6. BCH κώδικες

Δίνονται οι σταθερές c, d, n, q, φυσικοί αριθμοί, όπου q δύναμη πρώτου, $2 \le d \le n$ και ΜΚΔ(n, q) = 1.
Έστω m ο ελάχιστος φυσικός αριθμός ο οποίος διαιρεί το $q^m - 1$.

Έστω ζ μια n-ρίζα της μονάδας τάξης ακριβώς n. (Λέγεται πρωταρχική n-ρίζα της μονάδας) Έστω m_{ζ_i} το ελάχιστο πολυώνυμο που έχει σαν ρίζα του το ζ^i $(1 \le i \le m)$. Τέλος έστω I = {c, c + 1, …, c + d – 2}. Ο BCH – κώδικας $C \le V_n$ με καθορισμένη (designed) απόσταση d είναι ένας κυκλικός κώδικας ο οποίος ικανοποιεί τις ακόλουθες συνθήκες:

(i) $\upsilon \in C \Leftrightarrow \upsilon(\zeta^i) = 0$ για κάθε $i \in I$
(ii) Ο γεννήτορας g του κώδικα C, είναι το πολυώνυμο ΕΚΠ{m_{ζ_i} όπου $i \in I$}
(iii) Ο πίνακας ελέγχου ισοτιμίας είναι ο

$$H = \begin{bmatrix} 1 & \zeta^c & \dots & \zeta^{c(n-1)} \\ 1 & \zeta^{c+1} & \dots & \zeta^{(c+1)(n-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \zeta^{c+d-2} & \dots & \zeta^{(c+d-2)(n-1)} \end{bmatrix}$$

Παρατηρήσεις – ορισμοί 6.1

(i) Αν c = 1 τότε ο κώδικας λέγεται BCH – κώδικας **με στενή σημασία**.
(ii) Αν $n = q^m - 1$ τότε ο κώδικας λέγεται **πρωταρχικός** BCH – κώδικας
(iii) Η διάσταση του κώδικα είναι μεγαλύτερη ή ίση από n – m(d –1)

Πρακτικό παράδειγμα Το European and Transatlantic information and communication's system χρησιμοποίησε BCH-κώδικες. Το πολυώνυμο γεννήτορας ήταν 24ου βαθμού και το κωδικοποιημένο μήνυμα είχε μήκος $2^8 - 1 = 255$. Ο κώδικας ανιχνεύει τουλάχιστον 6 λάθη και η πιθανότητα λάθους είναι $\frac{1}{16 \cdot 10^6}$.

Ισχύει το

Θεώρημα 6.2 Η ελάχιστη απόσταση ενός BCH-κώδικα C με δοσμένο d είναι μεγαλύτερη ή ίση από αυτό.

Κώδικες Reed-Solomon Λέγονται πρωταρχικοί BCH-κώδικες με στενή σημασία, δηλαδή με c = 1, δοσμένη απόσταση d και μήκος n = q – 1, δηλαδή με m = 1.

Το πολυώνυμο γεννήτορας του κώδικα είναι $g(X) := \prod_{i=1}^{d-1} (X - \zeta^i)$ όπου ζ πρωταρχική n-ρίζα της μονάδας.

Θεώρημα 6.3 Η ελάχιστη απόσταση $d_{min}(C)$ ενός Reed-Solomon κώδικα C με δοσμένο d είναι $d_{min}(C) = d$.

Απόδειξη Ο C είναι BCH-κώδικας άρα $d_{min}(C) \geq d$. Από το φράγμα του Singleton ισχύει ότι $d_{min}(C) \leq n - k + 1$ όπου $k \geq n - m(d - 1) = n - (d - 1)$ αφού $m = 1$. Άρα $d_{min}(C) \leq n - (n - m(d - 1)) + 1 = d - 1 + 1 = d$. Από τις δυο ανισότητες προκύπτει ότι $d_{min}(C) = d$.

Παρατήρηση 6.4 Οι Reed-Solomon κώδικες χρησιμοποιούνται για την παραγωγή υψηλής ευκρίνειας ήχου στα CD.

Παραδείγματα BCH-κωδίκων 6.5

i) Αν ζ πρωταρχική $(2^m - 1)$-ρίζα της μονάδας, δηλαδή γεννήτορας της ομάδας $\mathbf{F}^*_{2^m}$, και $m_\zeta(X) \in \mathbf{F}_2[X]$ το ελάχιστο πολυώνυμο του ζ τότε $\deg m_\zeta(X) = m$. Αν πάρουμε $n = 2^m - 1$, $c = 2$, $d = 3$ τότε $I = \{1, 2\}$ και ο $C = \langle m_\zeta \rangle$ είναι ένας BCH-κώδικας και αφού $n = 2^m - 1$ είναι επίσης ένας δυαδικός κώδικας Hamming.

ii) Έστω $m = 4$. Έστω ζ πρωταρχική ρίζα της n-μονάδας όπου $n = 2^4 - 1 = 15$ και με ελάχιστο πολυώνυμο $m_\zeta(X) = X^4 + X + 1 \in \mathbf{F}_2[X]$. Έχουμε ότι $k = 15 - 4 = 11$. Ο κώδικας $C = \langle m_\zeta(X) \rangle$ μπορεί να θεωρηθεί σαν BCH-κώδικας με στενή σημασία ($c = 1$). Φυσικά, είναι και δυαδικός κώδικας Hamming, άρα $d_{min}(C) = 3$.

iii)Παίρνουμε $q = 2$, $n = 15$ και $d = 4$. Έστω ζ πρωταρχική 15-ρίζα της μονάδας με ελάχιστο πολυώνυμο $m_\zeta(X) = X^4 + X + 1 \in \mathbf{F}_2[X]$. Τα ζ^2 και ζ^4 είναι επίσης ρίζες του $m_\zeta(X)$. Το ζ^3 έχει σαν ελάχιστο πολυώνυμο το $m_{\zeta^3}(X) = X^4 + X^3 + X^2 + X + 1$. Ισχύει ότι $ΕΚΠ(m_\zeta(X), m_{\zeta^3}(X)) = m_\zeta(X)\, m_{\zeta^3}(X)$. Επομένως, το πολυώνυμο $g(X) = m_\zeta(X)\, m_{\zeta^3}(X) = (X^4 + X + 1)(X^4 + X^3 + X^2 + X + 1)$ παράγει τον κυκλικό BCH-κώδικα με στενή σημασία ($c = 1$) όπου $I = \{1, 2, 3\}$. Ο $C = \langle g \rangle$ είναι επίσης ένας BCH-κώδικας με δοσμένη απόσταση $d = 5$ διότι ισχύει ότι $\upsilon \in C$ αν και μόνο αν ισχύει $\upsilon(\zeta^i) = 0$ για κάθε $i = 1, 2, 3, 4$. Οπότε έχουμε ότι $c + d - 2 = 4$ ή $d = 5$.

Παρατήρηση 6.6 Οι BCH-κώδικες είναι πάρα πολύ δυναμικοί αφού για κάθε φυσικό αριθμό d μπορεί να κατασκευαστεί BCH-κώδικας C με $d_{min}(C) \geq d$

iv)Έστω $q = 3$. Το πολυώνυμο $X^2 + 2X + 2 \in \mathbf{F}_3[X]$ είναι ανάγωγο. Θεωρούμε το σώμα με 9 στοιχεία $\mathbf{F}_9 = \mathbf{F}_3[X] / \langle X^2 + 2X + 2 \rangle$. Αν ζ ρίζα του πολυωνύμου $X^2 + 2X + 2$ τότε $\zeta^8 = 1$. Οι ρίζες του πολυωνύμου $m_\zeta(X) = X^2 + 2X + 2$ είναι ζ και ζ^3. Έχουμε ότι $\zeta^2 + 2\zeta + 2 = 0$ ή $\zeta^2 = \zeta + 1$. Το ελάχιστο πολυώνυμο του ζ^2, το $m_{\zeta^2}(X)$, έχει σαν ρίζες τα ζ^2, $(\zeta^2)^3 = \zeta^6$. Επομένως, $m_{\zeta^2}(X) = (X - \zeta^2)(X - \zeta^6) = X^2 - (\zeta^2 + \zeta^6)X + \zeta^8 = X^2 - (\zeta^2 + \zeta^6)X + 1$. Έχουμε ότι $\zeta^2 = \zeta + 1$ άρα $\zeta^6 = (\zeta^2)^3 = (\zeta + 1)^3 = \zeta^3 + 1 = \zeta^2 + \zeta + 1 = 2\zeta + 2$. Οπότε, $\zeta^2 + \zeta^6 = 2\zeta + 2 + \zeta + 1 = 0$. Άρα $M_{\zeta^2}(X) = X^2 - 0\, X + 1 = X^2 + 1$. Δηλαδή ο BCH-κώδικας $C = \langle g \rangle$ όπου $g = M_\zeta(X)\, M_{\zeta^2}(X) = (X^2 + 2X + 2)(X^2 + 1)$. Έχει επομένως $d_{min}(C) \geq 4$.

Αποκωδικοποίηση των BCH-κωδίκων

Έστω ότι στάλθηκε το διάνυσμα υ και πήραμε το w. Το λάθος είναι το διάνυσμα $e = w - u$. Για το σύνδρομο S(w) ισχύει ότι $S(w) = Hw^T = (S_c, S_{c+1}, \ldots, S_{c+d-2})^T$ όπου $S_j = w(\zeta^j)$ για κάθε j τέτοιο ώστε $c \le j \le c + d - 2$. Επίσης, ισχύει ότι $w(\zeta^j) = e(\zeta^j) + \upsilon(\zeta^j)$. Εξ ορισμού για έναν BCH-κώδικα ισχύει $\upsilon(\zeta^j) = 0$ για κάθε j τέτοιο ώστε $c \le j \le c + d - 2$. Επομένως, $w(\zeta^j) = e(\zeta^j)$.

Έστω $r \le \left[\frac{d-1}{2}\right]$. Υποθέτουμε ότι μπορούμε να διορθώσουμε r λάθη. Έστω ότι $e = \sum_{i \in J} e_i X^i$ όπου $J = \{i_1, i_2, \ldots, i_r\}$ όπου τα i_λ μας δείχνουν τις θέσεις λάθους. Σχηματίζουμε το ακόλουθο σύστημα γραμμικών εξισώσεων $S_j = \sum_{i \in J} e_i \zeta^{ij} = 0$ για j με $c \le j \le c + d - 2$. Εδώ γνωστά είναι τα S_j και άγνωστοι οι δείκτες που ανήκουν στο J και τα e_i, $i \in J$.

Ορίζουμε το πολυώνυμο $S := S(X) = \prod_{i \in J} (X - \zeta^i) = s_0 + s_1 X + \ldots + s_{r-1} X^{r-1} + s_r X^r$.

Προκύπτει το σύστημα

$$
\begin{aligned}
&S_c s_0 + S_{c+1} s_1 + \ldots + S_{c+r-1} s_{r-1} = -S_{c+r} \\
&S_{c+1} s_0 + S_{c+2} s_1 + \ldots + S_{c+r} s_{r-1} = -S_{c+r+1} \\
&\ldots \\
&S_{c+r-1} s_0 + S_{c+r} s_1 + \ldots + S_{c+2r-2} s_{r-1} = -S_{c+r+1}
\end{aligned}
$$

Ο πίνακας των συντελεστών είναι

$$
S = \begin{bmatrix} S_c & S_{c+1} & \ldots & S_{c+r-1} \\ S_{c+1} & S_{c+2} & \ldots & S_{c+r} \\ \vdots & \vdots & \ldots & \vdots \\ S_{c+r-1} & S_{c+r} & \ldots & S_{c+2r-2} \end{bmatrix}
$$

Γράφουμε τον πίνακα στην μορφή $S = VDV^T$ όπου

$$
V = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \zeta^{i_1} & \zeta^{i_2} & \ldots & \zeta^{i_r} \\ \vdots & \vdots & \ldots & \vdots \\ \zeta^{i_1(r-1)} & \zeta^{i_2(r-1)} & \ldots & \zeta^{i_r(r-1)} \end{bmatrix} \text{ και } D = \begin{bmatrix} e_1\zeta^{i_1 c} & & & \\ & e_2\zeta^{i_2 c} & & \\ & & \ddots & \\ & & & e_r\zeta^{i_r c} \end{bmatrix}.
$$

Ο S είναι αντιστρέψιμος αν και μόνο αν $\det S \neq 0$ δηλαδή αν $\det V \neq 0$. Ο πίνακας D είναι Vandermonde άρα $\det V \neq 0$ αν και μόνο αν $e_1, e_2, \ldots, e_r$ είναι όλα διαφορετικά μεταξύ τους ανά δύο.

Άμεση συνέπεια των παραπάνω είναι το ακόλουθο

Λήμμα 6.7 Το παραπάνω σύστημα έχει μοναδική λύση αν και μόνο αν εμφανίζονται τουλάχιστον r λάθη.

Ο μέγιστος αριθμός r τέτοιος ώστε το σύστημα να λύνεται μονοσήμαντα είναι ακριβώς ο αριθμός των θέσεων που μπορεί να εμφανιστεί λάθος. Αν λύσουμε το σύστημα βρίσκουμε ένα πολυώνυμο. Από αυτό βρίσκουμε τις θέσεις λάθους.

Παρατήρηση 6.8 Στην περίπτωση τον δυαδικών BCH κωδίκων αν βρούμε μια θέση λάθους μπορούμε και να τη διορθώσουμε.

Για να αποκωδικοποιήσουμε έναν BCH-κώδικα εφαρμόζουμε, σύμφωνα με τα παραπάνω, τον ακόλουθο αλγόριθμο.

Αλγόριθμος αποκωδικοποίησης BCH-κωδίκων

Έστω ότι μπορούν να εμφανιστούν t το πολύ λάθη όπου $d \geq 2t + 1$.
(Το d είναι του ορισμού του BCH-κώδικα).

Υποθέτουμε ότι στείλαμε το διάνυσμα υ και πήραμε w.

Βήμα 1 Υπολογίζουμε το σύνδρομο $S(w) = (S_c, S_{c+1}, \ldots, S_{c+d-2})$

Βήμα 2 Ορίζουμε τον μέγιστο αριθμό $r \leq t$ εξισώσεων της μορφής

$$S_j s_0 + S_{j+1} s_1 + \ldots + S_{j+r-1} s_{r-1} + S_{c+r} = 0, \text{ όπου } c \leq j \leq c + r - 1$$

έτσι ώστε ο πίνακας των συντελεστών να είναι μη-ιδιάζων (non-singular). Έτσι βρίσκουμε τον αριθμό των λαθών r που εμφανίζονται. Λύνουμε το σύστημα που σχηματίσαμε και βρίσκουμε το πολυώνυμο λάθους $s = \sum_{i=0}^{r} s_i X^i$

Βήμα 3 Βρίσκουμε τις ρίζες του s δοκιμάζοντας τις τιμές $\zeta^0 = 1, \zeta^1, \zeta^2, \ldots$

Βήμα 4 Για δυαδικό κώδικα αν $\zeta^{i_1}, \zeta^{i_2}, \ldots, \zeta^{i_r}$ είναι οι ρίζες του πολυωνύμου s, αυτές μας δίνουν το διάνυσμα (πολυώνυμο) λάθους.
Αλλιώς τα e_i θα τα πάρουμε από τις εξισώσεις $\sum_{i \in J} e_j \zeta^{ij} = 0$ για $j \in \{c, c + 1, \ldots, c + d - 2\}$.

Παρατήρηση 6.9 Το δύσκολο βήμα είναι το 2. Υπάρχουν σχετικοί αλγόριθμοι (για παράδειγμα Berlekamp και Massey).

Παράδειγμα 6.10 Έστω c = 1, n = 15, q = 2. Θεωρούμε τον BCH κώδικα $C = \langle g \rangle$, όπου $g = 1 + X^4 + X^6 + X^7 + X^8$, με προκαθορισμένη ελάχιστη απόσταση 5. Υποθέτουμε ότι πήραμε το w = 100 100 110 000 100 που αντιστοιχεί στο πολυώνυμο $w = 1 + X^3 + X^6 + X^7 + X^{12}$. Για την αποκωδικοποίηση θα χρησιμοποιήσουμε τον παραπάνω αλγόριθμο.

Υπολογίζουμε το σύνδρομο $S_1 = e(\zeta^1) = w(\zeta^1) = 1 + \zeta^3 + \zeta^6 + \zeta^7 + \zeta^{12} = 1 + \zeta^3 + (\zeta^3 + \zeta^2) + (\zeta^3 + \zeta + 1) + (\zeta^3 + \zeta^2 + \zeta + 1) = 1$.

Ομοίως,

$S_2 = e(\zeta^2) = w(\zeta^2) = 1 + \zeta^6 + \zeta^{12} + \zeta^{14} + \zeta^9 =$
$= 1 + (\zeta^3 + \zeta^2) + (\zeta^3 + \zeta^2 + \zeta + 1) + (\zeta^3 + 1) + (\zeta^3 + \zeta)$
$= 1$
$S_3 = e(\zeta^3) = w(\zeta^3) = 1 + \zeta^9 + \zeta^3 + \zeta^6 + \zeta^6 = 1 + \zeta^3 + \zeta + \zeta^3 = 1 + \zeta = \zeta^4$
$S_4 = e(\zeta^3) = w(\zeta^3) = 1 + \zeta^{12} + \zeta^9 + \zeta^{13} + \zeta^3 = 1$

Έχουμε ότι $t = \left[\frac{5-1}{2}\right] = 2$ άρα $r \leq 2$. Το βήμα 2 μας δίνει το σύστημα:

$$\begin{matrix} S_1 s_0 + S_2 s_1 = S_3 \\ S_2 s_0 + S_3 s_1 = S_4 \end{matrix} \quad \text{ή} \quad \begin{matrix} s_0 + s_1 = \zeta^4 \\ s_0 + \zeta^4 s_1 = 1 \end{matrix}$$

Το σύστημα έχει μοναδική λύση αφού $\begin{vmatrix} 1 & 1 \\ 1 & \zeta^4 \end{vmatrix} = \zeta^4 + 1 = \zeta \neq 0$. Άρα υπάρχουν δύο λάθη (r = 2). Το σύστημα έχει λύση $s_0 = \zeta^4 + 1 = \zeta$ και $s_1 = 1$ άρα το πολυώνυμο s είναι το $s = s_0 + s_1 X + X^2 = \zeta + X + X^2$. Βρίσκουμε τις ρίζες του οι οποίες θα μας δώσουν τις θέσεις των λαθών. Το s έχει στο $\mathbf{F}_{16}$ δύο ρίζες, τις ζ^7 και ζ^9. Άρα τα λάθη εμφανίζονται στις θέσεις 8 και 10. Το λάθος είναι το $e = X^7 + X^9$ και το πολυώνυμο υ το $\upsilon = w - e = 1 + X^3 + X^6 + X^9 + X^{12}$. Άρα μας έχουν στείλει το πολυώνυμο υ mod g $= 1 + X + X^4$, δηλαδή το μήνυμα 1100100.