5. Κυκλικοί κώδικες (συνέχεια)

Έστω C = <g> κυκλικός κώδικας όπου g πολυώνυμο του $\mathbf{F}_q[X]$ βαθμού deg g(X) = m το οποίο διαιρεί $X^n - 1$. Υπάρχει, επομένως, κάποιο πολυώνυμο $t(X) \in \mathbf{F}_q[X]$ τέτοιο ώστε $X^n - 1 = g(X)t(X)$. Αν α μια ρίζα του g(X) τότε από την τελευταία σχέση έχουμε $\alpha^n - 1 = g(\alpha)t(\alpha) = 0$ $t(\alpha) = 0$. Δηλαδή η α είναι ρίζα του πολυωνύμου $X^n - 1$. Άρα, κάθε ρίζα του g(X) είναι μια n-ρίζα της μονάδας. Ας ονομάσουμε $\alpha_1, \alpha_2, \ldots, \alpha_m$ τις ρίζες του g(X).

Πρόταση 5.1 $\upsilon \in C = \langle g \rangle$ αν και μόνο αν $\upsilon(\alpha_1) = \upsilon(\alpha_2) = \ldots = \upsilon(\alpha_m) = 0$.

Απόδειξη $\upsilon \in C = \langle g \rangle \Leftrightarrow \upsilon(X) = g(X)\, t(X)$ για κάποιο πολυώνυμο $t(X) \in \mathbf{F}_q[X]$ $\Leftrightarrow \upsilon(\alpha_i) = g(\alpha_i)\, t(\alpha_i) = 0$ για κάθε i = 1, 2, …, m.

Παρατήρηση 5.2 Αν C = <g> κυκλικός κώδικας τύπου (n, k) και $\alpha_1, \alpha_2, \ldots, \alpha_m$, όπου m = n – k, οι ρίζες του πολυωνύμου g τότε το πολυώνυμο $\upsilon \in V_n$ είναι κωδικό πολυώνυμο. Έστω $\upsilon = \upsilon_0 + \upsilon_1 X + \ldots + \upsilon_{n-1} X^{n-1} \in V_n$. Το διάνυσμα των συντελεστών $v = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1})$ ανήκει στο μηδενόχωρο του πίνακα

$$H = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{n-1} \end{bmatrix}$$

Απόδειξη [υ κωδική λέξη] $\Leftrightarrow$ [$\upsilon \in C = \langle g \rangle$] $\Leftrightarrow$ [$\upsilon(\alpha_i) = 0$ για κάθε i = 1, 2, …, m] $\Leftrightarrow [(1, \alpha_i, \ldots, \alpha_i^{n-1})(\upsilon_0, \upsilon_1, \ldots, \upsilon_{n-1})^T$ για κάθε i = 1, 2, …, m] $\Leftrightarrow H\upsilon^T = 0$.

Υπενθυμίζουμε:

(1) Αν F πεπερασμένο σώμα με q στοιχεία τότε υπάρχει πρώτος p και φυσικός αριθμός n τέτοιοι ώστε $q = p^n$.
(2) Δυο πεπερασμένα σώματα με τον ίδιο αριθμό στοιχείων q είναι ισόμορφα. Δηλαδή, για κάθε $q = p^n$ υπάρχει ακριβώς ένα σώμα με q στοιχεία.

Κατασκευή σώματος με 4 στοιχεία

Επειδή το 4 είναι δύναμη του 2 θεωρούμε τον δακτύλιο των πολυωνύμων $\mathbf{F}_2[X]$. Επειδή $4 = 2^2$ αναζητούμε ένα ανάγωγο πολυώνυμο f(X) στο $\mathbf{F}_2[X]$ βαθμού 2. Για παράδειγμα το $f(X) = X^2 + X + 1$ είναι ανάγωγο στο $\mathbf{F}_2[X]$ διότι $f(0) = 1 \neq 0$ και $f(1) = 1 \neq 0$. Θεωρούμε το σύνολο όλων των δυνατών υπολοίπων της διαίρεσης των ενός πολυωνύμου του $\mathbf{F}_2[X]$ με το $X^2 + X + 1$ δηλαδή το $\mathbf{F}_2[X] / \langle X^2 + X + 1 \rangle = \{0, 1, X, X + 1\}$. Το σύνολο αυτό είναι αντιμεταθετική ομάδα ως προς την πρόσθεση και χωρίς το μηδέν είναι αντιμεταθετική ομάδα ως προς τον πολλαπλασιασμό. Δηλαδή είναι σώμα.

Οι πίνακες πρόσθεσης και πολλαπλασιασμού είναι οι εξής:

+	0	1	X	X + 1
0	0	1	X	X + 1
1	1	0	X + 1	X
X	X	X + 1	0	1
X + 1	X + 1	X	1	0

·	1	X	X + 1
1	1	X	X + 1
X	X	X + 1	1
X + 1	X + 1	1	X

Έστω F πεπερασμένο σώμα με $q = p^n$ στοιχεία. Το F είναι ταυτισμένο με το σώμα $\mathbf{F}_q[X] / \langle f(X) \rangle$ όπου $f(X) \in \mathbf{F}_p[X]$ ανάγωγο πολυώνυμο βαθμού n.

Θα αναφέρουμε λίγα στοιχεία από την θεωρία των πεπερασμένων σωμάτων:

Σε κάθε σώμα το $F^* = F \setminus \{0\}$ είναι πολλαπλασιαστική ομάδα τάξης $q - 1$.

1. Αν $\alpha \in F^*$ τότε η τάξη του $t = \text{ord}(\alpha)$ διαιρεί το $q - 1$.
2. Αν το t δεν διαιρεί το $q - 1$ τότε δεν υπάρχει $\alpha \in F^*$ τάξης t
3. Αν το t διαιρεί το $q - 1$ τότε υπάρχουν πάντοτε $\alpha \in F^*$ τάξης t.
   Το πλήθος τους είναι $\varphi(t)$.
4. Η πεπερασμένη πολλαπλασιαστική ομάδα F^* τάξης $q - 1$ είναι <u>κυκλική</u>. Δηλαδή υπάρχει τουλάχιστον ένα στοιχείο $\zeta \in F^*$ τάξης $q - 1$.
5. Σε κάθε στοιχείο $\alpha \in F$ αντιστοιχεί <u>μονοσήμαντα</u> ένα μονικό πολυώνυμο $p(X) \in \mathbf{F}_q[X]$ όπου $q = p^n$ τέτοιο ώστε
   a. $p(\alpha) = 0$
   b. $\deg p(X) \leq n$
   c. $p(X)$ ανάγωγο στο $\mathbf{F}_q[X]$
   d. Αν υπάρχει $f(X) \in \mathbf{F}_q[X]$ με $f(\alpha) = 0$ τότε το $p(X)$ διαιρεί το $f(X)$

   Το $p(X)$ λέγεται το **ελάχιστο πολυώνυμο** του α
6. Αν $f(X) \in \mathbf{F}_q[X]$ έχει ρίζα το $\alpha \in F$ τότε έχει ρίζες και τα $\alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$ Θα σταματήσουμε στον εκθέτη d όπου d ο ελάχιστος φυσικός αριθμός τέτοιος ώστε $q^d \equiv 1 \bmod t$ και όπου $t = \text{ord}(\alpha)$

Με βάση τα παραπάνω θα δώσουμε ένα παράδειγμα το οποίο θα μας οδηγήσει στον ορισμό μια πολύ ενδιαφέρουσας κλάσης κωδίκων, τους BCH κώδικες.

<u>Παράδειγμα 5.3</u> Ξεκινάμε από το σώμα $\mathbf{F}_2$. Θεωρούμε τον δακτύλιο $\mathbf{F}_2[X]$. Έστω $f(X) = X^4 + X + 1 \in \mathbf{F}_2[X]$. Το $f(X)$ είναι ανάγωγο στο $\mathbf{F}_2[X]$. Με αυτό το πολυώνυμο κατασκευάζουμε το σώμα $F = \mathbf{F}_2[X] / \langle X^4 + X + 1 \rangle$ με $2^4 = 16$ στοιχεία. Έστω ζ μια ρίζα αυτού του πολυωνύμου. Δηλαδή θα ισχύει $\zeta^4 + \zeta + 1 = 0$ ή $\zeta^4 = \zeta + 1$. Το F^* έχει τάξη 15. Το ζ δεν έχει τάξη ούτε 1 ούτε 3 αλλά ούτε και 5 αφού $\zeta^5 = \zeta^2 + \zeta \neq 1$ άρα έχει τάξη $\text{ord}(\zeta) = 15$. Πιο αναλυτικά:

$$\begin{array}{ll}
\zeta^0 = 1 & \zeta^8 = \zeta^2 + 1 \\
\zeta^1 = \zeta & \zeta^9 = \zeta^3 + \zeta \\
\zeta^2 = \zeta^2 & \zeta^{10} = \zeta^2 + \zeta + 1 \\
\zeta^3 = \zeta^3 & \zeta^{11} = \zeta^3 + \zeta^2 + \zeta \\
\zeta^4 = \zeta + 1 & \zeta^{12} = \zeta^3 + \zeta^2 + \zeta + 1 \\
\zeta^5 = \zeta^2 + \zeta & \zeta^{13} = \zeta^3 + \zeta^2 + 1 \\
\zeta^6 = \zeta^3 + \zeta^2 & \zeta^{14} = \zeta^3 + 1 \\
\zeta^7 = \zeta^3 + \zeta + 1 & \zeta^{15} = 1
\end{array}$$

Το ζ είναι ρίζα $X^4 + X + 1$. Οι υπόλοιπες ρίζες του πολυωνύμου είναι τα $\zeta^2, \zeta^{2^2}, ..., \zeta^{2^{d-1}}$ όπου d ο ελάχιστος φυσικός αριθμός τέτοιος ώστε $2^d \equiv 1 \bmod t$ όπου $t = \text{ord}(\zeta) = 15$. Οπότε $d = 4$ και επομένως οι ρίζες του $X^4 + X + 1$ είναι $\zeta, \zeta^2, \zeta^4, \zeta^8$.

Στη συνέχεια παίρνουμε μια δύναμη του ζ με εκθέτη μικρό αλλά διαφορετικό από αυτό των ριζών. Το ζ^3.

Θυμίζουμε ότι αν G ομάδα τάξης n και $\alpha \in G$ τάξης $t = \text{ord}(\alpha)$ τότε η τάξη του στοιχείου α^k είναι $\text{ord}(\alpha^k) = \dfrac{t}{\mu\kappa\delta(k,n)}$. Επομένως, η τάξη του στοιχείου ζ^3 είναι $\text{ord}(\zeta^3) = \dfrac{t}{\mu\kappa\delta(15,3)} = \dfrac{15}{3} = 5$.

Το ελάχιστο πολυώνυμο του ζ^3 θα έχει σαν ρίζες τα ζ^3, $(\zeta^3)^2 = \zeta^6$, $(\zeta^3)^4 = \zeta^{12}$, $(\zeta^3)^8 = \zeta^9$.

Θα βρούμε το ελάχιστο πολυώνυμο του ζ^3 με δύο τρόπους.

1. Έχουμε ότι $\zeta^{15} = 1$ ή αλλιώς $(\zeta^3)^5 = 1$. Επομένως, το ζ^3 είναι ρίζα του πολυωνύμου $X^5 - 1 = (X - 1)(X^4 + X^3 + X^2 + X + 1)$. Ισχύει ότι $\zeta^3 \neq 1$ διότι τα $1, \zeta, \zeta^2, \zeta^3$ είναι $\mathbf{F}_2$ – γραμμικά ανεξάρτητα. Άρα το ζ^3 είναι ρίζα του $X^4 + X^3 + X^2 + X + 1$. Το ελάχιστο πολυώνυμο $p(X)$ του ζ^3 είναι βαθμού 4 αφού έχει ακριβώς 4 ρίζες. Το πολυώνυμο $X^4 + X^3 + X^2 + X + 1$ έχει επίσης ρίζα το ζ^3 άρα διαιρείται από το $p(X)$ διαιρεί και έχουν τον ίδιο βαθμό. Άρα $p(X) = X^4 + X^3 + X^2 + X + 1$.

2. Το ελάχιστο πολυώνυμο του ζ^3 είναι το $f_3(X) = (X - \zeta^3)(X - \zeta^6)(X - \zeta^9)(X - \zeta^{12})$ το οποίο είναι βαθμού 4 άρα ισχύει ότι $f_3(X) = X^4 + AX^3 + BX^2 + \Gamma X + \Delta$ για κάποια $A, B, \Gamma, \Delta \in \mathbf{F}_2$. Από τις σχέσεις ριζών-συντελεστών έχουμε:

   $A := \zeta^3 + \zeta^6 + \zeta^9 + \zeta^{12} = \zeta^3 + (\zeta^3 + \zeta^2) + (\zeta^3 + \zeta) + (\zeta^3 + \zeta^2 + \zeta + 1) = 1$
   $B := \zeta^3\zeta^6 + \zeta^3\zeta^9 + \zeta^3\zeta^{12} + \zeta^6\zeta^9 + \zeta^6\zeta^{12} + \zeta^9\zeta^{12} = \zeta^9 + \zeta^{12} + 1 + 1 + \zeta^3 + \zeta^6 = 1$
   $\Gamma := \zeta^3\zeta^6\zeta^9 + \zeta^3\zeta^6\zeta^{12} + \zeta^3\zeta^9\zeta^{12} + \zeta^6\zeta^9\zeta^{12} = \zeta^3\zeta^{15} + \zeta^6\zeta^{15} + \zeta^9\zeta^{15} + \zeta^{12}\zeta^{15} = 1$
   $\Delta := \zeta^3\zeta^6\zeta^9\zeta^{12} = \zeta^{30} = 1$

   Άρα και πάλι, το ελάχιστο πολυώνυμο είναι το $X^4 + X^3 + X^2 + X + 1$.

Θεωρούμε το πολυώνυμο $g(X) = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)$. Το g έχει ρίζες τα $\zeta, \zeta^2, \zeta^4, \zeta^8, \zeta^3, \zeta^6, \zeta^9, \zeta^{12}$ και $\deg g = 8$. Άρα το $g(X)$ διαιρεί το $X^{15} - 1$. Κατασκευάζουμε τον κυκλικό κώδικα $C = \langle g \rangle$. Ισχύει ότι $n = 15$ και $k = 15 - 8 = 7$ άρα ο C είναι ένας (15, 7)-κώδικας. Ο πίνακας ελέγχου ισοτιμίας γράφεται:

$$H = \begin{bmatrix} 1 & \zeta & \zeta^2 & \zeta^3 & \dots & \zeta^{14} \\ 1 & \zeta^3 & \zeta^6 & \zeta^9 & \dots & \zeta^{42} \end{bmatrix}$$

Θα αποδείξουμε στην επόμενη παράγραφο ότι $d_{min}(C) \geq 5$ δηλαδή ότι ο C είναι 2-error correcting και 4-error detecting.

Έχουμε ότι $\upsilon \in C$ αν και μόνο αν ισχύει $S(\upsilon) = H\upsilon^T = 0$. Έχουμε ότι $S(\upsilon) = (S_1, S_3)$ όπου $S_1 = \sum_{i=0}^{14} \upsilon_i \zeta^i$ και $S_3 = \sum_{i=0}^{14} \upsilon_i \zeta^{3i}$. Οπότε $\upsilon \in C$ αν και μόνο αν $S_1 = S_3 = 0$. Ουσιαστικά παραλείψαμε το S_2 γιατί $S_2 = S_1^2$. Ο πίνακας H σε δυαδική μορφή γράφεται

$$H = \left[\begin{array}{cccccccccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hdashline 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{array}\right]$$

Υποθέτουμε ότι πήραμε το διάνυσμα $v = (\upsilon_0, \upsilon_1, \ldots, \upsilon_{14})$ το οποίο έχει 2 λάθη. Παίρνουμε το πολυώνυμο λάθους $e = X^{\alpha_1} + X^{\alpha_2}$ όπου $0 \le \alpha_1, \alpha_2 \le 14$. Ονομάζουμε $X_1 = \zeta_1^{\alpha_1}$ και $X_2 = \zeta_2^{\alpha_2}$. Οπότε $S_1 = \zeta^{\alpha_1} + \zeta^{\alpha_2} = X_1 + X_2$ και $S_3 = \zeta^{3\alpha_1} + \zeta^{3\alpha_2} = X_1^3 + X_2^3$. Και επομένως, $X_2^3 = (S_1 + X_1)^3 = S_1^3 + S_1^2 X_1 + S_1 X_1^2 + X_1^3$ ή αλλιώς

$$S_1 X_1^2 + S_1^2 X_1 + (S_1^3 - S_3) = 0 \qquad (1)$$

- Αν εμφανίζονται δύο λάθη τότε η εξίσωση έχει δύο λύσεις.
- Αν εμφανίζεται ένα λάθος ισχύει $S_1 = X_1$ και $S_3 = X_1^3$ και η εξίσωση γίνεται $X_1 + S_1 = 0$.
- Αν δεν εμφανίζεται κανένα λάθος ισχύει $S_1 = 0$ και $S_3 = 0$.
- Αν η εξίσωση δε λύνεται αυτό σημαίνει ότι εμφανίζονται περισσότερα από δύο λάθη το οποία όμως δεν μπορούμε να διορθώσουμε

Υποθέτουμε ότι πήραμε το υ = 100 111 000 000 000. Υπολογίζουμε το σύνδρομο $S(\upsilon) = (S_1, S_3)$. Έχουμε:

$S_1 = 1 + \zeta^3 + \zeta^4 + \zeta^5 = 1 + \zeta^3 + 1 + \zeta + \zeta + \zeta^2 = \zeta^2 + \zeta^3$
και $S_3 = 1 + \zeta^9 + \zeta^{12} + \zeta^{15} = 1 + (\zeta + \zeta^3) + (1 + \zeta + \zeta^2 + \zeta^3) + 1 = 1 + \zeta^2$.

Τότε έχουμε ότι $S_1^2 = (\zeta^2 + \zeta^3)^2 = \zeta^4 + \zeta^6 = 1 + \zeta + \zeta^2 + \zeta^3$ και $S_1^3 - S_3 =$
$(1 + \zeta^2 + \zeta^3 + \zeta^4)(\zeta^2 + \zeta^3) - (1 + \zeta^2) = \zeta^2 + \zeta^4 + \zeta^5 + \zeta^6 + \zeta^3 + \zeta^5 + \zeta^6 + \zeta^7 + 1 + \zeta^3 =$
$\zeta^2 + (1 + \zeta) + (\zeta + \zeta^2) + (1 + \zeta + \zeta^3) + 1 + \zeta^2 = 1 + \zeta^2 + \zeta^3$

Η εξίσωση (1) γράφεται $(\zeta^2 + \zeta^3)X_1^2 + (1 + \zeta + \zeta^2 + \zeta^3)X_1 + (1 + \zeta^2 + \zeta^3) = 0$. Με τη μέθοδο της δοκιμής και της επιτυχίας βρίσκουμε ότι το ζ^8 είναι λύση της αφού αν θέσουμε όπου X_1 το ζ^8 έχουμε:

$(\zeta^2 + \zeta^3)\zeta^{16} + (1 + \zeta + \zeta^2 + \zeta^3)\zeta^8 + (1 + \zeta^2 + \zeta^3) =$
$(\zeta^2 + \zeta^3)\zeta + (\zeta^8 + \zeta^9 + \zeta^{10} + \zeta^{11}) + (1 + \zeta^2 + \zeta^3) =$

$\zeta^3 + (\zeta + 1) + (\zeta^2 + 1) + (\zeta^3 + \zeta) + (\zeta^2 + \zeta + 1) + (\zeta^3 + \zeta^2 + \zeta) + 1 + \zeta^2 + \zeta^3 = 0$

Με τον ίδιο τρόπο βρίσκουμε και την άλλη λύση της εξίσωσης. Το ζ^{14}. Επομένως, τα λάθη εμφανίζονται στις θέσεις 9 και 15. Διορθώνουμε το υ σε αυτές τις θέσεις και παίρνουμε την κωδική λέξη w = 100 111 001 000 001 που στάλθηκε. Άρα, το μήνυμα που στάλθηκε ήταν $\frac{w}{g} = X^6 + X^5 + X^3 + 1$ δηλαδή το α = 1001011.