4. Κυκλικοί κώδικες

Πρόκειται για ειδικούς γραμμικούς κώδικες $C \leq F_q^n$ για τους οποίους για κάθε κωδική λέξη $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in C$ έπεται ότι $(\alpha_{n-1}, \alpha_0, \ldots, \alpha_{n-2}) \in C$. Δηλαδή, ο C είναι κυκλικός όταν για κάθε κωδική λέξη όλες οι λέξεις που προκύπτουν με κυκλικές μεταθέσεις των δεικτών της είναι επίσης κωδικές λέξεις.

Η απεικόνιση $Z : \mathbf{F}_q^n \to \mathbf{F}_q^n$ με τύπο $Z(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) = (\alpha_{n-1}, \alpha_0, \ldots, \alpha_{n-2})$ λέγεται **κυκλική μετατόπιση** (shift).

Θεωρούμε το δακτύλιο των πολυωνύμων μιας μεταβλητής με συντελεστές από το σώμα $\mathbf{F}_q$, $\mathbf{F}_q[X]$. Έστω $V_n = \{f(X) \in \mathbf{F}_q[X] \text{ με } \deg f(X) \leq n-1\} = \{f(X) \in \mathbf{F}_q[X] \text{ όπου } f(X) = \alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1} X^{n-1}\}$. Ταυτίζουμε (ισομορφία), το $\mathbf{F}_q^n = \{ (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \text{ όπου } \alpha_i \in \mathbf{F}_q \}$ με το χώρο V_n μέσω της απεικόνισης $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \mapsto \alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1} X^{n-1}$. Θεωρούμε επίσης τον χώρο $W_n = \mathbf{F}_q[X] / \langle X^n - 1 \rangle$ των υπολοίπων όλων των πολυωνύμων του $\mathbf{F}_q[X]$ διαιρουμένων με το πολυώνυμο $X^n - 1$, δηλαδή έχουμε τρεις όψεις του ίδιου "νομίσματος".

Παράδειγμα κυκλικού κώδικα 4.1

Αν $C \leq \mathbf{F}_2^7$ που ορίζεται από τον γεννήτορα πίνακα $G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$

$= \begin{bmatrix} g^{(1)} \\ g^{(2)} \\ g^{(3)} \end{bmatrix}$. Ο κώδικας είναι κυκλικός. Οι κωδικές λέξεις του C είναι γραμμικοί συνδυασμοί, ως προς το σώμα $\mathbf{F}_2$, των γραμμών του C και ισχύει:

$$(C \text{ κυκλικός}) \Leftrightarrow (Z(g^{(i)}) \in C \text{ για κάθε } i = 1, 2, 3).$$

Πράγματι : $Z(g^{(1)}) = g^{(2)} \in C$, $Z(g^{(2)}) = g^{(3)} \in C$, $Z(g^{(3)}) = g^{(1)} + g^{(2)} \in C$.

Χωρίς απόδειξη, αναφέρουμε :

(1) Ο υπόχωρος $C \leq W_n$ είναι κυκλικός κώδικας αν και μόνο αν ο C είναι ιδεώδες του δακτυλίου W_n
(2) Αν C ένας κυκλικός κώδικας τότε υπάρχει ακριβώς ένα πολυώνυμο $g \in V_n$ τέτοιο ώστε
    i. Το g διαιρεί το $X^n - 1$ στο $\mathbf{F}_q[X]$
    ii. Ο συντελεστής του μεγιστοβάθμιου όρου του g είναι 1

Ορισμός 4.2 Το πολυώνυμο g λέγεται **πολυώνυμο γεννήτορας** του κώδικα C. Τα στοιχεία του C λέγονται κωδικές λέξεις ή κωδικά πολυώνυμα ή κωδικά διανύσματα.

Από το (2) συμπεραίνουμε ότι γνωρίζουμε όλους τους κυκλικούς κώδικες μήκους n αν γνωρίζουμε όλα τα πολυώνυμα $g \in \mathbf{F}_q[X]$ τα οποία διαιρούν το $X^n - 1$.

Παρατήρηση 4.3 Αν το πολυώνυμο $g = g_0 + g_1X + \ldots + g_mX^m \in V_m$ διαιρεί το πολυώνυμο $X^n - 1$ και $\deg(g) = m < n$ τότε ο γραμμικός κώδικας C τύπου (n, k) που ορίζεται από τον γεννήτορα πίνακα

$$G = \begin{bmatrix} g_0 & g_1 & \ldots & g_m & 0 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{m-1} & g_m & 0 & \ldots & 0 \\ \vdots & & & \vdots & & & & \vdots \\ 0 & 0 & \ldots & g_0 & g_1 & g_2 & \ldots & g_m \end{bmatrix}$$

είναι κυκλικός.

Κωδικοποίηση κυκλικών κωδίκων

Έστω C κυκλικός κώδικας που παράγεται από το πολυώνυμο g. Στέλνουμε το μήνυμα $\alpha_0\alpha_1\alpha_2\ldots\alpha_{k-1}$ με $\alpha_i \in \mathbf{F}_q$.

(i) Το κάνουμε πολυώνυμο. Δηλαδή γίνεται $\alpha_0 + \alpha_1X + \ldots + \alpha_{k-1}X^{k-1}$
(ii) Το πολλαπλασιάζουμε με το πολυώνυμο g
(iii) Αν χρειαστεί, το διαιρούμε με το $X^n - 1$ και παίρνουμε το υπόλοιπο της διαίρεσης.

Το πολυώνυμο που προκύπτει γίνεται διάνυσμα και στέλνεται στον παραλήπτη.

Παράδειγμα 4.4 Έστω n = 6, q = 2. Δηλαδή στο $\mathbf{F}_2[X]$ θα πάρουμε πολυώνυμο g που να διαιρεί το $X^6 - 1$. Ας πάρουμε $g = X^3 - 1 = X^3 + 1$. Επομένως το g παράγει κυκλικό κώδικα. Έχουμε ότι k = 3. Κωδικοποιούμε ως εξής:

$000 \mapsto (0 + 0X + 0X^2)(1 + X^3) = 0 + 0X + 0X^2 + 0X^3 + 0X^4 + 0X^5 \mapsto 000000$
$100 \mapsto (1 + 0X + 0X^2)(1 + X^3) = 1 + X^3 \mapsto 100100$
$010 \mapsto X(1 + X^3) = X + X^4 \mapsto 010010$
$110 \mapsto (1 + X)(1 + X^3) = 1 + X + X^3 + X^4 \mapsto 110110$
$001 \mapsto X^2(1 + X^3) = X^2 + X^5 \mapsto 001001$
$101 \mapsto (1 + X^2)(1 + X^3) = 1 + X^2 + X^3 + X^5 \mapsto 101101$
$011 \mapsto (1 + X^2)(1 + X^3) = 1 + X^2 + X^3 + X^5 \mapsto 101101$
$111 \mapsto (1 + X + X^2)(1 + X^3) = 1 + X + X^2 + X^3 + X^4 + X^5 \mapsto 111111$

Ισχύει ότι αν $q = p^k$ και ο πρώτος p δεν διαιρεί το n τότε το πολυώνυμο $X^n - 1 \in \mathbf{F}_q[X]$ έχει απλές ρίζες.

Ορισμός 4.5 Έστω πρώτος p που δεν διαιρεί το n. Αν $X^n - 1 = g_1g_2 \ldots g_t$ η ανάλυση του $X^n - 1$ στο $\mathbf{F}_q[X]$ σε γινόμενο αναγώγων πολυωνύμων g_i τότε οι κώδικες $C_i = \langle g_i \rangle$ λέγονται **maximal κυκλικοί κώδικες**.

Έστω $C = \langle g \rangle$ κυκλικός κώδικας ως προς το σώμα $\mathbf{F}_q$ τύπου (n, k). Τότε $g \in V_n$ με $\deg g = m = n - k$ τέτοιο ώστε το g να διαιρεί $X^n - 1$. Οπότε υπάρχει $h(X) \in \mathbf{F}_q[X]$ τέτοιο ώστε $X^n - 1 = g(X)h(X)$, δηλαδή $h(X) = \dfrac{X^n - 1}{g(X)}$.

Ορισμός 4.6 Το πολυώνυμο h(X) λέγεται **πολυώνυμο ελέγχου** (parity check) του κυκλικού κώδικα C = <g>.

Συμβολισμός 4.7 Πολλαπλασιάζουμε δύο πολυώνυμα f_1, f_2, διαιρούμε το $X^n - 1$ και παίρνουμε το υπόλοιπο. Αυτό θα το συμβολίζουμε $f_1 * f_2$.

Πρόταση 4.8 Έστω κυκλικός κώδικας C = <g> $\leq V_n$, έστω $h(X) = \frac{X^n - 1}{g(X)}$ και έστω κάποιο $v \in V_n$, τότε $v \in C$ αν και μόνο αν $v * h = 0$.

Απόδειξη
($\Rightarrow$) Έστω $v \in C$ τότε υπάρχει πολυώνυμο α τέτοιο ώστε $v = \alpha * g$. Ισχύει ότι $gh = X^n - 1$, δηλαδή $g*h = 0$, οπότε $v * h = (\alpha * g) * h = \alpha * 0 = 0$.

($\Leftarrow$) Έστω $v * h = 0$, τότε $vh = (X^n - 1)k(X)$ για κάποιο πολυώνυμο $k(X) \in \mathbf{F}_q[X]$. Ξανά, ισχύει $X^n - 1 = gh$. Επομένως, $vh = k(X)gh = (k(X)g)h$ δηλαδή $v = k(X)g = k(X) * g$, οπότε $V \in C$.

Αποδεικνύεται ότι ο πίνακας ελέγχου ισοτιμίας του κυκλικού κώδικα C = <g> όπου $h = \frac{X^n - 1}{g} = h_0 + h_1X + \ldots + h_kX^k$ είναι ο

$$H = \begin{bmatrix} 0 & 0 & \ldots & 0 & h_k & \ldots & h_1h_0 \\ 0 & 0 & \ldots & h_k & h_{k-1} & \ldots & h_00 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ h_kh_{k-1} & \ldots & \ldots & h_0 & 0 & \ldots & 00 \end{bmatrix}$$

Αν C = <g> κυκλικός κώδικας (n, k) τότε και ο $C^{\perp}$ είναι επίσης κυκλικός τύπου (n, n – k) με πολυώνυμο γεννήτορα $h^{\perp} = X^{\deg h}(h \circ X^{-1})$.

Επεξήγηση Αν $h = h_0 + h_1X + \ldots + h_kX^k$ τότε $h \circ X^{-1} = h_0 + h_1\frac{1}{X} + h_2\frac{1}{X^2} + \ldots + h_k\frac{1}{X^k}$ τότε $h^{\perp} = X^k(h \circ X^{-1}) = h_0X^k + h_1X^{k-1} + \ldots + h_k$.

Παράδειγμα 4.9 Αν n = 7, q = 2 θεωρούμε το πολυώνυμο $X^7 - 1$. Παίρνουμε το πολυώνυμο $g(X) = X^3 + X + 1 \in \mathbf{F}_2[X]$. Το g(X) διαιρεί το $X^7 - 1$. Επομένως, το πολυώνυμο g(X) ορίζει κυκλικό κώδικα τύπου (n, k) = (n, n – m) = (7, 4).

Έστω C = <g>. Έχουμε ότι $G = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$

Ισχύει ότι $h(X) = \frac{X^7 - 1}{g(X)} = X^4 + X^2 + X + 1$ οπότε $h \circ X^{-1} = \frac{1}{X^4} + \frac{1}{X^2} + \frac{1}{X} + 1$ και επομένως $h^{\perp} = X^4(h \circ X^{-1}) = 1 + X^2 + X^3 + X^4$.

Ο πίνακας ελέγχου είναι $H = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$.

Ο Η έχει όλες τις δυνατές μη-μηδενικές στήλες στοιχείων του $\mathbf{F}_2$ μήκους 3 και μάλιστα μια φορά την καθεμία, δηλαδή ο κυκλικός κώδικας $C = \langle g(X) \rangle$, όπου $g(X) = 1 + X + X^3$ είναι ο (7, 4)-κώδικας Hamming.

Δίνονται το n και το πολυώνυμο g το οποίο διαιρεί το $X^n - 1$. Έστω degg = m. Ο κώδικας $C = \langle g \rangle$ είναι τύπου (n, k) όπου k = n – m. Θεωρούμε της δυνάμεις του X, X^j, $j \in \mathbf{N}$.

Διαιρούμε τα πολυώνυμα X^j με το g. Υπάρχουν μοναδικά πολυώνυμα $\alpha^{(j)}$ και $r^{(j)}$ τέτοια ώστε $X^j = \alpha^{(j)} g + r^{(j)}$ όπου $r^{(j)} = 0$ ή $degr^{(j)} < degg = m$. Τότε, ισχύει ότι $X^j - r^{(j)} = \alpha^{(j)} g \in C$.

Ισχύει ότι τα k στο πλήθος πολυώνυμα $g^{(i)} := X^k (X^j - r^{(j)})$ με $m \leq j \leq n - 1$ είναι $\mathbf{F}_q$ – γραμμικά ανεξάρτητα, θεωρούμενα σαν στοιχεία του W_n, και μας δίνουν τις γραμμές του γεννήτορα πίνακα σε κανονική μορφή $G = [I_k \mid - A_{k \times m}]$. Ο πίνακας ελέγχου ισοτιμίας Η προκύπτει αν σαν στήλες του θέσουμε τα υπόλοιπα της διαίρεσης των 1, X, X^2, …, X^m, …, X^{n-1} με το g.

Παράδειγμα 4.9 Ας πάρουμε n = 7, q = 2, $g = 1 + X + X^3$. Τότε:

$X^0 \bmod g \equiv 1 = r^{(0)}$
$X^1 \bmod g \equiv X = r^{(1)}$
$X^2 \bmod g \equiv X^2 = r^{(2)}$
$X^3 \bmod g \equiv 1 + X = r^{(3)}$
$X^4 \bmod g \equiv X + X^2 = r^{(4)}$
$X^5 \bmod g \equiv 1 + X + X^2 = r^{(5)}$
$X^6 \bmod g \equiv 1 + X^2 = r^{(6)}$

Άρα, ο πίνακας ισοτιμίας του κώδικα είναι ο $H = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right]$.

Επίσης, έχουμε $g^{(3)} = X^4(X^3 - (1 + X)) = X^7 + X^5 + X^4 \equiv 1 + X^4 + X^5 \rightarrow 1000110$. Ομοίως, $g^{(4)} = X + X^5 + X^6 \rightarrow 0100011$, $g^{(5)} = X^2 + X^4 + X^5 + X^6 \rightarrow 0010111$, $g^{(6)} = X^3 + X^4 + X^6 \rightarrow 0001101$. Επομένως ο γεννήτορας πίνακας του κώδικα είναι

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right].$$

Έστω $v = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1}) \in \mathbf{F}_q^n$. Αν συμβολίσουμε $\upsilon = \upsilon_0 + \upsilon_1 X + \ldots + \upsilon_{n-1} X^{n-1} \in V_n$ τότε το σύνδρομο του v είναι $S(v) \equiv \upsilon \bmod g$. Αν λοιπόν, $v = c + e$ για κάποια κωδική λέξη $c \in C = \langle g \rangle$ και κάποιο διάνυσμα λάθους e έχουμε ότι $S(v) = S(c) + S(e) = S(e) = e$ (το αντίστοιχο πολυώνυμο του διανύσματος e).

Αλγόριθμος αποκωδικοποίησης κυκλικών κωδικών

(Γνωρίζουμε ότι ο κώδικας διορθώνει t το πολύ λάθη)

Έστω $C = \langle g \rangle \leq V_n$ κυκλικός κώδικας όπου το g(X) διαιρεί το $(X^n - 1)$ και deg g = m τύπου (n, k) όπου k = n – m. Υποθέτουμε ότι είναι t-error correcting.

(1) Διαιρούμε το μήνυμα $\upsilon \in V_n$ που πήραμε με το πολυώνυμο γεννήτορα g και βρίσκουμε το υπόλοιπο της διαίρεσης r. Αν e το πολυώνυμο λάθους, τότε $r = S(\upsilon) = S(e)$.

(2) Για $0 \leq i \leq n - 1$, υπολογίζουμε, τα $S_i := X^i \, r \pmod g$. Υπολογίζουμε το βάρος του S_j μέχρι να βρούμε κάποιο j_0 τέτοιο ώστε $w(S_{j_0}) \leq t$. Τότε το $X^{n-j_0} S_{j_0} \bmod (X^n - 1)$ είναι το πιο πιθανό λάθος.

Παρατήρηση Ο αλγόριθμος δουλεύει μόνο υπό την προϋπόθεση ότι υπάρχει κάποιο j τέτοιο ώστε $\deg (X^j e) \leq \deg g$.

Παράδειγμα 4.10 Ας πάρουμε n = 15, q = 2. Θεωρούμε το πολυώνυμο

$$g(X) = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1) = X^8 + X^7 + X^6 + X^4 + 1 \in \mathbf{F}_2[X].$$

Το g(X) διαιρεί το πολυώνυμο $X^{15} - 1$ επομένως παράγει κυκλικό (15, 7)-κώδικα C. Θα δούμε αργότερα, στην παράγραφο 6, ότι ο C έχει $d_{min}(C) = 5$. Άρα $t = \left\lfloor \frac{d-1}{2} \right\rfloor = 2$.

Ο κώδικας C είναι 2-error correcting.

Υποθέτουμε ότι πήραμε το μήνυμα v = 1001110 το οποίο αντιστοιχεί στο πολυώνυμο $\upsilon = 1 + 0\,X + 0\,X^2 + 1\,X^3 + 1\,X^4 + 1\,X^5 + 0\,X^6 = 1 + X^3 + X^4 + X^5$. Ισχύει ότι $\deg \upsilon = 5 < \deg g = 8$ συνεπώς $r = S(\upsilon) = \upsilon$ και $w(\upsilon) = 4 > 2$.

Υπολογίζουμε το $S_1 = X\,r = X\,\upsilon = X\,(1 + X^3 + X^4 + X^5) = X + X^4 + X^5 + X^6$. Επειδή, $\deg S_1 < \deg g$ το S_1 ταυτίζεται με το υπόλοιπο της διαίρεσής τους με το g οπότε $w(S_1) = w(X\,\upsilon) = 4 > 2$. Αναγκαζόμαστε να συνεχίσουμε.

$S_2 = X^2\,\upsilon = X^2 + X^5 + X^6 + X^7$. Πάλι το βάρος είναι $w(S_2) = 4$. Συνεχίζουμε: $S_3 = X^3\,\upsilon = X^3 + X^6 + X^7 + X^8$. Επειδή $g(X) = X^8 + X^7 + X^6 + X^4 + 1$ έπεται ότι $X^8 = X^7 + X^6 + X^4 + 1 \pmod g$ οπότε $S_3 = X^4 + X^3 + 1 \pmod g$. Επομένως, το υπόλοιπο της διαίρεσης με το g έχει βάρος $w(S_3) = 3 > 2$. Συνεχίζουμε:

$S_4 = X^4\,\upsilon = X^5 + X^4 + X \pmod g$ άρα $w(S_4) = 3 > 2$
$S_5 = X^5\,\upsilon = X^6 + X^5 + X^2 \pmod g$ άρα $w(S_5) = 3 > 2$

$S_6 = X^6\,\upsilon = X^7 + X^6 + X^3 \pmod g$ άρα $w(S_6) = 3 > 2$
$S_7 = X^7\,\upsilon = X^8 + X^7 + X^4 = X^6 + 1 \pmod g$ άρα $w(S_7) = 2 \leq 2 = t$.

Άρα το πιο πιθανό λάθος είναι το πολυώνυμο $X^{15-7}\,S_7 = X^8\,(X^6 + 1) = X^{14} + X^8$. Επομένως, αποκωδικοποιούμε στο πολυώνυμο:

$$\upsilon + X^8 + X^{14} = 1 + X^3 + X^4 + X^5 + X^8 + X^{14}$$

Διαιρούμε αυτό το πολυώνυμο με το g και βρίσκουμε $1 + X^3 + X^5 + X^6$. Άρα το μήνυμα που στάλθηκε είναι το 1001011.

Τέλος, χωρίς απόδειξη αναφέρουμε την

Πρόταση 4.11 Κάθε δυαδικός κώδικας Hamming είναι κυκλικός