ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
Κώδικες Διόρθωσης Λαθών
Φθινόπωρο 2003

Φυλλάδιο 5^o

1. Έστω C_1 ένας κώδικας ως προς το $\mathbb{F}_5$ με πίνακα γεννήτορα

$$G_1 = \begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix}$$

και C_2 ο κώδικας ως προς το σώμα $\mathbb{F}_3$ με πίνακα γεννήτορα

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

Να βρείτε έναν πίνακα ελέγχου ισοτιμίας για κάθε κώδικα και να υπολογίσετε την ελάχιστη απόσταση αυτού.

Σε ότι ακολουθεί η πράξη $a\Gamma_i+\Gamma_j = \Gamma_j$, αναφέρεται στον πολλαπλασιαμό των στοιχείων της γραμμής i ενός πίνακα επί το συντελεστή $a \in \mathbb{F}_q$, την πρόσθεση modulo-q των στοιχείων της γραμμής j του πίνακα στο αποτέλεσμα του πολλαπλασιασμού και την αποθήκευση της πρόσθεσης στη γραμμή j του πίνακα.

$$G_1 = \begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix} \sim^{2\Gamma_1+\Gamma_3=\Gamma_3} \begin{bmatrix} 1 & 2 & 4 & 0 & 3 \\ 0 & 2 & 1 & 4 & 1 \\ 0 & 1 & 0 & 1 & 3 \end{bmatrix} \sim^{\Gamma_2+\Gamma_1=\Gamma_1} \begin{bmatrix} 1 & 4 & 0 & 4 & 4 \\ 0 & 2 & 1 & 4 & 1 \\ 0 & 1 & 0 & 1 & 3 \end{bmatrix}$$

$$\sim^{\Gamma_3+\Gamma_1=\Gamma_1} \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 2 & 1 & 4 & 1 \\ 0 & 1 & 0 & 1 & 3 \end{bmatrix} \sim^{3\Gamma_3+\Gamma_2=\Gamma_2} \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 1 & 3 \end{bmatrix}$$

Με εναλλαγή των δύο τελευταίων γραμμών της τελευταίας μορφής του G_1 προκύπτει ο πίνακας

$$G_1' = \begin{bmatrix} 1 & 0 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 & 3 \\ 0 & 0 & 1 & 2 & 0 \end{bmatrix}$$

Άρα,

$$-A_1^T = \begin{bmatrix} 0 & 2 \\ 1 & 3 \\ 2 & 0 \end{bmatrix} \text{ οπότε } A_1 = \begin{bmatrix} 0 & 4 & 3 \\ 3 & 2 & 0 \end{bmatrix} \text{ και } H_1 = \begin{bmatrix} 0 & 4 & 3 & 1 & 0 \\ 3 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Παρατηρούμε ότι για παράδειγμα η 3η στήλη του H_1 είναι πολλαπλάσια της 4ης στήλης, οπότε $mld(H_1) = d_{min}(C_1) = 2$.

Για τον κώδικα C_2 έχουμε

$$G_2 = \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 2 & 0 & 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 \end{bmatrix} \sim^{\Gamma_1+\Gamma_2=\Gamma_2} \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 2 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 & 2 \end{bmatrix} \sim^{2\Gamma_1+\Gamma_3=\Gamma_3}$$

$$\begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 2 & 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 0 & 0 & 2 \end{bmatrix} \sim^{2\Gamma_2+\Gamma_3=\Gamma_3} \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 2 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{bmatrix} \sim^{2\Gamma_3+\Gamma_2=\Gamma_2} \begin{bmatrix} 1 & 2 & 0 & 2 & 1 & 0 \\ 0 & 2 & 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{bmatrix}$$

Με αντιμετάθεση της 2ης και 3ης στήλης της τελευταίας μορφής του G_2, προκύπτει ο πίνακας

$$G_{21} = \begin{bmatrix} 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 1 & 2 & 2 & 2 & 0 \\ 0 & 0 & 0 & 2 & 2 & 1 \end{bmatrix}$$

ενώ με αντιμετάθεση της 3ης και της 6ης στήλης του G_{21}, προκύπτει ο πίνακας

$$G_{22} = \begin{bmatrix} 1 & 0 & 0 & 2 & 1 & 2 \\ 0 & 1 & 0 & 2 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 & 0 \end{bmatrix}.$$

Επομένως,

$$-A_{22}^T = \begin{bmatrix} 2 & 1 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 0 \end{bmatrix} \text{ οπότε } A_{22} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

και

$$H_{22} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Ο πίνακας H_{22} είναι ο πίνακας ελέγχου ισοτιμίας του κώδικα C_{22} με γεννήτορα πίνακα τον G_{22}. Αν και οι δύο κώδικες είναι ισοδύναμοι, δεν είναι ίδιοι, αλλά διαφέρουν

ως προς τις κωδικές λέξεις τους, λόγω της αλλαγής στηλών κατά την εύρεση της κανονικής μορφής G_{22} του G_2. Για να βρούμε έναν πίνακα ελέγχου ισοτιμίας H_2του C_2, θα πρέπει να εκτελέσουμε αυτές τις μεταθέσεις με αντίστροφη σειρά, πάνω στον H_{22}. Αντιμεταθέτοντας την 3η με την 6η στήλη του H_{22} προκύπτει ο πίνακας

$$H'_{22} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 2 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

ενώ με αντιμετάθεση της 2ης με την 3η στήλη του H'_{22}, προκύπτει ο πίνακας ελέγχου ισοτιμίας

$$H_2 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

του C_2.

Παρατηρούμε ότι καμία από τις στήλες του H_2 δεν είναι πολλαπλάσια κάποιας άλλης, ενώ για παράδειγμα η 6η στήλη του είναι το άθροισμα της 4ης με την 5η στήλη. Επομένως $mld(H_2) = d_{min}(C_2) = 3$.

2. Ποιά είναι η ελάχιστη απόσταση του δυαδικού κώδικα C με γεννήτορα πίνακα

$$G = \left[\begin{array}{c|cccc} & 1 & 1 & 0 & 0 \\ & 1 & 0 & 1 & 0 \\ & 0 & 1 & 1 & 0 \\ \mathbf{I}_7 & 1 & 1 & 1 & 1 \\ & 1 & 1 & 0 & 1 \\ & 0 & 1 & 0 & 1 \\ & 1 & 0 & 0 & 1 \end{array}\right].$$

Ο κώδικας έχει πίνακα ελέγχου ισοτιμίας τον

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

Παρατηρούμε ότι καμία στήλη του H δεν εμφανίζεται δύο φορές, ενώ για παράδειγμα, η 1η στήλη είναι το άθροισμα της 8ης και 9ης στήλης του H. Επομένως $mld(H) = d_{min}(C) = 3$.

3. Να κατασκευάσετε ένα $[6, 3, 4]$ κώδικα ως προς το σώμα $\mathbb{F}_5$.

Όπως και στην Άσκηση 7 του 2ου φυλλαδίου, ο πίνακας ελέγχου ισοτιμίας H του κώδικα θα πρέπει να περιλαμβάνει ως στήλες, έξι διανύσματα του $\mathbb{F}_5^3$ τα οποία ανά τρία

να είναι γραμμικώς ανεξάρτητα μεταξύ τους. Για να έχουμε ακριβώς $d_{min} = 4$, θα πρέπει επιπλέον κάποιο από αυτά να προκύπτει ως ο γραμμικός συνδυασμός τριών από τις υπόλοιπες στήλες του H. Εργαζόμενοι όπως στην Άσκηση 7 του 2ου φυλλαδίου, κάθε φορά που επιλέγουμε μια τριάδα $\mathbf{a} \in \mathbb{F}_5^3 - \mathbf{0}_3$ ως στήλη του H, θα πρέπει να αφαιρούμε από το σύνολο των υπό επιλογή τριάδων

- τα πολλαπλάσια $\lambda\mathbf{a}$, $\forall\lambda \in \mathbb{F}_5$, και
- τα αθροίσματα $\mu\mathbf{h} + \lambda\mathbf{a}$, $\mu, \lambda \in \mathbb{F}_5$, για όλες τις τριάδες $\mathbf{h}$ που έχουν επιλεγεί πρίν το $\mathbf{a}$ ως στήλες του H.

Σύμφωνα με τα παραπάνω ο πίνακας ελέγχου ισοτιμίας του κώδικα θα μπορούσε να είναι ο

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 1 & 3 & 4 \end{bmatrix}$$

διότι οι στήλες του H είναι ανά τρείς γραμμικώς ανεξάρτητες ενώ το άθροισμα των τριών πρώτων στηλών του δίνει την τέταρτη και άρα $mld(H) = d_{min} = 4$.

4. Να γράψετε τον πίνακα ελέγχου ισοτιμίας του δυαδικού $[15, 11, 3]$ κώδικα Hamming. Να αποκωδικοποιήσετε τα διανύσματα

$$y_1 = \begin{bmatrix} 100 & 000 & 000 & 000 & 000 \end{bmatrix}$$

και

$$y_2 = \begin{bmatrix} 111 & 111 & 111 & 111 & 111 \end{bmatrix}.$$

Ο πίνακας ελέγχου ισοτιμίας H του κώδικα, θα περιλαμβάνει ως στήλες τα $2^4 - 1 = 15$ μή μηδενικά διανύσματα του $\mathbb{F}_2^4$, εξ ορισμού. Μπορούμε να κατασκευάσουμε τον πίνακα ελέγχου ισοτιμίας του κώδικα, έτσι ώστε κάθε μή μηδενικό σύνδρομο να αποτελεί το δυαδικό ισοδύναμο της θέσης στην οποία έχει γίνει λάθος, δηλ. της αντίστοιχης στήλης του H. Ο πίνακας ελέγχου ισοτιμίας σε αυτή τη μορφή είναι ο

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

Για τη λέξη y_1 έχουμε $Hy_1^T = (0, 0, 0, 1)^T$ δηλ. έχει γίνει λάθος στην 1η θέση της κωδικής λέξης x_1 που είχε σταλεί . Επομένως,

$$x_1 = y_1 \oplus (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) = y_1 \oplus y_1 = \mathbf{0}_{15}.$$

Για τη λέξη y_2 ισχύει $Hy_2^T = 0$ και άρα η y_2 είναι κωδική λέξη του κώδικα.

5. Θεωρήστε τον $[7,4,3]$ δυαδικό κώδικα Hamming. Κωδικοποιήστε τα μηνύματα

$$0\quad 1\quad 1\quad 0 \quad \text{και} \quad 1\quad 0\quad 1\quad 1\ .$$

Κωδικοποιήστε τα ίδια μηνύματα στον *επεκτεταμένο* Hamming $[8,4,4]$ κώδικα. Αποκωδικοποιήστε το

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

στον $[8,4,4]$.

Ένας πίνακας ελέγχου ισοτιμίας του δυαδικού $[7,4,3]$ κώδικα Hamming C είναι ο

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

οπότε ο γεννήτορας πίνακας του κώδικα C είναι ο

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

Οπότε

$$(0,1,1,0)G = (0,1,1,0,0,1,1) \text{ και } (1,0,1,1)G = (1,0,1,1,0,0,1)$$

είναι η κωδικοποίηση για το κάθε μήνυμα.

Στον επεκτεταμένο κώδικα Hamming τα δύο μηνύματα κωδικοποιούνται ως

$$(0,1,1,0,0,1,1,0) \text{ και } (1,0,1,1,0,0,1,0)$$

αντίστοιχα, δηλ. προσθέτοντας ως 8ο ψηφίο σε κάθε κωδική λέξη x του C, το αποτέλεσμα του ελέγχου ισοτιμίας για τη x. Γνωρίζουμε επίσης, πως ο πίνακας ελέγχου ισοτιμίας $\overline{H}$ του επεκτεταμένου κώδικα $\overline{C}$ είναι ο

$$\overline{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

οπότε $\overline{H}y^T = (1,1,1,1)^T$, άρα υπάρχει λάθος στην 1η θέση του y και η κωδική λέξη x που στάλθηκε είναι η

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