9. MDS κώδικες

Έστω C ένας γραμμικός (n, k, d)-κώδικας. Υπενθυμίζουμε το φράγμα του Singleton: $k \leq n - d + 1$. Επίσης, είχαμε ορίσει ως MDS-κώδικα έναν γραμμικό κώδικα για τον οποίο ισχύει η ισότητα στο φράγμα του Singleton. Δηλαδή, $k = n - d + 1$ ή αλλιώς $d = m + 1$ όπου $m = n - k$.

Συμβολισμός 9.1 $V(m, q) = (\mathbf{F}_q)^n$

Ορισμός 9.2 Ένα (n, s)-σύνολο του $V(m, q)$ είναι ένα σύνολο από n διανύσματα του $V(m, q)$ τέτοιο ώστε s οποιαδήποτε από αυτά να είναι γραμμικά ανεξάρτητα.

Έχουμε ήδη αναφέρει την

Πρόταση 9.3 Υπάρχει κώδικας C τύπου $(n, n - m, d)$ στο $\mathbf{F}_q$ ακριβώς τότε όταν υπάρχει ένα $(n, d - 1)$ σύνολο του $V(m, q)$.

Συμβολισμός 9.4 Το $\max_s(m, q)$ θα συμβολίζει τη μέγιστη τιμή του n για την οποία υπάρχει ένα (n, s)-σύνολο του $V(m, q)$. Ένα τέτοιο n θα λέγεται βέλτιστο.

Άμεση συνέπεια της πρότασης 9.3 είναι το

Πόρισμα 9.5 Αν μας δοθούν τα q, d και m τότε η μεγαλύτερη τιμή για το n έτσι ώστε να υπάρχει ένας $(n, n - m, d)$ κώδικας στο $\mathbf{F}_q$ είναι $\max_{d-1}(m, q)$.

Αν έχουμε τώρα έναν MDS-κώδικα $(n, n - m, d)$ στο $\mathbf{F}_q$ τότε το μέγιστο μήκος n του κώδικα σύμφωνα με το πόρισμα 9.5 είναι $\max_m(m, q)$. Δηλαδή, το μέγιστο μήκος ενός (n, m)-συνόλου στο $V(m, q)$.

Γνωστά αποτελέσματα υποβάλλουν την ανάγκη διατύπωσης της ακόλουθης εικασίας.

Εικασία 9.6 Έστω m με $2 \leq m \leq q$, $m \neq 3$. Ισχύει: $\max_m(m, q) = q + 1$.

Για $m = 3$ έχει αποδειχθεί ότι ισχύει $\max_3(3, q) = q + 2$.

Θα αποδείξουμε την εικασία κατ' αρχήν για $m = 2$. Θα αποδείξουμε δηλαδή ότι ισχύει:

$$\max_2(2, q) = q + 1. \quad (1)$$

Γενικότερα ισχύει η

Πρόταση 9.10 Δίδεται το m. Το μέγιστο μήκος n τέτοιο ώστε να υπάρχει $(n, n - m, 3)$-κώδικας ως προς το σώμα $\mathbf{F}_q$ είναι $n = \dfrac{q^m - 1}{q - 1}$.

Σημείωση 9.11 Αυτό σημαίνει ότι $\max_2(m, q) = \dfrac{q^m - 1}{q - 1}$.

Ειδικά για m = 2 έχουμε $\max_2(2, q) = \frac{q^2 - 1}{q - 1} = q + 1$ δηλαδή την (1).

Απόδειξη Σύμφωνα με το πόρισμα 9.5, αρκεί να αποδείξουμε ότι το n είναι η μεγαλύτερη τιμή ύπαρξης ενός (n, 2) – συνόλου στο V(m, g).

Ένα σύνολο S διανυσμάτων του V(m, g) είναι ένα (n, 2) – σύνολο τότε και μόνο τότε όταν δεν υπάρχει διάνυσμα στο S το οποίο να είναι scalar πολλαπλάσιο οποιουδήποτε άλλου διανύσματος του S. Τώρα θυμόμαστε, όταν γράφουμε τον τύπο … κωδίκων Hamming ότι εκεί τα $(q^m - 1)$ – μη μηδενικά διανύσματα του V(m, q) διαμερίζονται σε $\frac{q^m - 1}{q - 1}$ - κλάσεις, όπου κάθε κλάση περιέχει (q – 1) – διανύσματα τα οποία είναι scalar πολλαπλάσια το ένα του άλλου. Επομένως ένα (n, 2) – σύνολο μέγιστου μήκους – είναι ένα σύνολο $\frac{q^m - 1}{q - 1}$ διανυσμάτων. Παίρνουμε ένα από κάθε κλάση.

Ερώτημα Γιατί ξεκινάμε από m = 2;

Για m = 0 το V(n, q) είναι ένας (n, n – 1)-κώδικας για οποιοδήποτε n.

Για m = 1 ο πίνακας $\left[\begin{array}{c|c} I_{n-1} & \begin{matrix}1\\1\\\vdots\\1\end{matrix} \end{array}\right]$ είναι γεννήτορας ενός (n, n – 1, 2)-κώδικα για οποιοδήποτε n.

Εντελώς φυσικά προκύπτει και το επόμενο

Ερώτημα Τι γίνεται όταν m > q;

Απάντηση σ’ αυτό το ερώτημα δίνει η ακόλουθη

Πρόταση 9.12 Αν $m \geq q$ τότε $\max_m(m, q) = m + 1$ και κάθε MDS-κώδικας με $m \geq q$ είναι ισοδύναμος με κάποιον κώδικα επανάληψης μήκους m + 1.

Απόδειξη Ο κώδικας επανάληψης μήκους (m + 1) είναι του τύπου (m + 1, 1, m + 1) και έχει πίνακα γεννήτορα τον [11…1]. Επομένως, $\max_m(m, q) \geq m + 1$. Επίσης είναι σαφές ότι κάθε (m + 1, 1, m + 1) – κώδικας είναι ισοδύναμος με κάποιο κώδικα επανάληψης. Υποθέτουμε ότι $m \geq q$ και ότι $\max_m(m, q) \geq m + 2$. Τότε, σύμφωνα με τα προηγούμενα υπάρχει ένας (m + 2, 2, m + 1) – κώδικας C ως προς το σώμα $\mathbf{F}_q$. Ο κώδικας αυτός θα πρέπει να είναι ισοδύναμος με έναν κώδικα με γεννήτορα πίνακα της μορφής

$$G = \left[\begin{array}{cc|cccc} 1 & 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & a_1 & a_2 & \dots & a_m \end{array}\right]$$

Για να έχει κάθε γραμμικός συνδυασμός των γραμμών του πίνακα G βάρος τουλάχιστον (m + 1) θα πρέπει τα a_i να είναι διαφορετικά του μηδενός και διαφορετικά μεταξύ τους ανά δύο, στοιχεία του $\mathbf{F}_q$ από όπου έπεται ότι $m \leq q - 1$, άτοπο.

Άμεση συνέπεια της πρότασης 9.12 αλλά και άλλων στοιχείων στα οποία εμείς δεν αναφερθήκαμε είναι η ακόλουθη ταξινόμηση:

Οι μοναδικοί δυαδικοί MDS-κώδικες είναι:

- Ο $V(n, 2) = (\mathbf{F}_2)^n$, δηλαδή όλος ο χώρος.
- Ο κώδικας όλων των διανυσμάτων άρτιου βάρους του V(n, 2)
- Οι κώδικες επανάληψης

Χωρίς απόδειξη αναφέρουμε την

Πρόταση 9.13 Έστω m με $2 \leq m \leq q$ και $\mathbf{F}_q^* = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$. Ο πίνακας

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \ldots & \alpha_{q-1}^{m-1} & 0 & 1 \end{bmatrix}$$

είναι πίνακας ελέγχου ισοτιμίας ενός MDS-κώδικα τύπου $(q+1, q-1-m, m+1)$

Πόρισμα 9.14 Για m με $2 \leq m \leq q$ ισχύει $\max_m(m, q) \leq q + 1$.
Τέλος ισχύουν,

1. Ο δυικός MDS-κώδικα είναι επίσης MDS.
2. Υπάρχει MDS κώδικας τύπου $(n, n - m)$ ως προς το σώμα $\mathbf{F}_q$ ακριβώς τότε όταν υπάρχει MDS κώδικας τύπου (n, m).
3. Αν $q = 2^t$, $t > 1$ τότε υπάρχει $(q + 2, 3, q)$-κώδικας ως προς το σώμα $\mathbf{F}_q$.