ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
Τμήμα Μαθηματικών και
Εφαρμοσμένων Μαθηματικών

Χειμερινό Εξάμηνο 2024-2025
Θεόδουλος Γαρεφαλάκης

Α32 – Κωδικοποίηση

Φυλλάδιο Ασκήσεων 4

Άσκηση 4.1 Έστω $\alpha = (a_1, \ldots, a_n) \in (\mathbb{F}_q^*)^n$, $a_i \neq a_j$ για $i \neq j$, $v = (v_1, \ldots, v_n) \in (\mathbb{F}_q^*)^n$, $a \in \mathbb{F}_q^*$ και $b \in \mathbb{F}_q$. Ονομάστε $\alpha' = (aa_1 + b, \ldots, aa_n + b)$. Δείξτε ότι $\mathrm{GRS}_k(\alpha, v) = \mathrm{GRS}_k(\alpha', v)$.
Υπόδειξη: Για κάθε $f \in \mathbb{F}_q[X]_{<k}$ βρείτε $g \in \mathbb{F}_q[X]_{<k}$, τέτοιο ώστε $f(a_j) = g(aa_j + b)$ για $j = 1, \ldots, n$.

Άσκηση 4.2 Έστω C ο GRS κώδικας με πίνακα βάσης

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}$$

και C_1 ο κώδικας με πίνακα βάσης

$$G_1 = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}.$$

(i) Δείξτε ότι κάθε $k-1$ στήλες του G_1 είναι γραμμικώς ανεξάρτητες.

(ii) Υπολογίστε τις παραμέτρους του $C_1^\perp$ και δείξτε ότι είναι MDS, άρα και ο C_1 είναι MDS.

Άσκηση 4.3 Έστω C ένας $[n, k, d]$-κώδικας πάνω από το $\mathbb{F}_q$ και $G \in \mathbb{F}_q^{k \times n}$ ένας πίνακας βάσης του. Έστω $R \subseteq [n]$ ένα υποσύνολο δεικτών με $|R| = r \geq n - d + 1$. Θεωρήστε την προβολή στις συντεταγμένες του R:

$$\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^r, \quad \pi(x_i)_{i \in [n]} = (x_i)_{i \in R}$$

και ονομάστε $C' = \pi(C)$.

(i) Δείξτε ότι ο C' έχει διάσταση k.

(ii) Δείξτε ότι ο πίνακας $G' \in \mathbb{F}_q^{k \times r}$ που αποτελείται από τις στήλες του G που αντιστοιχούν στο σύνολο R, είναι πίνακας βάσης του C' (και άρα έχει τάξη k).

(iii) Περιγράψτε πώς μπορείτε να διορθώσετε έως $d-1$ ereasures: Αν σας δοθεί ένα διάνυσμα του $(c_1, \ldots, c_n)$ του C, στο οποίο έχουν σβηστεί $t \leq d-1$ συντεταγμένες, περιγράψτε πώς μπορείτε να βρείτε τις σβησμένες συντεταγμένες.

Άσκηση 4.4 Θα κατασκευάσουμε ένα secret sharing scheme βασισμένο σε ένα q-αδικό $[n, k, d]$ κώδικα C με πίνακα βάσης G. Το μυστικό είναι το $s \in \mathbb{F}_q$.

1. Επιλέγουμε $(w_2, \ldots, w_k) \in \mathbb{F}_q^{k-1}$ τυχαία και θέτουμε $w = (s, w_2, \ldots, w_k)$.

2. Υπολογίζουμε το διάνυσμα του κώδικα $c = (c_1, \ldots, c_n) = wG$.

3. Τα μερίδια είναι τα $c_1, \ldots, c_n$.

Για την παρακάτω ανάλυση, θεωρήστε τον κώδικα C_1 με πίνακα βάσης G_1 που αποτελείται από της $k-1$ τελευταίες γραμμές του G (όλες εκτός της πρώτης γραμμής).

(i) Δείξτε ότι για οποιοδήποτε $R \subseteq [n]$ με $|R| \geq n - d + 1$, το σύνολο μεριδίων $\{c_j : j \in R\}$ αρκεί για να υπολογίσετε το μυστικό.

(ii) Δείξτε ότι για οποιοδήποτε $R \subseteq [n]$ με $|R| \leq d_1^{\perp} - 1$, το σύνολο μεριδίων $\{c_j : j \in R\}$ δεν δίνει καμία πληροφορία για το μυστικό, όπου $d_1^{\perp}$ είναι η ελάχιστη απόσταση του $C_1^{\perp}$.

(iii) Όταν ο C είναι ένας GRS με πίνακα βάσης τον

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{k-1} & a_2^{k-1} & \cdots & a_n^{k-1} \end{pmatrix},$$

τι παρατηρήτε για τις τιμές $n - d + 1$ και $d_1^{\perp} - 1$;

(iv) Τι εικάζετε ότι συμβαίνει για κώδικες οι οποίοι δεν είναι GRS και για σύνολα μεριδίων με $d_1^{\perp} \leq r \leq n - d$ μερίδια;