8. Κώδικες τετραγωνικού υπολοίπου

Υποθέτουμε ότι n είναι ένας περιττός πρώτος αριθμός και q δύναμη πρώτου με ΜΚΔ(n, q) = 1. Επιπλέον υποθέτουμε ότι ο q είναι τετραγωνικό υπόλοιπο mod n.

Με U_0 θα συμβολίζουμε το σύνολο όλων των τετραγωνικών υπολοίπων mod n. Το U_0 είναι το σύνολο όλων των τετραγώνων της ομάδας $\mathbf{F}_q^*$.

Με U_1 θα συμβολίζουμε το σύνολο όλων των μη-τετραγωνικών υπολοίπων mod n. Το U_1 είναι το σύνολο όλων στοιχείων της ομάδας $\mathbf{F}_q^*$ που δεν είναι τετράγωνα άλλων στοιχείων.

Παράδειγμα Για n = 11 έχουμε ότι $\mathbf{F}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Βρίσκουμε τα τετραγωνικά υπόλοιπα mod n:

k	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\mathbf{k^2}$	1	4	9	5	3	3	5	9	4	1

Οπότε, $U_0 = \{1, 3, 4, 5, 9\}$ και $U_1 = \{2, 6, 7, 8, 10\}$

Θεωρούμε το σώμα $\mathbf{F}_{q^{n-1}}$. Η ομάδα $\mathbf{F}_{q^{n-1}}^*$ έχει $q^{n-1} - 1$ στοιχεία. Επειδή ΜΚΔ(n, q) = 1 ισχύει ότι $q^{n-1} \equiv 1 \bmod n$. Άρα το n διαιρεί το $q^{n-1} - 1$. Επομένως, υπάρχει $\zeta \in \mathbf{F}_{q^{n-1}}^*$ τέτοιο ώστε ord(ζ) = n. Το ζ αυτό λέγεται πρωταρχική n-ρίζα της μονάδας.

Στη συνέχεια ορίζουμε τα πολυώνυμα $g_0(X) = \prod_{i \in U_0} (X - \zeta^i)$ και $g_1(X) = \prod_{i \in U_1} (X - \zeta^i)$.
Τα U_0 και U_1 αποτελούνται από κυκλικά cosets, δηλαδή είναι γινόμενα ανάγωγων πολυωνύμων με συντελεστές από το σώμα $\mathbf{F}_q$. Επομένως, $g_0(X), g_1(X) \in \mathbf{F}_q[X]$.

Προφανώς, $X^n - 1 = \prod_{i=0}^{n-1} (X - \zeta^i) = (X - 1)\, g_0(X)\, g_1(X)$.

Ορισμός 8.1 Οι **κώδικες τετραγωνικού υπολοίπου** (QR-κώδικες) C_0^+, C_0, C_1^+, C_1 είναι κυκλικοί κώδικες με πολυώνυμο γεννήτορα $g_0(X)$, $(X - 1)\, g_0(X)$, $g_1(X)$, $(X - 1)\, g_1(X)$ αντίστοιχα.

Προφανώς, $C_0^+ \supseteq C_0$ και $C_1^+ \supseteq C_1$.

Αν q = 2, στο σώμα $\mathbf{F}_2$ ο πολλαπλασιασμός με X – 1 δίνει κώδικα όπου όλες οι λέξεις έχουν άρτιο βάρος. Δηλαδή ο C_0 είναι υποκώδικας του C_0^+ άρτιου βάρος. Ομοίως, ο C_1 είναι υποκώδικας του C_1^+ άρτιου βάρους.

Παράδειγμα 8.2 Αν n = 7 και q = 2. Έστω ζ ένας γεννήτορας του σώματος $\mathbf{F}_8 = \mathbf{F}_2[X] / \langle X^3 + X + 1 \rangle$. Τότε $\zeta^3 = \zeta + 1$ και $\zeta^7 = 1$. Έχουμε ότι $U_0 = \{1, 2, 4\}$ και $U_1 = \{3, 5, 6\}$. Οπότε $g_0 = (X - \zeta)(X - \zeta^2)(X - \zeta^4) = X^3 + X + 1$. Επομένως, ο

κώδικας C_0^+ είναι ο $C_0^+ = <g_0(X)>$.Είναι ο γνωστός μας (7, 4, 3)-Hamming κώδικας. Ο C_0 είναι ο υποκώδικας $C_0 = <(X+1)g_0(X)>$ Αντίστοιχα, $C_1^+ = <X^3 + X^2 +1>$ και $C_1 = <(X + 1)(X^3 + X^2 +1)>$.

Ο Golay κώδικας G_{23} μπορεί να οριστεί και σαν ο κώδικας τετραγωνικού υπολοίπου C_0^+ για q = 2 και n = 23. Επίσης, ο Golay κώδικας G_{11} μπορεί να οριστεί και σαν ο κώδικας τετραγωνικού υπολοίπου C_0^+ για q = 3 και n = 11. Αυτοί οι κώδικες έχουν τύπο (23, 12, 7) και (11, 6, 5) αντίστοιχα. Θεωρούμε την γνωστή παραγοντοποίηση του $X^{23} + 1$ στο σώμα $\mathbf{F}_2$:

$$X^{23} + 1 = (X+1)\,(X^{11}+X^{10}+X^6+X^5+X^4+X^2+1)(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$

Σαν γεννήτορας του κώδικα G_{23} μπορεί να ληφθεί ένα από τα παραπάνω δύο πολυώνυμα βαθμού 11.

Στο $\mathbf{F}_3$, έχουμε ότι $X^{11} - 1 = (X - 1)(X^5 + X^4 - X^3 + X^2 - 1)\,(X^5 - X^3 + X^2 - X - 1)$ και σαν γεννήτορα του κώδικα G_{11} μπορούμε να θεωρήσουμε οποιοδήποτε από τα παραπάνω δύο πολυώνυμα βαθμού 5.

<u>Σημείωση</u> Υπενθυμίζουμε ότι οι μόνοι γραμμικοί τέλειοι κώδικες είναι οι δυαδικοί κώδικες Hamming, ο G_{11} και ο G_{23}.

Το ερώτημα για την ελάχιστη απόσταση ενός QR-κώδικα βρίσκει απάντηση στην ακόλουθη

<u>Πρόταση 8.3</u> Αν $d := d_{min}(C_0^+)$ τότε ισχύει $d^2 \geq n$. Ανάλογη πρόταση ισχύει και για την $d_{min}(C_1^+)$.

Αν, επιπλέον, $n = 4k - 1$ τότε μπορούμε να πάρουμε το, καλύτερο, αποτέλεσμα $d^2 - d + 1 \geq n$.

<u>Απόδειξη</u> Έστω c μια κωδική λέξη στο C_0^+ με το ελάχιστο μη-μηδενικό βάρος d. Η c θα είναι ένα πολυώνυμο c(X) πολλαπλάσιο του $g_0(X)$. Έστω $c(X) = t_1(X)g_0(X)$. Αν λ ένας φυσικός αριθμός ο οποίος δεν είναι τετραγωνικό υπόλοιπο mod n τότε το πολυώνυμο $\bar{c}(X) = c(X^\lambda)$ είναι μια κωδική λέξη ελάχιστου βάρος για C_1^+. Το πολυώνυμο $\bar{c}(X)$ είναι πολλαπλάσιο του $g_1(X)$. Έστω $\bar{c}(X) = t_2(X)g_1(X)$. Εδώ παρατηρούμε ότι η απεικόνιση όπου $X \mapsto X^\lambda$ εναλλάσσει τα στοιχεία των C_0^+ και C_1^+. Επίσης, εναλλάσσει τα στοιχεία των C_0 και C_1. Αυτό σημαίνει ότι τα δύο C_0^+ και C_1^+ έχουν διάσταση $\frac{1}{2}(n + 1)$ ενώ οι C_0 και C_1 έχουν και οι δύο διάσταση $\frac{1}{2}(n - 1)$. Συνεπώς, η κωδική λέξη $c(X)\bar{c}(X) = t_1(X)g_0(X)\; t_2(X)g_1(X)$ ανήκει στο $C_0^+ \cap C_1^+$. Δηλαδή, είναι πολλαπλάσιο του πολυωνύμου

$$g_0(X)g_1(X) = \frac{X^n - 1}{X - 1} = X^{n-1} + X^{n-2} + \ldots + X^2 + X + 1.$$

Επομένως, η κωδική λέξη $c(X)\,\bar{c}\,(X)$ έχει βάρος n. Αφού, υποθέσαμε ότι η c(X) έχει βάρος d έπεται ότι το μέγιστο πλήθος των μη-μηδενικών συντελεστών του $c(X)\,\bar{c}\,(X)$ είναι d^2. Συνεπώς, $d^2 \geq n$.

Παράδειγμα 8.4 Ο (7, 4, d)-κώδικας τετραγωνικού υπολοίπου ως προς το σώμα $\mathbf{F}_q$ έχει n = 7 οπότε $d^2 \geq 7$ ή $d \geq 3$. Ειδικά αν q = 2 ο κώδικας μας είναι Hamming και η ελάχιστη απόσταση είναι d = 3.

Παρατήρηση 8.5 Γενικά η ελάχιστη απόσταση ενός QR-κώδικα είναι μεγαλύτερη από το κάτω φράγμα της πρότασης 8.3.

Τέλος, χωρίς απόδειξη αναφέρουμε την

Πρόταση 8.6

- Αν n = 4k – 1 τότε $C_0^+ = C_0^\perp$ και $C_1^+ = C_1^\perp$
- Αν n = 4k + 1 τότε $C_0^+ = C_1^\perp$ και $C_1^+ = C_0^\perp$

Και στις δύο περιπτώσεις ο C_0^+ παράγεται από τον C_0 και το 1 ενώ ο C_1^+ παράγεται από τον C_1 και το 1.