Φυλλάδιο 1^o

Άσκηση 1

(i) Αν ένας κώδικας C ως προς το σώμα $\mathbb{F}_3$ είναι τύπου $(3, M, 2)$, τότε $M \leq 9$.

(ii) Αποδείξτε ότι υπάρχει ένας $(3, 9, 2)$ κώδικας ως προς το $\mathbb{F}_3$.

(iii) Γενικεύστε τα αποτελέσματα των (i) (ii) σε $(3, M, 2)$ κώδικες ως προς το σώμα $\mathbb{F}_q$.

(iv) Αποδείξτε ότι $A_q(3, 2) = q^2$.

(iii),(iv) Από το φράγμα Singleton $M \leq q^{n-d+1}$ δηλ. $M \leq q^{3-2+1} = q^2$. Για να ισχύει $A_q(3, 2) = q^2$ πρέπει να δειχθεί ότι υπάρχει κώδικας $(3, M, 2)$ με $M = q^2$. Έστω κώδικας $C = \{xx_3 : x = x_1x_2 \in \mathbb{F}_q^2$ και $x_3 = x_1 \otimes x_2\}$, όπου $\otimes$ είναι η πρόσθεση $modulo - q$. Ισχύει ότι

$$|C| = \left|\mathbb{F}_q^2\right| = q^2$$

Γνωρίζουμε επίσης ότι $\forall x, y \in \mathbb{F}_q^2$, $d(x, y) \geq 1$. θεωρούμε δύο κωδικές λέξεις $xx_3, yy_3 \in C$ για τις οποίες ισχύει $d(x, y) = 1$, γεγονός που συνεπάγεται ότι

$$x_1 \oplus x_2 \oplus y_1 \oplus y_2 = 1$$

και

$$d(xx_3, yy_3) = \sum_{i=1}^{2} x_i \oplus y_i + x_1 \oplus x_2 \oplus y_1 \oplus y_2 = 1 + 1 = 2$$

Άρα $d_{min}(C) = 2$ και ο C είναι ένας $(3, q^2, 2)$ κώδικας. Επομένως $A_q(3, 2) = q^2$. Θέτοντας $q = 3$ προκύπτουν όμοια οι απαντήσεις στα υποερωτήματα (i),(ii).

Άσκηση 2

Έστω E_n το σύνολο όλων των διανυσμάτων του $\mathbb{F}_2^n$ τα οποία έχουν *άρτιο* βάρος. Να αποδείξετε ότι το E_n είναι ο κώδικας C που προκύπτει προσθέτοντας παντού το σύμβολο ελέγχου ισοτιμίας (parity check) στον κώδικα $\mathbb{F}_2^{n-1}$. Να συμπεράνετε ότι ο E_n είναι ένας $(n, 2^{n-1}, 2)$ κώδικας.

Από την εκφώνηση

$$C = \left\{ xx_n : x = x_1 x_2 \ldots x_{n-1} \in \mathbb{F}_2^{n-1} \text{ και } x_n = \bigoplus_{i=1}^{n-1} x_i \right\}$$

όπου

$$\bigoplus_{k=1}^{n} x_k = x_1 \oplus x_2 \oplus \ldots \oplus x_n$$

Πρέπει να δείξουμε ότι $C = E_n$.

- Αποδεικνύουμε αρχικά ότι $C \subset E_n$. Για κάθε $xx_n \in C$ ισχύουν τα εξής

  (α) $w(xx_n) = w(x) + x_n$ και

  (β) εάν $x_n = 0 \Rightarrow w(x)$ άρτιος $\Rightarrow w(xx_n) = w(x) + 0$ άρτιος

  (γ) εάν $x_n = 1 \Rightarrow w(x)$ περιττός $\Rightarrow w(xx_n) = w(x) + 1$ άρτιος.

  Άρα σε κάθε περίπτωση ο $w(xx_n)$ είναι άρτιος οπότε $xx_n \in E_n$. Άρα $C \subset E_n$.

- Αποδεικνύουμε στη συνέχεια ότι $E_n \subset C$. Για κάθε $y = y_1 y_2 \ldots y_n \in E_n$ ισχύει ότι $w(y)$ άρτιος. Επομένως

  (α) εάν $y_n = 0 \Rightarrow w(y_1 y_2 \ldots y_{n-1})$ άρτιος $\Rightarrow \bigoplus_{i=1}^{n-1} y_i = 0$

  (β) εάν $y_n = 1 \Rightarrow w(y_1 y_2 \ldots y_{n-1})$ περιττός $\Rightarrow \bigoplus_{i=1}^{n-1} y_i = 1.$

  Άρα για κάθε $y \in E_n$ ισχύει ότι $\bigoplus_{i=1}^{n-1} y_i = y_n$ δηλ. $y \in C$. Οπότε $E_n \subset C$.

Από το γεγονός ότι $E_n = C$ έχουμε

$$|E_n| = |C| = \left|\mathbb{F}_2^{n-1}\right| = 2^{n-1}$$

Επίσης $\forall x, y \in \mathbb{F}_2^{n-1}$, $d(x,y) \geq 1$. θεωρούμε δύο κωδικές λέξεις $xx_n, yy_n \in C$ για τις οποίες ισχύει $d(x,y) = 1$, γεγονός που συνεπάγεται ότι

$$\bigoplus_{i=1}^{n-1}(x_i \oplus y_i) = \bigoplus_{k=1}^{n-2} 0 + 1 = 1$$

και

$$d(xx_n, yy_n) = \sum_{i=1}^{n-1} x_i \oplus y_i + \bigoplus_{i=1}^{n-1}(x_i \oplus y_i) = 1 + 1 = 2$$

Άρα $d_{min}(C) = 2$ και ο C είναι ένας $(n, 2^{n-1}, 2)$ κώδικας.

Άσκηση 3

Αν οι παράμετροι ενός block design είναι $(b, u, r, \kappa, \lambda)$, τότε να αποδείξετε ότι

(i) $b\kappa = ur$

(ii) $r(\kappa - 1) = \lambda(u - 1)$

Ακολουθούν τα blocks ενός $(11, 5, 2)$ design:

{1,3,4,5,9}	{2,4,5,6,10}	{3,5,6,7,11}	{1,4,6,7,8}
{2,5,7,8,9}	{3,6,8,9,10}	{4,7,9,10,11}	{1,5,8,10,11}
{1,2,6,9,11}	{1,2,3,7,10}	{2,3,4,8,11}	

Να τα χρησιμοποιήσετε για να κατασκευάσετε έναν $(11, 24, 5)$ κώδικα.

(i) Συμβολίζοντας με Σ το συνολικό αριθμό σημείων όλων των blocks ισχύουν οι παρακάτω σχέσεις:

$$\Sigma = (\text{αριθμός σημείων/block})(\text{αριθμός blocks}) = \kappa b$$

και

$$\Sigma = (\text{αριθμός των blocks στα οποία εμφανίζεται κάθε σημείο})(\text{αριθμός σημείων}) \\ = ru$$

οπότε $b\kappa = ru$.

(ii) Παρατηρούμε ότι για κάθε σημείο x του design, $r\kappa$ είναι ο συνολικός αριθμός των σημείων που περιέχονται στα r blocks στα οποία εμφανίζεται το σημείο x του design. Αφαιρώντας τον αριθμό r των εμφανίσεων του x, προκύπτει ο συνολικός αριθμός Σ_x εμφάνισης όλων των σημείων $y \neq x$ στα blocks που εμφανίζεται το x:

$$\Sigma_x = r\kappa - r = r(\kappa - 1)$$

Από την άλλη γνωρίζουμε ότι το σημείο x εμφανίζεται από κοινού με το καθένα από τα υπόλοιπα $(u-1)$ σημεία του design σε λ blocks. Επομένως

$$\Sigma_x = \lambda(u-1)$$

οπότε $r(\kappa-1) = \lambda(u-1)$.

Για το $(11, 5, 2)$ design της εκφώνησης ισχύει $b = 11$, $\kappa = 5$, $\lambda = 2$, $u = 11$ και $r = \dfrac{\kappa b}{u} = \dfrac{5 \cdot 11}{11}$, ενώ ο 11×11 incidence πίνακας $A = [a_{ij}]$ του design είναι 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

Από το γεγονός ότι κάθε σημείο i εμφανίζεται σε $r = 5$ blocks προκύπτει ότι για κάθε γραμμή a_i του A ισχύει $w(a_i) = 5$. Επιπλέον, γνωρίζουμε ότι κάθε ζεύγος σημείων (i, j) εμφανίζεται σε ακριβώς $\lambda = 2$ blocks, bl_k και bl_l. Αυτό συνεπάγεται ότι ισχύει $a_{ik} = a_{jk} = a_{il} = a_{jl} = 1$ για τις θέσεις k,l των γραμμών a_i,a_j, ενώ υπάρχουν επιπλέον $2(5-2) = 6$ θέσεις m,για τις οποίες ισχύει $a_{im} \neq a_{jm}$. Άρα

$$d(a_i, a_j) = 6, \ \forall i, j \in \{1, 2, \ldots, 11\}, \ (i \neq j)$$

Σημειώνεται ότι στις υπόλοιπες $11 - 2 - 6 = 3$ θέσεις z ισχύει $a_{iz} = a_{jz} = 0$, ενώ οι θέσεις z μαζί με τις θέσεις k και l αποτελούν την τομή $a_i \cap a_j$ των δύο γραμμών.
Θεωρούμε επίσης τον πίνακα $B = [b_{ij}] = [1 \oplus a_{ij}]$ και τον κώδικα C που έχει ως κωδικές λέξεις τις γραμμές των A, B, το μηδενικό 1×11 διάνυσμα $\mathbf{0}$ και το συμπληρωματικό του διάνυσμα $\mathbf{1}$. Αφού κάθε γραμμή b_i του B προκύπτει από το συμπλήρωμα των στοιχείων της γραμμής a_i του A ισχύει ότι $d(a_i, b_i) = 11$. Αν b_i, b_j είναι οι γραμμές του B που προκύπτουν από τις γραμμές a_i, a_j του A αντίστοιχα τότε

- στις δύο θέσεις k, l για τις οποίες ισχύει $a_{ik} = a_{jk} = a_{il} = a_{jl} = 1$ ισχύει $b_{ik} = b_{jk} = b_{il} = b_{jl} = 0$
- στις έξι θέσεις m για τις οποίες ισχύει $a_{im} \neq a_{jm}$, ισχύει $b_{im} \neq b_{jm}$
- στις τρείς θέσεις z για τις οποίες ισχύει $a_{iz} = a_{jz} = 0$, ισχύει ότι $b_{iz} = b_{jz} = 1$.

Άρα

$$d(b_i, b_j) = 6,\ \forall i, j \in \{1, 2, \ldots, 11\},\ (i \neq j)$$

Τέλος, θεωρούμε τις γραμμές a_i του A και $b_j = \mathbf{1} \oplus a_j$ του B για $i \neq j$ και $1 \leq i, j \leq 11$. Έχουμε ότι

- στις δύο θέσεις k, l για τις οποίες ισχύει $a_{ik} = a_{jk} = a_{il} = a_{jl} = 1$ ισχύει $a_{ik} \neq b_{jk}$, $a_{il} \neq b_{jl}$
- στις έξι θέσεις m για τις οποίες ισχύει $a_{im} \neq a_{jm}$, ισχύει $a_{im} = b_{jm}$
- στις τρείς θέσεις z για τις οποίες ισχύει $a_{iz} = a_{jz} = 0$, ισχύει ότι $a_{iz} \neq b_{jz}$

οπότε

$$d(a_i, b_j) = 3 + 2 = 5,\ \forall i, j \in \{1, 2, \ldots, 11\},\ (i \neq j)$$

Επίσης $d(a_i, \mathbf{0}) = d(b_i, \mathbf{1}) = 5$ και $d(a_i, \mathbf{1}) = d(b_i, \mathbf{0}) = 6$. Άρα $d_{min}(C) = 5$, ενώ $|C| = 24$ και $n = 11$, δηλ. ο C είναι ένας $(11, 24, 5)$ κώδικας.