ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
Θεωρία Πληροφορίας και Κωδικοποίησης
Φθινόπωρο 2002

2^{η} σειρά ασκήσεων

1. Αν H, G οι πίνακες ελέγχου ισοτιμίας και γεννήτορας πίνακας αντίστοιχα ενός κώδικα C, να αποδείξετε ότι:

$$G \cdot H^T = 0 \text{ και } H \cdot G^T = 0$$

Για κάθε γραμμή $\mathbf{g_i}$ του G, $(1 \leq i \leq k)$ ισχύει:

$$H\mathbf{g_i}^T = 0 \tag{1}$$

διότι οι $\mathbf{g_i}$ αποτελούν κωδικές λέξεις του C. Γράφοντας για όλες τις γραμμές του G την (1) σε μορφή πινάκων προκύπτει

$$HG^T = 0.$$

'Αναστρέφοντας' και τα δύο μέλη της (1), έχουμε

$$\mathbf{g_i}H^T = 0$$

για κάθε γραμμή του G. Επομένως

$$GH^T = HG^T = 0.$$

2. Αν H ο πίνακας ελέγχου ισοτιμίας και G ο γεννήτορας πίνακας, κώδικα C, να αποδείξετε ότι ο G είναι πίνακας ελέγχου ισοτιμίας και ο H γεννήτορας πίνακας του δυϊκού κώδικα $C^{\perp}$.

Για κάθε $x \in C^{\perp}$, $y \in C$ ισχύει

$$x \cdot y^T = y \cdot x^T = 0.$$

Επομένως και για τις γραμμές $\mathbf{g_i}$ του G, $(1 \leq i \leq k)$, οι οποίες είναι κωδικές λέξεις του C, ισχύει

$$\mathbf{g_i} \cdot x^T = 0$$

για κάθε $x \in C^{\perp}$. Σε μορφή πινάκων η παραπάνω σχέση γράφεται

$$Gx^T = 0,\ \forall x \in C^{\perp}. \tag{2}$$

Επομένως ο πίνακας G είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα $C^{\perp}$.

Η εξίσωση (2) συνεπάγεται:

$$xG^T = 0,\ \forall x \in C^{\perp}. \tag{3}$$

Γνωρίζουμε πως η (3) ισχύει για κάθε γραμμή του H, $\mathbf{h_j}$, $(1 \leq j \leq n-k)$. Αυτό διότι $HG^T = 0$. Επομένως όλες οι γραμμές $\mathbf{h_j}$, ανήκουν στον κώδικα $C^{\perp}$ και ως $(n-k)$ γραμμικώς ανεξάρτητα διανύσματα, παράγουν τον κώδικα $C^{\perp}$. Άρα ο H είναι ο γεννήτορας πίνακας του $C^{\perp}$.

3. Να συγκρίνετε τα φράγματα Hamming, Singleton, Gilbert - Varshamov και Plotkin για δυαδικό κώδικα C όταν $[n,d] = [7,5], [8,5], [15,9]$.

   Για τον $[7,5]$ κώδικα έχουμε για τον αριθμό κωδικών λέξεων $M = 2^k$:

   - Από το φράγμα Hamming:

     $$M \leq \frac{2^7}{1 + \binom{7}{1} + \binom{7}{2}}$$

     δηλ. $M \leq 4$ ή $k \leq 2$.

   - Από το φράγμα Singleton:

     $$M \leq 2^{7-5+1}$$

     δηλ. $M \leq 8$ ή $k \leq 3$.

   - Από το φράγμα Gilbert - Varshamov:

     $$2^k < \frac{2^7}{1 + \binom{6}{1} + \binom{6}{2} + \binom{6}{3}}$$

     δηλ. $2^k < 3$ ή $k \leq 1,\ M \leq 2$.

   - Τέλος, από το φράγμα Plotkin έχουμε:

     $$M \leq \frac{2d}{2d-n}$$

     οπότε για $n = 7$, $d = 5$:

     $$M \leq 3.03 \text{ ή } 2^k \leq 3.03 \text{ δηλ. } k = 1.$$

Άρα, όπως προκύπτει από τα δύο τελευταία φράγματα, υπάρχει οπωσδήποτε κώδικας $[7, 1, 5]$.

Με όμοιο τρόπο για το γραμμικό κώδικα $[8, 5]$ έχουμε:

- από το φράγμα Hamming, $M \leq 6$ ή $k \leq 2$,
- από το φράγμα Singleton, $M \leq 2^4$ ή $k \leq 4$,
- από το φράγμα Gilbert - Varshamov, $2^k < 4$ ή $k < 2$ και
- από το φράγμα Plotkin $M \leq 5$ ή $k \leq 2$.

Άρα, λόγω του φράγματος Gilbert - Varshamov, υπάρχει οπωσδήποτε $[8, 1, 5]$ κώδικας.

Για το γραμμικό κώδικα $[15, 9]$ έχουμε:

- από το φράγμα Hamming, $M \leq 16$ ή $k \leq 4$,
- από το φράγμα Singleton, $M \leq 2^7$ ή $k \leq 7$,
- από το φράγμα Gilbert - Varshamov, $2^k < 3.3$ ή $k \leq 1$ και
- από το φράγμα Plotkin $M \leq 6$, ή $k \leq 2$.

Άρα, λόγω του φράγματος Gilbert - Varshamov, υπάρχει οπωσδήποτε κώδικας $[15, 1, 9]$.

4. Να αποδείξετε ότι σε γραμμικό δυαδικό κώδικα C, όλες οι λέξεις έχουν άρτιο βάρος ή οι μισές άρτιο και οι μισές περιττό.

Έστω ότι ο γραμμικός κώδικας C περιλαμβάνει μία ή περισσότερες κωδικές λέξεις με περιττό βάρος. Ορίζουμε τη διαμέριση του C σε δύο υποσύνολα C_{odd}, και C_{even} ως εξής:

$$C_{odd} = \{x \in C : w(x) \text{ περιττός}\}$$

$$C_{even} = \{x \in C : w(x) \text{ άρτιος}\}.$$

Προφανώς $C_{odd} \cap C_{even} = \emptyset$ και $C_{odd} \cup C_{even} = C$ οπότε

$$|C_{odd}| + |C_{even}| = |C| \tag{4}$$

Γνωρίζουμε επίσης πως ισχύει γενικότερα για την απόσταση των $u,\ v \in \mathbb{F}_2^k$ και ειδικότερα στους γραμμικούς κώδικες και για το $w(u \oplus v)$ ότι:

$$w(u \oplus v) = d(u, v) = w(u) + w(v) - 2w(u \cap v) \tag{5}$$

όπου $u \cap v = \{u_i, v_i : u_i = v_i,\ i \in \{1, 2, \ldots, k\}\}$. Για να αποδείξουμε ότι $C_{odd} = C_{even}$, θεωρούμε συνάρτηση $f : C_{even} \to C_{odd}$:

$$\forall a \in C_{even},\ f(a) = a \oplus x$$

όπου x είναι μια τυχαία λέξη του C_{odd}. Το ότι $\forall a \in C_{even} f(a) \in C_{odd}$, προκύπτει αφενός από την (5), διότι $w(a)$ άρτιος και $w(x)$ περιττός και αφετέρου από την κλειστότητα του C ως προς την πράξη $\oplus$. Η συνάρτηση f είναι $1-1$:

$$\forall a_1, a_2 \in C_{even} \text{ με } f(a_1) = f(a_2) \Longleftrightarrow (a_1 \oplus x) = (a_2 \oplus x) \Longleftrightarrow a_1 = a_2.$$

Επίσης η f είναι επί. Υποθέτοντας ότι δεν είναι, υπάρχει $b \in C_{odd} : (a \oplus x) \neq b$, $\forall a \in C_{even}$. Δηλ.

$$\forall a \in C_{even},\ (x \oplus b) \neq a \Longrightarrow (x \oplus b) \notin C_{even}.$$

Από την (5) όμως προκύπτει ότι το $(x \oplus b)$ δε μπορεί να ανήκει ούτε στο C_{odd}, διότι $w(x \oplus b)$ άρτιος, εφόσον $w(x)$, $w(b)$ περιττοί. Άρα $(x \oplus b) \notin C$, άτοπο διότι ο C είναι γραμμικός.

Επομένως υπάρχει συνάρτηση f, $1-1$ και επί, από το C_{even} στο C_{odd} και άρα

$$|C_{even}| = |C_{odd}|.$$

Αντικαθιστώντας την τελευταία σχέση στην (4) έχουμε:

$$|C_{even}| = |C_{odd}| = \frac{|C|}{2}.$$

Η απόδειξη ξεκίνησε υποθέτοντας ότι υπάρχει τουλάχιστο μια κωδική λέξη του C με περιττό βάρος. Αν δεν υπάρχει ούτε μία, τότε όλες οι κωδικές λέξεις έχουν άρτιο βάρος και δεν υπάρχει κάτι προς απόδειξη.

5. Αν C δυαδικός (n, M, d) κώδικας όπου $n < 2 \cdot d$ να αποδείξετε ότι

$$M \leq \begin{cases} \frac{2d}{2d-n} & \text{, όταν ο M άρτιος} \\ \frac{2d}{2d-n} - 1 & \text{, όταν ο M περιττός} \end{cases}$$

6. Ο γεννήτορας πίνακας κώδικα C είναι ο

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

Να τον γράφετε στην κανονική του μορφή.

Με πρόσθεση της 1ης και 4ης γραμμής του G και αποθήκευση του αποτελέσματος στην 1η γραμμή προκύπτει ο πίνακας

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

Με πρόσθεση της 3ης και 4ης γραμμής του G_1 και αποθήκευση του αποτελέσματος στην 4η γραμμή προκύπτει ο πίνακας

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

Με πρόσθεση της 1ης και 2ης γραμμής του G_2 και αποθήκευση του αποτελέσματος στην 1η γραμμή προκύπτει ο πίνακας

$$G_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Εκτελώντας τις διαδοχικές μεταθέσεις στηλών του G_3 $(1,4)$, $(3,4)$, $(2,3)$, $(2,5)$, προκύπτει ο πίνακας

$$G_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

ο οποίος αποτελεί την κανονική μορφή του G.

7. Αν G_1, G_2 γεννήτορες πίνακες δύο γραμμικών (n_1, k, d_1) και (n_2, k, d_2) κωδίκων αντιστοίχως, να αποδείξετε ότι οι κώδικες με γεννήτορα πίνακα

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

$$G' = [G_1,\, G_2]$$

είναι του τύπου $(n_1+n_2, 2\cdot k, min\{d_1,d_2\})$ και (n_1+n_2,k,d) αντίστοιχα, όπου $d \geq d_1+d_2$.

Έστω C_1, C_2 οι γραμμικοί κώδικες με γεννήτορες πίνακες G_1, G_2 αντίστοιχα και C ο κώδικας με γεννήτορα τον πίκακα G. Ο κώδικας C είναι γραμμικός διότι θέτοντας για τις γραμμές του G:

$$\bigoplus_{i=1}^{k}\lambda_i(\mathbf{g_i^1},\mathbf{0}_{n_2}) \oplus \bigoplus_{j=1}^{k}\mu_j(\mathbf{0}_{n_1},\mathbf{g_j^2}) = \left(\bigoplus_{i=1}^{k}\lambda_i\mathbf{g_i^1}, \bigoplus_{j=1}^{k}\mu_j\mathbf{g_j^2}\right) = (\mathbf{0}_{n_1},\mathbf{0}_{n_2}) = \mathbf{0}_{n_1+n_2}$$

προκύπτει ότι θα πρέπει να ισχύει:

$$\bigoplus_{i=1}^{k}\lambda_i\mathbf{g_i^1} = \mathbf{0}_{n_1} \text{ και } \bigoplus_{j=1}^{k}\mu_j\mathbf{g_j^2} = \mathbf{0}_{n_2} \tag{6}$$

όπου $\mathbf{g_i^1}$, $\mathbf{g_j^2}$ είναι οι γραμμές των G_1, G_2 αντίστοιχα και λ_i, $\mu_j \in \mathbb{F}_2$ για $1 \leq i,j \leq k$. Λόγω της γραμμικής ανεξαρτησίας των γραμμών του καθενός από τους G_1, G_2 ισχύει από την (6) ότι

$$\lambda_i = \mu_j = 0,\ \forall i,\ j \in \{1,2,\dots,k\}.$$

Επομένως οι $2k$ γραμμές του G είναι γραμμικά ανεξάρτητες, δηλ. αποτελούν βάση του C και άρα ο C είναι γραμμικός κώδικας μήκους n_1+n_2 και διάστασης $2k$.

Για κάθε a, $b \in \mathbb{F}_2^k$ ισχύει ότι

$$z = (x,y) = (aG_1, bG_2) \in C \tag{7}$$

οπότε

$$w(z) = w(x) + w(y) = w(aG_1) + w(bG_2) \tag{8}$$

ενώ λόγω γραμμικότητας

$$d_{min}(C) = \min\{w(z) : z \in C,\ z \neq \mathbf{0}_{n_1+n_2}\} \tag{9}$$

Υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι $d_1 \leq d_2$. Τότε θέτοντας $b = \mathbf{0}_k$ και a τέτοιο ώστε $w(x = aG_1) = w_{min}(C - \mathbf{0}_{n_1}) = d_1$, έχουμε μέσω των (7) (8), ότι $z \neq \mathbf{0}_{n_1+n_2}$ και

$$w(z) = w(x) + w(y) = w(aG_1) + w(\mathbf{0}_{n_2}) = w(aG_1) = d_1 = \min\{d_1,d_2\}$$

Προφανώς για κάθε $z' = (x',y') \neq z$, με $z' \neq \mathbf{0}_{n_1+n_2}$, ισχύει από την (8) ότι

$$w(z') = w(x') + w(y') \geq w(x) = w(z)$$

οπότε μέσω της (9)

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

Επομένως ο κώδικας C είναι ένας $[n_1 + n_2, 2k, min\{d_1, d_2\}]$ κώδικας.

Ο κώδικας C' που παράγεται από τον πίνακα G' είναι επίσης γραμμικός διότι θέτοντας για τις γραμμές του G':

$$\bigoplus_{i=1}^{k} \lambda_i(\mathbf{g_i^1}, \mathbf{g_i^2}) = \left(\bigoplus_{i=1}^{k} \lambda_i \mathbf{g_i^1}, \bigoplus_{i=1}^{k} \lambda_i \mathbf{g_i^2} \right) = (\mathbf{0}_{n_1}, \mathbf{0}_{n_2}) = \mathbf{0}_{n_1+n_2}$$

προκύπτει ότι θα πρέπει να ισχύει:

$$\bigoplus_{i=1}^{k} \lambda_i \mathbf{g_i^1} = \mathbf{0}_{n_1} \text{ και } \bigoplus_{j=1}^{k} \lambda_i \mathbf{g_i^2} = \mathbf{0}_{n_2} \tag{10}$$

όπου $\mathbf{g_i^1}$, $\mathbf{g_i^2}$ είναι οι γραμμές των G_1, G_2 αντίστοιχα και $\lambda_i \in \mathbb{F}_2$ για $1 \leq i \leq k$. Λόγω της γραμμικής ανεξαρτησίας των γραμμών του καθενός από τους G_1, G_2 ισχύει από τη (10) ότι

$$\lambda_i = 0, \ \forall i \in \{1, 2, \ldots, k\}.$$

Επομένως οι k γραμμές του G' είναι γραμμικά ανεξάρτητες, δηλ. αποτελούν βάση του C' και άρα ο C' είναι γραμμικός κώδικας μήκους $n_1 + n_2$ και διάστασης k.

Για κάθε $a \in \mathbb{F}_2^k$ ισχύει ότι

$$z = (x, y) = (aG_1, aG_2) \in C' \tag{11}$$

οπότε

$$w(z) = w(x) + w(y) = w(aG_1) + w(aG_2) \tag{12}$$

ενώ λόγω γραμμικότητας

$$d_{min}(C') = \min\{w(z) : z \in C', \ z \neq \mathbf{0}_{n_1+n_2}\} \tag{13}$$

Για κάθε $a \neq \mathbf{0}_k$ ισχύει:

$$x = aG_1 \neq \mathbf{0}_{n_1} \text{ και } y = aG_2 \neq \mathbf{0}_{n_2}$$

οπότε για $z = (x, y)$ έχουμε από τη (12) ότι:

$$w(z) = w(x) + w(y) \geq d_1 + d_2$$

ενώ εάν $a = \mathbf{0}_k$, από την (11) συνεπάγεται ότι $z = \mathbf{0}_{n_1+n_2}$. Επομένως για κάθε $z \neq \mathbf{0}_{n_1+n_2}$, ισχύει $w(z) \geq d_1 + d_2$ (με την ισότητα να ισχύει εφόσον $w(aG_1) = d_1$ και $w(aG_2) = d_2$, για το ίδιο $a \in \mathbb{F}_2^k$) και από τη (13) $d_{min}(C') \geq d_1 + d_2$. Άρα, ο κώδικας C' είναι ένας $[n_1 + n_2, k, d \geq d_1 + d_2]$ κώδικας.