3. Κώδικες Hamming

Πρόκειται για κώδικες που διορθώνουν ένα το πολύ λάθος και είναι εύκολοι στην κωδικοποίηση και στην αποκωδικοποίηση.

Ορισμός 3.1 Έστω C (n, k)-γραμμικός κώδικας στο σώμα $\mathbf{F}_q$. Έστω το διάνυσμα α του διανυσματικού χώρου $\mathbf{F}_q^n$. Ορίζουμε **coset** (σύμπλοκο) του διανύσματος α το σύνολο $\alpha + C = \{\alpha + x \mid x \in C\}$.

Παρατηρήσεις 3.2

(i) Κάθε διάνυσμα b του $\mathbf{F}_q^n$ ανήκει σε κάποιο coset. Δηλαδή υπάρχει $y \in \mathbf{F}_q^n$ τέτοιο ώστε $b = y + C$ ή αλλιώς $y \in \mathbf{F}_q^n$ τέτοιο ώστε $b - y = x \in C$.

(ii) Έστω $a, b \in \mathbf{F}_q^n$. Τα a, b ανήκουν στο ίδιο coset αν και μόνο αν $a - b \in C$.

(iii) Κάθε coset έχει q^k στοιχεία

Απόδειξη

(i) Επειδή ο κώδικας C είναι γραμμικός το μηδενικό διάνυσμα ανήκει σ' αυτόν επομένως αν πάρουμε ένα διάνυσμα b του $\mathbf{F}_q^n$ αυτό θα ανήκει στο coset b + C.

(ii) $a, b \in \mathbf{F}_q^n$ ανήκουν στο ίδιο coset $\Leftrightarrow a + C = b + C \Leftrightarrow$ υπάρχουν $x, y \in C$ τέτοια ώστε $a + x = b + y \Leftrightarrow a - b = y - x$ με $x, y \in C \Leftrightarrow a - b \in C$.

(iii) Ο κώδικας C έχει q^k στοιχεία. Έστω $x, y \in C$ τότε $[a + x = a + y \Leftrightarrow x = y]$ επομένως και κάθε coset έχει q^k στοιχεία, όσα στοιχεία έχει και ο γραμμικός κώδικας C.

Πρόταση 3.3 Δυο οποιαδήποτε στοιχεία cosets είναι ξένα μεταξύ τους ή συμπίπτουν

Απόδειξη

Έστω $a, b \in \mathbf{F}_q^n$ και έστω a + C, b + C τα αντίστοιχα cosets. Αν είναι ξένα μεταξύ τους τελειώσαμε. Αλλιώς έστω $\gamma \in (a + C) \cap (b + C)$ τότε [$\gamma \in (a + C)$ και $\gamma \in (b + C)$] ή αλλιώς [υπάρχουν $x, y \in C$ τέτοια ώστε $\gamma = a + x$ και $\gamma = b + y$]. Επομένως, $a + x = b + y$. Οπότε $a - b = y - x \in C$, δηλαδή $a + C = b + C$.

Ορισμός 3.4 Ένα διάνυσμα ελάχιστου βάρους ενός coset θα λέγεται **οδηγός** του coset

Το πλήθος των coset είναι $\frac{q^n}{q^k} = q^{n-k}$, δηλαδή

$$\mathbf{F}_q^n = C \cup (\alpha^{(1)} + C) \cup \ldots \cup (\alpha^{(\tau)} + C),$$

όπου $\tau = q^{n-k} - 1$ και το $\cup$ συμβολίζει ξένη ένωση.

Αν πάρουμε το $\mathbf{F}_q^n$ και $y \in \mathbf{F}_q^n$, αυτό θα είναι στοιχείο κάποιου coset $\alpha^{(i)} + C$. Υποθέτουμε ότι στάλθηκε η κωδική λέξη $x \in C$. Το λάθος είναι $e = y - x$, όπου $y \in \alpha^{(i)} + C$. Άρα $y = \alpha^{(i)} + z$, όπου $z \in C$. Επομένως $e = y - x = \alpha^{(i)} + (z - x)$, με $(z - x) \in C$. Άρα $e \in \alpha^{(i)} + C$.

Επομένως, το διάνυσμα λάθους ανήκει στο ίδιο coset που ανήκει και το y.

Αξίωμα 3.5 Το πιο πιθανό λάθος είναι ένα διάνυσμα του coset με το μικρότερο δυνατό βάρος.

Συνεπώς, αποκωδικοποιούμε στο $x = y - e$, όπου e ο οδηγός του coset.

Παράδειγμα 3.6 Αν $q = 2$ και $(n, k) = (4, 2)$ κώδικας με γεννήτορα πίνακα

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Σχηματίζουμε τα cosets ως εξής:

Από τα μηνύματα και τον γεννήτορα πίνακα G βρίσκουμε τις κωδικές λέξεις. Στη συνέχεια επιλέγουμε ένα τυχαίο διάνυσμα με ελάχιστο βάρος που δεν είναι κωδική λέξη. Σχηματίζουμε το coset που του αντίστοιχεί προσθέτοντας το διάνυσμα σε όλες τις κωδικές λέξεις. Συνεχίζουμε με τον ίδιο τρόπο διαλέγοντας κάθε φορά ένα διάνυσμα με ελάχιστο βάρος που δεν ανήκει σε κανένα από τα cosets που έχουμε κατασκευάσει.

Μηνύματα	00	10	01	11
Κωδικές λέξεις C	0000	1011	0101	1110
Τυχαίο διάνυσμα με ελάχιστο βάρος	0001			
coset 0001	0001	1010	0100	1111
coset 0010	0010	1001	0111	1100
coset 1000	1000	0011	1101	0110
coset 0000	0000	1011	0101	1110

Αν υποθέσουμε ότι πήραμε $y = 1101$, επομένως αποκωδικοποιούμε στο $x = y - e$, όπου e ο οδηγός του coset έχουμε $x = 1101 - 1000 = 0101$.

Για μεγάλους κώδικες είναι μη-πρακτικό, αδύνατο να κατασκευάσουμε τον πίνακα των cosets. Τα πράγματα γίνονται πιο εύκολα αν παρατηρήσουμε ότι

$$Hw^T = H(\alpha + x)^T = H(\alpha^T + x^T) = H\alpha^T + Hx^T = H\alpha^T$$

Ορισμός 3.7 Έστω C γραμμικός κώδικας τύπου (n, k) με πίνακα ελέγχου ισοτιμίας H. Αν $y \in \mathbf{F}_q^n$, **σύνδρομο** του y ορίζεται το $S(y) := Hy^T$.

Ιδιότητες 3.8

(α) S(y) διάνυσμα μήκος $(n - k)$

(β) $S(y) = 0 \Leftrightarrow y \in C$
(γ) $S(y) = S(e)$, e ο οδηγός του coset στον οποίο ανήκει το y
(δ) Για δυαδικό κώδικα αν e = 0010…10…0…1

$$\downarrow \quad \downarrow \qquad \downarrow$$

α-θέση b-θέση c-θέση

Το σύνδρομο είναι $S(e) = He^T = H_\alpha + H_b + H_c$, όπου H_i είναι η i-οστή στήλη του H.

Επομένως,

Πρόταση3.9 Σε δυαδικό κώδικα το σύνδρομο είναι ίσο με το άθροισμα των στηλών του πίνακα H στις οποίες εμφανίζεται λάθος.

(ε) Δύο διανύσματα ανήκουν στο ίδιο coset αν και μόνο αν έχουν το ίδιο σύνδρομο.

Απόδειξη
x, y ανήκουν στο ίδιο coset $\Leftrightarrow S(x - y) = 0 \Leftrightarrow H(x - y)^T = 0 \Leftrightarrow Hx^T - Hy^T = 0 \Leftrightarrow Hx^T = Hy^T \Leftrightarrow S(x) = S(y)$

Αλγόριθμος Αποκωδικοποίησης
Έστω ότι πήραμε κάποιο $y \in \mathbf{F}_q^n$. Υπολογίζουμε το σύνδρομο S(y). Βρίσκουμε τον οδηγό e για τον οποίο S(e) = S(y). Αποκωδικοποιούμε στο x = y – e.

Από τα προηγούμενα, φαίνεται ότι χρειαζόμαστε μόνο τους οδηγούς των cosets αλλά και αυτών το πλήθος μπορεί να είναι μεγάλο. Για παράδειγμα αν (n, k) = (50, 20) στο $\mathbf{F}_2$ έχουμε $\frac{2^{50}}{2^{20}} = 2^{30} \sim 10^9$ cosets.
Επιθυμούμε να κατασκευάσουμε κώδικες που να διορθώνουν το πολύ ένα λάθος (1-error correcting codes). Άρα, ο κώδικας θα ανιχνεύει την ύπαρξη τουλάχιστον ενός λάθους. Επομένως, θα πρέπει όλες οι στήλες του πίνακα H να μην είναι μηδενικές, διότι αν η i-οστή στήλη είναι μηδενική δεν θα μπορούσαμε να ανιχνεύσουμε την ύπαρξη λάθους στην i-οστή θέση. Επίσης, θα πρέπει οι στήλες του πίνακα H να είναι ανά δύο διαφορετικές μεταξύ τους, αλλιώς δεν θα μπορούσαμε να διαπιστώσουμε τη θέση του λάθους.

Ορισμός 3.10 Έστω $m \in \mathbf{N}$, $m \geq 2$. Ο κώδικας C_m τύπου (n, k), $n = 2^m - 1$, $k = 2^m - 1 - m$ θα λέγεται **δυαδικός κώδικας Hamming**, όταν ο πίνακας ισοτιμίας $H \in M_{m \times n}(\mathbf{F}_2)$ έχει σαν στήλες όλες τις δυνατές, μη-μηδενικές, στήλες μήκους m που μπορούμε να κατασκευάσουμε.

Παράδειγμα 3.11 Έστω m = 3, $n = 2^3 - 1 = 7$, k = n – m = 7 – 3 = 4. Ο κώδικας Hamming C_3 είναι ένας (7, 4) – κώδικας (δυαδικός) με πίνακα ελέγχου ισοτιμίας

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

1 2 3 4 5 6 7 (στο δυαδικό σύστημα αρίθμησης)

Υποθέτουμε ότι στην k-στή θέση της λέξης $y = y_1y_2 \ldots y_7$ που πήραμε υπάρχει μοναδικό λάθος. Τότε το σύνδρομο είναι $S(y) = Hy^T = H_k$, η k-στη στήλη του πίνακα H. Το διάνυσμα H_k που θα βρούμε θα το μεταφράσουμε στο δυαδικό σύστημα αρίθμησης και θα βρούμε τη θέση λάθους την οποία και θα διορθώσουμε. Για παράδειγμα αν $S(y) = (101)^T$ τότε επειδή $101_2 = 5$ το λάθος είναι στην πέμπτη θέση.

Επειδή τα διανύσματα είναι ανά δύο γραμμικά ανεξάρτητα (βρισκόμαστε στο σώμα $\mathbf{F}_2$ οπότε οι έννοιες «γραμμικά ανεξάρτητα» και «διαφορετικά μεταξύ τους» διανύσματα είναι ταυτόσημες) αλλά όχι ανά τρία, αφού το άθροισμά τους είναι επίσης διάνυσμα-στήλη του H, έπεται ότι $mld(H) = 3$. Τώρα, ισχύει $d = \dim(C)$ αν και μόνο αν οποιεσδήποτε s στήλες του H, όπου $s \leq d - 1$, είναι γραμμικά ανεξάρτητες. Άρα $d - 1 = 2$ οπότε $d = 3$.

Πρόταση 3.12 Οι δυαδικοί κώδικες Hamming είναι τέλειοι.

Απόδειξη Επειδή $d = 3$ έπεται ότι ο (n, k)-κώδικας Hamming C_m είναι 1-error correcting οπότε ο σφαίρες κέντρου κωδικής λέξης και ακτίνας 1 είναι ξένες μεταξύ τους. Αν $c \in C_m$ τότε $S_1(c) = 1 + \binom{n}{1} = n + 1$ διανύσματα ανήκουν σε κάθε σφαίρα και έχουμε 2^k σφαίρες. Συνολικά όλες περιέχουν $(n + 1)2^k = (2^m - 1 + 1)2^{n-m} = 2^n$ λέξεις. Άρα ο κώδικας είναι τέλειος.

Παρατηρήσεις 3.13

1. Οι δυαδικοί κώδικες Hamming είναι **κυκλικοί** (η έννοια θα οριστεί στην επόμενη παράγραφο).
2. Οι δυαδικοί κώδικες Hamming είναι **τέλειοι** (μόλις το έχουμε αποδείξει).
3. Γενικευμένοι κώδικες Hamming.

   Στο $\mathbf{F}_q$ θεωρούμε τον πίνακα $H \in M_{m \times n}(\mathbf{F}_q)$ όπου $n = \frac{q^m - 1}{q - 1}$ και δύο οποιεσδήποτε στήλες δεν είναι η μια πολλαπλάσιο της άλλης. Παίρνουμε τον κώδικα Hamming C_m τύπου $\left(\frac{q^m - 1}{q - 1}, \frac{q^m - 1}{q - 1} - m, 3 \right)$
4. Οι κώδικες Hamming είναι 1-error correcting. Γενίκευσή τους αποτελούν οι BCH-κώδικες. (Μελέτη στην παράγραφο 6)
5. Αν σε (n, k, d)-κώδικα C προσθέσουμε στο τέλος κάθε λέξης ένα στοιχείο, το αρνητικό άθροισμα των πρώτων n συμβόλων, κατασκευάζουμε ένα κώδικα $\overline{C}$ που λέγεται **επεκτεταμένος**

$$C \rightarrow \overline{C}$$

$$H \mapsto \overline{H} = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 \\ & & & & 0 \\ & & H & & \vdots \\ & & & & 0 \end{pmatrix}$$

Για παράδειγμα ο C_3 (7, 4, 3) κώδικας γίνεται (8, 4, 4) ο οποίος ανιχνεύει 3 λάθη το πολύ (κάτι παραπάνω από τον αρχικό) και διορθώνει 1 λάθος (ότι και ο αρχικός)

6. Ο δυικός ενός δυαδικού κώδικα Hamming C_m $(2^m - 1, 2^m - 1 - m, 3)$ είναι ο **δυαδικός simplex κώδικας** τύπου $(2^m - 1, m, 2^{m-1})$
7. Ο δυικός του επεκτεταμένου ενός δυαδικού κώδικα Hamming C_m $(2^m - 1, 2^m - 1 - m, 4)$ λέγεται κώδικας Reed-Muller πρώτης τάξης και είναι τύπου $(2^m, m + 1, 2^{m-1})$. Για αποκωδικοποίηση χρησιμοποιείται η θεωρία του Fast Fourier Transforms.
   Η NASA (1969 – 1977) χρησιμοποίησε (n, k, d) = (32, 6, 16) Reed Muller κώδικες πρώτης τάξης στο πρόγραμμα Mariner για μεταφορά εικόνας από Σελήνη και Άρη στη Γη.

Εκτός του ότι είναι και οι καλύτεροι κώδικες για δοσμένα n, d οι τέλειοι κώδικες είναι πολύ ενδιαφέροντες για Μαθηματικούς, κυρίως για τα επισυναπτόμενα designs και την ομάδα αυτομορφισμών τους.

Πρόβλημα Να βρεθούν όλοι οι τέλειοι κώδικες

Η προσπάθεια άρχισε με τον M. Golay το 1949 και τελείωσε, εν μέρει, με τους J. H. Lint και A. Tietäväinen.

Κατ' αρχήν, έχουμε μια κλάση τέλειων κωδίκων, τους κώδικες Hamming στο $\mathbf{F}_q$, οι οποίοι είναι τύπου (n, M, d) = $\left(\frac{q^r - 1}{q - 1}, q^{n-r}, 3 \right)$ όπου $r \geq 2$ και q δύναμη πρώτου. Ψάχνοντας για άλλους τέλειους κώδικες μια ιδέα είναι να ψάξουμε για ακέραιους q, M, n, t οι οποίοι να επαληθεύουν την ισότητα στο φράγμα του Hamming, δηλαδή

$$M\left(1 + (q-1)\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}\right) = q^n$$

Ο Golay (1949) απέδειξε ότι υπάρχουν και τρεις άλλοι πιθανοί τύποι, εκτός των παραπάνω του Hamming. Οι $(23, 2^{12}, 7)$ και $(90, 2^{78}, 5)$ για q =2 και $(11, 3^6, 5)$ για q = 3. Ο Golay ασχολήθηκε μόνο με γραμμικούς κώδικες όμως απέδειξε ότι

Θεώρημα 3.14 Δεν υπάρχει γραμμικός $(90, 2^{78}, 5)$-κώδικας αλλά υπάρχει γραμμικός $(23, 2^{12}, 7)$-κώδικας

Ο Golay έδωσε τον γεννήτορα πίνακα του κώδικα, αργότερα δόθηκαν ισοδύναμοι πίνακες. Μειονέκτημα αποτελεί το πως βρέθηκε ο πίνακας.

Για d περιττό υπάρχει δυαδικός (n, M, d)-κώδικας C αν και μόνο αν υπάρχει δυαδικός (n + 1, M, d + 1)-κώδικας $\hat{C}$. Μάλιστα αν ο C είναι γραμμικός τότε είναι και ο $\hat{C}$. Επομένως, η ύπαρξη ενός $(23, 2^{12}, 7)$-κώδικα είναι ισοδύναμη με την ύπαρξη ενός $(24, 2^{12}, 8)$-κώδικα. Θα ορίσουμε κατ' αρχήν τον $\hat{C}$.

Ο κώδικας G_{24} με γεννήτορα πίνακα $G = [\, I_{12} \mid A]$ όπου

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

είναι ένας $(24, 2^{12}, 8)$-κώδικας. Από τον G_{24} παίρνουμε τον G_{23} κώδικα ο οποίος είναι αυτοδυικός και τέλειος.

Για τον τριαδικό (ternary) κώδικα Golay $(11, 3^6, 5)$ δίνουμε γεννήτορα πίνακα του τριαδικού G_{12}. Είναι ο $G = [\, I_6 \mid A]$ όπου

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}$$

Αυτός είναι ένας $(12, 3^6, 6)$-κώδικας punctured στον κώδικα Golay $(12, 3^5, 5)$

Θεώρημα 3.15 (Van Lint – Tietäväinen, 1967) Κάθε μη τετριμμένος τέλειος κώδικας, ως προς το σώμα $\mathbf{F}_q$ όπου q δύναμη πρώτου, έχει τύπο ίδιο με κάποιο κώδικα Hamming ή κώδικα Golay.