και αφαιρούμε από το σύνολο $H_{us}$ τις τετράδες που προκύπτουν ως γραμμικός συνδυασμός της νέας στήλης με μία εκ των στηλών του $H_s$ που είχαν εισαχθεί σε προηγούμενα βήματα. Ταυτόχρονα εισάγουμε τις αφαιρεθείσες τετράδες στο $H_r$. Αυτές είναι οι $(1,0,1,0)^T$, $(0,1,1,0)^T$ οπότε

$$H_r = \{(0,0,0,0)^T, (1,1,0,0)^T, (1,0,1,0)^T, (0,1,1,0)^T\}$$

Στο επόμενο βήμα επιλέγουμε για παράδειγμα την τετράδα $(1,1,1,0)^T$ από το $H_{us}$. Αφαιρώντας όπως πριν από το $H_{us}$ (και εισάγοντας στο $H_r$) τις τετράδες που αποτελούν γραμμικό συνδυασμό της $(1,1,1,0)^T$ με κάθε μια από τις υπόλοιπες στήλες του $H_s$ έχουμε:

$$H_s = \{(1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (1,1,1,0)^T\}$$

$$H_r = \{(0,0,0,0)^T, (1,1,0,0)^T, (1,0,1,0)^T, (0,1,1,0)^T\}$$

δηλ. οι τετράδες που προκύπτουν ως γραμμικός συνδυασμός της $(1,1,1,0)^T$ με τις υπόλοιπες στήλες του $H_s$, έχουν αφαιρεθεί ήδη από το $H_{us}$. Επιλέγοντας $(1,1,0,1)$:

$$H_s = \{(1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (1,1,1,0)^T, (1,1,0,1)^T\}$$

$$H_r = \left\{ \begin{array}{l} (0,0,0,0)^T, (1,1,0,0)^T, (1,0,1,0)^T, (0,1,1,0)^T \\ (1,0,0,1)^T, (0,1,0,1)^T, (0,0,1,1)^T, (1,1,1,1)^T \end{array} \right\}$$

$$H_{us} = \{(0,0,0,1)^T, (0,1,1,1)^T, (1,0,1,1)^T\}.$$

Σ΄ αυτό το σημείο, παρατηρούμε ότι εάν κατά τη συνέχιση της διαδικασίας απορριφθεί κάποια από τις τετράδες του $H_{us}$ ως γραμμικός συνδυασμός 2 στηλών του $H_s$, δεν υπάρχει τρόπος να κατασκευάσουμε τον $H$ ως ένα $4 \times 8$ πίνακα ανεξαρτήτων ανά τρεις τετράδων, ή αλλιώς δε μπορούμε να κατασκευάσουμε γραμμικό $[8,4,4]$ κώδικα. Κάτι τέτοιο δεν ισχύει στη συγκεκριμένη περίπτωση οπότε επιλέγοντας διαδοχικά

τις τετράδες $(0,0,0,1)^T$, $(0,1,1,1)^T$, $(1,0,1,1)^T$, προκύπτει η τελική κατάσταση των συνόλων:

$$H_s = \left\{ \begin{array}{l} (1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (1,1,1,0)^T \\ (1,1,0,1)^T, (0,0,0,1)^T, (0,1,1,1)^T, (1,0,1,1)^T \end{array} \right\}$$

$$H_r = \left\{ \begin{array}{l} (0,0,0,0)^T, (1,1,0,0)^T, (1,0,1,0)^T, (0,1,1,0)^T \\ (1,0,0,1)^T, (0,1,0,1)^T, (0,0,1,1)^T, (1,1,1,1)^T \end{array} \right\}$$

$$H_{us} = \emptyset.$$

Επομένως

$$H = \left[ \begin{array}{cccccccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right].$$

Με ανακατανομή στηλών προκύπτει η κανονική μορφή του $H$:

$$H = \left[ \begin{array}{cccccccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \right].$$

Οπότε

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

είναι ένας πίνακας γεννήτορας του κώδικα και μάλιστα σε κανονική μορφή.