Κωδικοποίηση

1. Εισαγωγή και γενικότητες

Ορισμός 1.1

(i) **Αλφάβητο** ονομάζεται το πεπερασμένο σύνολο των συμβόλων (πολλές φορές θα τα ονομάζουμε **γράμματα**) που χρησιμοποιούμε για να καταγράψουμε-διατυπώσουμε ένα μήνυμα. Το αλφάβητό μας θα είναι το πεπερασμένο σώμα $\mathbf{F}_q$ όπου το q είναι δύναμη πρώτου αριθμού.

(ii) Ένα **k-μήνυμα** αποτελείται από μια ακολουθία γραμμάτων των αλφαβήτου μας μήκους k. Είναι δηλαδή της μορφής: $a_1, a_2 \ldots, a_k$ με $a_i \in \mathbf{F}_q$.

(iii) Η αντίστοιχη **κωδική λέξη** x ενός k-μηνύματος είναι μια ακολουθία μήκους n. Είναι δηλαδή της μορφής $x = x_1, x_2 \ldots, x_n$ με $x_i \in \mathbf{F}_q$ και $n \geq k$. Όπου (σχεδόν) πάντα θα ισχύει ότι $x_1 = a_1$, $x_2 = a_2$, …, $x_k = a_k$ ενώ τα υπόλοιπα n – k σύμβολα $(x_{k+1}, x_{k+2}, \ldots, x_n)$ θα τα λέμε **σύμβολα ελέγχου** (**check symbols** ή **control symbols**).

Συμβολισμός 1.2 Οι κωδικές λέξεις θα γράφονται x ή $x_1, x_2, \ldots, x_n$ ή $(x_1, x_2, \ldots, x_n)$ ή $x_1x_2\ldots x_n$.

Ορισμός 1.3 Θα ονομάζουμε **διάνυσμα λήψης** (ή **μήνυμα λήψης**) το διάνυσμα $y = y_1, y_2, \ldots, y_n$ που λαμβάνουμε. Το y εν γένει είναι διαφορετικό από το μήνυμα x που μας στέλνουνε. Το $e := y - x = e_1e_2\ldots e_n$ θα λέγεται **διάνυσμα λάθους** (ή απλά **λάθος**).

Ορισμός 1.4 Ένας **n-κώδικας** C είναι ένα υποσύνολο του $\mathbf{F}_q^n$. Ακριβέστερα ο κώδικας θα λέγεται **(n, k)-κώδικας**, όπου k το μήκος του μηνύματος που κωδικοποιούμε. Αν ο κώδικας C είναι $\mathbf{F}_q$-διανυσματικός υπόχωρος του $\mathbf{F}_q^n$ τότε θα λέγεται **(n, k)-γραμμικός κώδικας**. Τα στοιχεία του C θα είναι οι κωδικές λέξεις.

Όταν πάρουμε το y θα πρέπει να αποφασίσουμε ποια κωδική λέξη μας έχουν στείλει. Θα διαλέγουμε από το σύνολο C μια κωδική λέξη που διαφέρει λιγότερο από το y. Αυτό το αξίωμα ονομάζεται **αποκωδικοποίηση μέγιστης πιθανότητας**.

Ορισμός 1.5 **Απόσταση Hamming** d(x, y) δύο διανυσμάτων x, y στο $\mathbf{F}_q^n$, με

$$x = x_1, x_2 \ldots, x_n \text{ και } y = y_1, y_2 \ldots, y_n,$$

είναι το πλήθος των συντεταγμένων στις οποίες τα x και y διαφέρουν. Δηλαδή

$$d(x, y) = \#\left\{i \in \mathbf{N},\ 1 \leq i \leq n \middle|\ x_i \neq y_i\right\}$$

Ορισμός 1.6 **Βάρος (weight) Hamming** w(x) ενός διανύσματος $x = x_1, x_2 \ldots, x_n$ στο $\mathbf{F}_q^n$ είναι το πλήθος των μη-μηδενικών συντεταγμένων του x. Δηλαδή,

$$w(x) = \#\{i \in \mathbf{N},\ 1 \le i \le n \mid x_i \neq 0\}$$

Προφανώς, $w(x) = d(x, 0)$.
Παράδειγμα 1.7 Έστω $C \subseteq \mathbf{F}_3^4$.
Το βάρος Hamming του 1201 είναι $w(1201) = 3$.
Η απόσταση Hamming των 1201 και 2211 είναι $d(1201, 2211) = 2$.

Παρατήρηση 1.8 Η απόσταση Hamming d(C) είναι μια μετρική στον $\mathbf{F}_q^n$ και το βάρος Hamming w είναι μια νόρμα στον $\mathbf{F}_2^n$.

Ορισμός 1.9 Αν $C \subseteq \mathbf{F}_q^n$ ένας (n, k)-κώδικας, **η ελάχιστη απόσταση $d_{min}(C)$ του κώδικα** είναι

$$d_{min}(C) = \min_{\substack{u,v \in C \\ u \neq v}} d(u, v)$$

Άρα, όταν παίρνουμε το y πρέπει να ελέγχουμε τις q^k κωδικές λέξεις για να βρούμε ποια έχει την μικρότερη απόσταση Hamming από το y. Προφανώς, αυτή η διαδικασία είναι αδύνατη για μεγάλα k και ένας από τους στόχους της θεωρίας κωδίκων είναι να βρει κώδικες με γρηγορότερους αλγόριθμους αποκωδικοποίησης.

Ορισμός 1.10 Το σύνολο $S_r(x) := \{y \in \mathbf{F}_q^n \mid d(x, y) \le r\}$ θα λέγεται η **σφαίρα ακτίνας r ως προς το x** $\in \mathbf{F}_q^n$.

Παράδειγμα 1.11 Έστω $C = \mathbf{F}_2^3$ τότε ο κύκλος με ακτίνα 1 ως προς το 100 είναι

$$S_1(100) = \{100, 000, 110, 101\}.$$

Στόχος Παίρνοντας σφαίρες κατάλληλης ακτίνας r κέντρου κωδικής λέξης θα πρέπει κατά το δυνατό να καλύπτει η ένωσή τους όλο το χώρο $\mathbf{F}_q^n$ ώστε να μπορούμε να αποκωδικοποιούμε όλα τα κωδικοποιημένα μηνύματα που λαμβάνουμε ενώ συγχρόνως η ακτίνα r θα πρέπει να είναι αρκετά μικρή ώστε οι σφαίρες να μην τέμνονται (ή εφάπτονται) και να μπορούμε να αποκωδικοποιούμε μονοσήμαντα.

Πρέπει πάντως να ισχύει ότι $r < \frac{1}{2} d_{min}(C)$.

Η σημασία της ιδέας της ελάχιστης απόστασης δίνεται από την

Πρόταση 1.12 Υποθέτουμε ότι ο C είναι γραμμικός κώδικας με ελάχιστη απόσταση $d_{min}(C) = d$. Ο C **ανιχνεύει** την ύπαρξη d–1 ή λιγότερων λαθών και **διορθώνει** το πολύ e λάθη όπου e τέτοιο ώστε $2e + 1 \le d$.

Απόδειξη Έστω ότι λάβαμε το μήνυμα y με απόσταση f από την κωδική λέξη x, όπου $f \le d–1$. Φανταζόμαστε ότι η x είναι η μεταδιδόμενη (αρχική) λέξη και y η λέξη που πήραμε τελικά. Δηλαδή έχουμε f λάθη κατά την μεταφορά. Επειδή d είναι η ελάχιστη

απόσταση του C η λέξη y καταλαβαίνουμε αμέσως ότι δεν μπορεί να είναι κωδική λέξη. Δηλαδή, ο κώδικας C ανακαλύπτει d – 1 ή λιγότερα λάθη.
Αν τώρα το μήνυμα y έχει απόσταση e από την κωδική λέξη x και $2e + 1 \leq d$ τότε δεν υπάρχει άλλη κωδική λέξη πιο κοντά στη y, διότι αν $d(y, x_1) \leq e$ για κάποια x_1 τότε θα ίσχυε

$$d(x, x_1) \leq d(x, y) + d(y, x_1) \leq e + e < d$$

άτοπο, διότι η ελάχιστη απόσταση του κώδικα C είναι d. Επομένως, υπάρχει μοναδική κοντινότερη λέξη του y και συνεπώς ο C διορθώνει e λάθη σ' αυτήν την περίπτωση.

Ένα από τα βασικά προβλήματα στη θεωρία κωδίκων είναι να ελαχιστοποιηθούν τα λάθη αλλά χωρίς να μειωθεί υποχρεωτικά **η αναλογία της πληροφορίας** $\frac{k}{n}$.
Κεντρικό πρόβλημα της Θεωρίας Κωδίκων είναι το εξής:

Δίνονται d, n, q *φυσικοί αριθμοί όπου q δύναμη πρώτου αριθμού. Να υπολογιστεί ο μέγιστος αριθμός διανυσμάτων, έστω* $A_q(n, d)$*, του διανυσματικού χώρου* $\mathbf{F}_q^n$ *τα οποία ανά δυο να έχουν απόσταση μεγαλύτερη ή ίση με* d*. Φυσικά, αν είναι δυνατόν να βρεθούν τα διανύσματα.*

Το πρόβλημα αυτό χαρακτηρίζεται και σαν discrete sphere packing problem (Conway & Sloan, 1988)

Ο επόμενος πίνακας μας δίνει κάποιες τιμές του $A_2(n, d)$ για d = 3

n	3	4	5	6	7	8	9	10
$A_2(n, 3)$	2	2	4	8	16	20	40	άγνωστος, μεταξύ 72 και 79

Ορισμός 1.13 Ένας κώδικας C ο οποίος **διορθώνει** την ύπαρξη t λαθών θα λέγεται **t-κώδικας διόρθωσης λαθών** (**t-error-correcting code**), ενώ ένας κώδικας C που **ανιχνεύει** e λάθη θα λέγεται **e-κώδικας ανίχνευσης λαθών** (**e-error-detecting code**).

Έστω τώρα C κώδικας ως προς το $\mathbf{F}_q$ μήκους n με πλήθος κωδικών λέξεων M. Υποθέτουμε ότι ο κώδικας είναι ένας t-κώδικας διόρθωσης λαθών. Υπάρχουν $\binom{n}{m}$ διανύσματα του $\mathbf{F}_q^n$ τα οποία να έχουν βάρος m στο $\mathbf{F}_q$. Αν $c \in C$ τότε μέσα στην σφαίρα $S_t(c)$ υπάρχουν $1 + (q-1)2c\binom{n}{1} + \ldots + (q-1)^t\binom{n}{t}$ διανύσματα του $\mathbf{F}_q^n$.

Θεώρημα 1.14 (Φράγμα του Hamming) Οι παράμετροι q, n, t, M ενός t-κώδικα διόρθωσης λαθών C ορισμένου στο σώμα $\mathbf{F}_q$ μήκους n με M κωδικές λέξεις ικανοποιούν την ανισότητα

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

Αν όλα τα διανύσματα του $\mathbf{F}_q^n$ είναι μέσα σε σφαίρες ακτίνας t κέντρου κωδικών λέξεων ενός (n, k)-γραμμικού κώδικα τότε παίρνουμε μια ειδική κατηγορία κωδίκων:

Στην περίπτωση όπου ο κώδικας είναι $\mathbf{F}_2$ – διανυσματικός υπόχωρος η ανισότητα γράφεται:

$$M\left(1+\binom{n}{1}+\ldots+\binom{n}{t}\right)\leq 2^n.$$

Ορισμός 1.15 Ένας t-κώδικας διόρθωσης λαθών ορισμένος στο σώμα $\mathbf{F}_q$ θα ονομάζεται **τέλειος** αν στο θεώρημα 1.16 ισχύει η ισότητα.

Αν ο C είναι κώδικας όπως αυτός του θεωρήματος 1.14 με $d_{min}(C) = d = 2t + 1$, τότε αν διαγράψουμε τα τελευταία d – 1 σύμβολα πάλι έχουμε έναν κώδικα με όλες τις κωδικές λέξεις διαφορετικές. Ο κώδικας που προκύπτει έχει μήκος n – d + 1, και παίρνουμε το

Θεώρημα 1.16 (Φράγμα του Singleton) Αν ένας κώδικας $C \subseteq \mathbf{F}_q^n$ έχει ελάχιστη απόσταση d, τότε $|C| \leq q^{n-d+1}$ ή αλλιώς $k \leq n - d + 1$.

Ορισμός 1.17 Ένας κώδικας C θα λέγεται **διαχωρίσιμος μέγιστης απόστασης** (**maximum distance separable**) ή πιο απλά **κώδικας MDS** αν στο θεώρημα 1.16 ισχύει η ισότητα.

Παράδειγμα 1.18 Έστω ο κώδικας

$$C=\{000000,\ 001011,\ 010101,\ 011110,\ 100110,\ 101101,\ 110011,\ 111000\}\subseteq \mathbf{F}_2^6$$

όπου $d_{min}(C) = 3$. Έχουμε επομένως, M = 8, q = 2, n = 6, d = 3, t = 1. Το φράγμα του Hamming δίνει την ανισότητα $8\left(1+\binom{6}{1}\right)\leq 2^6$, δηλαδή 56 < 64. Αυτό σημαίνει ότι μόνο 64 – 56 = 8 λέξεις μήκους 6 στο $\mathbf{F}_2^6$ βρίσκονται έξω από κάποια σφαίρα και δεν μπορούν να διορθωθούν σωστά (αυτό είναι προφανές και από το γεγονός ότι έχουμε 8 μη τεμνόμενες σφαίρες με 7 στοιχεία η κάθε μια). Ένα παράδειγμα μιας από τις 8 λέξεις που δεν μπορούν να διορθωθούν σωστά είναι η 100100 η οποία έχει απόσταση μεγαλύτερη ή ίση του 2 από όλες τις κωδικές λέξεις. Το φράγμα του Singleton μας δίνει $8 \leq 2^4 = 16$, άρα ο C δεν είναι MDS.

Τα φράγματα μας δείχνουν τα όρια μας. Μεγάλη έκπληξη αποτέλεσε το **θεώρημα του Shannon** (1948) ότι υπάρχουν όσο καλοί κώδικες θέλουμε.

2. Γραμμικοί κώδικες

Ας υποθέσουμε τώρα ότι τα σύμβολα ελέγχου μπορούν να προκύψουν από το k-μήνυμα με τέτοιο τρόπο ώστε οι κωδικές λέξεις x να ικανοποιούν το σύστημα με γραμμικές εξισώσεις

$$Hx^T = 0,$$

όπου H είναι ένας δοσμένος $(n - k) \times n$ πίνακας με στοιχεία από το σώμα $\mathbf{F}_q$. Η **κανονική μορφή** για τον H είναι $[A \mid I_{n-k}]$ όπου A ένας $(n - k) \times k$ πίνακας και I_{n-k} ο $(n - k) \times (n - k)$ μοναδιαίος πίνακας.

Προκύπτει ο παρακάτω

Ορισμός 1.21 Έστω H ένας $(n - k) \times n$ πίνακας με βαθμό $n - k$ και στοιχεία από το σώμα $\mathbf{F}_q$. Το σύνολο όλων των n-διάστατων διανυσμάτων x που ικανοποιούν την εξίσωση $Hx^T = 0$ ονομάζονται **γραμμικός κώδικας** C πάνω από το $\mathbf{F}_q$ με **μήκος** n. Ο πίνακας H είναι ο **πίνακας ελέγχου ισοτιμίας (parity-check matrix)** του κώδικα C ο οποίος ονομάζεται και γραμμικός (n, k)-κώδικας. Αν ο H είναι στην μορφή $[A \mid I_{n-k}]$ τότε τα πρώτα k σύμβολα από την κωδική λέξη x είναι το αρχικό k-μήνυμα, ενώ τα υπόλοιπα $n - k$ σύμβολα του x είναι τα σύμβολα ελέγχου. Ο C ονομάζεται επίσης **συστηματικός γραμμικός (n, k)-κώδικας** και τότε θεωρούμε ότι ο H είναι στην **κανονική μορφή**. Αν q = 2 τότε ο C ονομάζεται **δυαδικός κώδικας** (**binary code**).

Παρατήρηση 2.1 Το σύνολο C των λύσεων x της $Hx^T = 0$ (ή αλλιώς ο **μηδενόχωρος** του H) είναι ένας υπόχωρος του διανυσματικού χώρου $\mathbf{F}_q^n$ με διάσταση k. Επειδή οι κωδικές λέξεις είναι προσθετική ομάδα, ο C ονομάζεται επίσης **κώδικας-ομάδα**.

Ιδιότητες γραμμικών κωδίκων 2.2

1. $x \in C \Leftrightarrow Hx^T = 0$
2. Ο πίνακας ελέγχου ισοτιμίας H του κώδικα C γράφεται σε κανονική μορφή $H = [A \mid I_{n-k}]$
3. Ο πίνακας $G = [I_k \mid -A^T]$ ονομάζεται (**κανονικός**) **γεννήτορας πίνακας** του κώδικα C με πίνακα ελέγχου ισοτιμίας $H = [A \mid I_{n-k}]$ στην κανονική μορφή λόγω του ότι ισχύει $x = uG$ οι κωδικές λέξεις είναι γραμμικοί συνδυασμοί των γραμμών του G.

Ισχύει: $GH^T = HG^T = 0$.

Παράδείγμα 2.3

$$\text{Αν } H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \text{ τότε } G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Από τις τρεις γραμμές του πίνακα παίρνουμε τον (3, 6)-κώδικα $C \subseteq \mathbf{F}_2^6$ ο οποίος αποτελείται από 8 κωδικές λέξεις:

$$000000,\ 100110,\ 010101,\ 001011,\ 110011,\ 011110,\ 101101,\ 111000$$

Όπως και πριν κάθε κωδική λέξη x μπορεί να περιγραφεί σαν διανύσμα της μορφής $x = uG$, όπου $u = u_1u_2u_3$ με $u_i \in \mathbf{F}_2$.

Υπάρχουν τέσσερις κωδικές λέξεις βάρους 3, τρεις κωδικές λέξεις βάρους 4 και μια κωδική λέξη βάρους 0. Η ελάχιστη απόσταση του κώδικα είναι 3, επομένως ανιχνεύει την ύπαρξη το πολύ δύο λαθών και διορθώνει το πολύ ένα λάθος.

Θεώρημα 2.4 Έστω G ο γεννήτορας πίνακας ενός γραμμικού κώδικα C. Τότε οι γραμμές του G σχηματίζουν μια βάση του C.

Απόδειξη Οι k γραμμές του πίνακα G είναι γραμμικώς ανεξάρτητες από τον ορισμό του γεννήτορα πίνακα ενός γραμμικού κώδικα. Αν r είναι ένα διάνυσμα-γραμμή του G τότε $rH^T = 0$ άρα και $Hr^T = 0$ για κάθε $r \in C$. τώρα, dimC είναι η διάσταση του μηδενόχωρου του H, η οποία είναι $n - \text{rank}(H) = k$. Επομένως, οι k γραμμές του G σχηματίζουν μια βάση του C.

Ένας κώδικας μπορεί να έχει πολλούς πίνακες ελέγχου ισοτιμίας και γεννήτορες πίνακες. Κάθε $k \times n$ πίνακας του οποίου ο χώρος γραμμών είναι ίσος με τον C μπορεί να είναι επίσης ένας γεννήτορας πίνακας του C.

Αν ο «γεννήτορας πίνακας» H δεν είναι στην κανονική μορφή μπορούμε να τον μετατρέψουμε σε ένα πίνακα της μορφής $[I_k \mid -A^T]$ χωρίς να αλλάξουμε τον μηδενόχωρο του H, δηλαδή τον κώδικα C. Μετά μετατρέπουμε τις συντεταγμένες για να σχηματίσουμε τον πίνακα H' ο οποίος να είναι σε κανονική μορφή. Οι συντεταγμένες του κώδικα C' που αντιστοιχεί στον H' είναι «ισοδύναμος» με τον C με την ακόλουθη έννοια:

Ορισμός 2.5 Δύο κώδικες C και C' ίδιου μήκους n θα λέγονται **ισοδύναμοι** αν υπάρχει μια μετάθεση π του συνόλου $\{1, 2, \ldots, n\}$ τέτοια ώστε

$$(x_1, \ldots, x_n) \in C \Leftrightarrow \left(x_{\pi(1)}, \ldots, x_{\pi(n)}\right) \in C'$$

Έτσι, σχηματίζουμε τον γεννήτορα πίνακα G' του πίνακα C' και ύστερα εφαρμόζουμε την αντίστροφη μετάθεση π^{-1} στις συντεταγμένες.

Το επόμενο αποτέλεσμα μας δείχνει ότι για κάθε γραμμικό κώδικα, η ελάχιστη απόσταση μπορεί να υπολογισθεί από το βάρος Hamming των κωδικών λέξεων.

Μια από τις πιο σημαντικές ιδιότητες των γραμμικών κωδίκων είναι η παρακάτω

Πρόταση 2.6 Έστω C ένας γραμμικός (n, k)-κώδικας. Η ελάχιστη απόσταση του C είναι ίση με το ελάχιστο δυνατό βάρος που έχει κωδική λέξη διάφορη του μηδενικού στοιχείου.

Απόδειξη Έστω w το ελάχιστο δυνατό βάρος Hamming κωδικής λέξης διάφορης του μηδενικού στοιχείου 0. Έστω $x \in C$ μια κωδική λέξη βάρους Hamming w. Τότε ισχύει ότι $d(x, 0) = w(x) = w$. Επομένως, ισχύει ότι $w \geq d_{min}(C)$. Τώρα έστω u και v ένα ζευγάρι κωδικών λέξεων του C με απόσταση τέτοια ώστε $d(u, v) = d_{min}(C)$. Αφού C γραμμικός κώδικας έπεται ότι και η $u - v$ είναι επίσης κωδική λέξη. Η $u - v$ έχει βάρος $d_{min}(C)$. Επομένως, $d_{min}(C) \geq w$. Δηλαδή, $d_{min}(C) = w$.

Ορισμός 2.7 Ένα γραμμικός κώδικας C μήκους n, διάστασης k και ελάχιστης απόστασης d θα ονομάζεται **(n, k, d)-κώδικας**.

Έστω τώρα, $u = u_1, \ldots, u_n$ και $v = v_1, \ldots, v_n$ δύο διανύσματα του διανυσματικού χώρου $\mathbf{F}_q^n$ και έστω $u \cdot v = u_1v_1 + \ldots + u_nv_n$ να συμβολίζει το γινόμενο των u και v πάνω από τον $\mathbf{F}_q^n$. Αν $u \cdot v = 0$ τότε τα u και v θα λέγονται **ορθογώνια**.

Ορισμός 2.8 Έστω C ένας γραμμικός (n, k)-κώδικας ορισμένος στο σώμα $\mathbf{F}_q$. Ο **ορθογώνιος κώδικας** $C^{\perp}$ του κώδικα C ορίζεται να είναι ο

$$C^{\perp} = \{u \mid uv = 0 \text{ για κάθε } v \in C\}$$

Επειδή ο C είναι ένας k-διάστατος υπόχωρος του n-διάστατου διανυσματικού χώρου $\mathbf{F}_q^n$ το ορθογώνιο συμπλήρωμα του C είναι διάστασης $n - k$ και είναι ένας $(n, n - k)$ κώδικας. Μπορεί να αποδειχτεί ότι αν ο κώδικας C έχει γεννήτορα τον πίνακα G και πίνακα ελέγχου ισοτιμίας H τότε ο $C^{\perp}$ έχει γεννήτορα πίνακα τον H και πίνακα ελέγχου ισοτιμίας του G. Η ορθογωνιότητα των δύο κωδίκων μπορεί να εκφραστεί από τη σχέση $GH^T = HG^T = 0$. Τώρα θα συνοψίσουμε κάποιες απλές ιδιότητες των γραμμικών κωδίκων.

Παρατήρηση 2.9 Έστω mld(H) ο ελάχιστος αριθμός γραμμικά εξαρτημένων στηλών του H. Επειδή οποιεσδήποτε rank(H) + 1 το πλήθος στήλες του H είναι γραμμικά εξαρτημένες προφανώς ισχύει, $mld(H) \leq rank(H) + 1$ για κάθε πίνακα H.

Θεώρημα 2.10 Έστω H ένας πίνακας ελέγχου ισοδυναμίας ενός (n, k, d)-κώδικα C με $n > k$. Τότε ισχύουν:

(i) $\dim C = k = n - rank(H)$
(ii) $d = mld(H)$
(iii) $d \leq n - k + 1$.

Απόδειξη Το (i) είναι προφανές ενώ το (iii) προκύπτει από το (ii) και την προηγούμενη παρατήρηση. Για να αποδείξουμε το (ii) ας υποθέσουμε ότι ο H έχει στήλες $s_1, \ldots, s_n$. Παίρνουμε μια κωδική λέξη $c = (c_1, \ldots, c_n) \in C$ με βάρος w. Τότε επειδή

$$Hc^T = c_1s_1 + \ldots c_ns_n$$

ισχύει ότι $c_1s_1 + \ldots c_ns_n = 0$. Έχουμε επίσης ότι η c έχει μη-μηδενική συντεταγμένη σε w θέσεις επομένως κάποιες w, και μάλιστα όχι λιγότερες, στο πλήθος στήλες του H είναι γραμμικά εξαρτημένες. Δηλαδή, mld(H) = w. Εφαρμόζοντας την πρόταση 2.6

έχουμε ότι η ελάχιστη απόσταση d του κώδικα είναι ίση με το βάρος της c και συνεπώς το ζητούμενο.

Προκειμένου να επιβεβαιώσουμε την ύπαρξη γραμμικών (n, k)-κωδίκων με ελάχιστη απόσταση d πάνω από το $\mathbf{F}_q$ αρκεί να δείξουμε ότι υπάρχει $(n - k) \times n$ πίνακας H με $mld(H) = d$.

Αναφέρουμε δύο θεωρήματα χωρίς απόδειξη

Θεώρημα 2.11 (Φράγμα των Gilbert – Varshamov)

Αν

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$$

τότε μπορούμε να κατασκευάσουμε έναν γραμμικό (n, k)-κώδικα ορισμένο στο σώμα $\mathbf{F}_q$ με ελάχιστη απόσταση μεγαλύτερη ή ίση από d.

Θεώρημα 2.12 (Φράγμα του Plotkin) Αν υπάρχει ένας γραμμικός κώδικας μήκους n με M κωδικές λέξεις και ελάχιστη απόσταση d πάνω από το $\mathbf{F}_q$ τότε

$$d \leq n \frac{M(q-1)}{(M-1)q}$$

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

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

όπου $\tau = q^{n-k} - 1$ και το $\dot{\cup}$ 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 $\mathrm{mld}(H) = 3$. 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 $n = \dfrac{q^m - 1}{q - 1}$ και δύο οποιεσδήποτε στήλες δεν είναι η μια πολλαπλάσιο της άλλης. Παίρνουμε τον κώδικα Hamming C_m τύπου $\left(\dfrac{q^m - 1}{q - 1}, \dfrac{q^m - 1}{q - 1} - m, 3 \right)$
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.

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 $V_n = \{f(X) \in \mathbf{F}_q[X]$ με deg $f(X) \leq n - 1\} = \{f(X) \in \mathbf{F}_q[X]$ όπου $f(X) = \alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1}X^{n-1}\}$. Ταυτίζουμε (ισομορφία), το $\mathbf{F}_q^n = \{ (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ 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> ≤ 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
(⇒) Έστω $v \in C$ τότε υπάρχει πολυώνυμο α τέτοιο ώστε $v = \alpha * g$. Ισχύει ότι $gh = X^n - 1$, δηλαδή $g*h = 0$, οπότε $v * h = (\alpha * g) * h = \alpha * 0 = 0$.

(⇐) 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

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

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 $m \le j \le n - 1$ 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 $t = \left[\frac{d-1}{2} \right] = 2$. 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

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. $\deg p(X) \le n$
   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

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

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.

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 $I = \{c, c + 1, \ldots, c + d - 2\}$. 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$\{m_{\zeta_i}$ όπου $i \in I\}$
(iii) Ο πίνακας ελέγχου ισοτιμίας είναι ο

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

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 $r \le \left\lfloor \frac{d-1}{2} \right\rfloor$. 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

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

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

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

Ο S είναι αντιστρέψιμος αν και μόνο αν $\det S \ne 0$ δηλαδή αν $\det V \ne 0$. Ο πίνακας D είναι Vandermonde άρα $\det V \ne 0$ 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.

7. Reed-Muller κώδικες

Για κάθε φυσικό αριθμό $m > 0$ και ακέραιο αριθμό r με $0 \le r \le m$ ορίζουμε τον Reed – Muller κώδικα τάξης r σαν τον δυαδικό γραμμικό κώδικα με παραμέτρους $n = 2^m$, $M = 2^k$, $d = 2^m - r$ όπου $k = \left(1 + \binom{m}{1} + \ldots + \binom{m}{r}\right)$. Αυτό τον κώδικα θα τον συμβολίζουμε με R(r, m).

Στη συνέχεια, θα περιοριστούμε στην περίπτωση όπου r = 1. Δηλαδή θα ασχοληθούμε με τον Reed-Muller κώδικα R(m) : = R(1, m), ο οποίος είναι τύπου $(n, M, d) = (2^m, 2^{m+1}, 2^{m-1})$.

Σημείωση 7.1 Ο R(5) χρησιμοποιήθηκε από τους αμερικάνους στο πρόγραμμα Mariner 9 το 1972 για να στείλει ασπρόμαυρες φωτογραφίες από τον Ερμή.

Ορισμός 7.2 Οι Reed-Muller κώδικες R(m) είναι δυαδικοί γραμμικοί κώδικες οι οποίοι ορίζονται για κάθε φυσικό αριθμό m, $m \ge 1$ επαγωγικά ως εξής:

(1) $R(1) = \mathbf{F}_2^2 = \{00, 01, 10, 11\}$
(2) Για $m \ge 1$ ο R(m + 1) ορίζεται $R(m + 1) = \{uu \mid u \in R(m)\} \cup \{uu^c \mid u \in R(m)\}$

Παρατήρηση 7.3 Ο R(1) είναι τύπου $(2, 2^2, 2^0)$ δηλαδή η ελάχιστη απόσταση του κώδικα είναι 1 και αντιστοιχεί στο βάρος όλων των κωδικών λέξεων διαφορετικών των 11 και 00.

Αυτό ισχύει γενικά.

Θεώρημα 7.4 Ο R(m), $m \ge 1$ είναι δυαδικός γραμμικός κώδικας τύπου $(2^m, 2^{m+1}, 2^{m-1})$ όπου κάθε κωδική λέξη, εκτός των 00…0 και 11…1, έχει βάρος 2^{m-1}.

Παράδειγμα 7.5 Όλες οι κωδικές λέξεις του

$$R(2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$$

εκτός των 0000, 1111 έχουν βάρος 2.

Παρατήρηση 7.6 Ο κώδικας R(2) έχει γεννήτορα πίνακα

$$R_2 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

Γενικεύουμε επαγωγικά

Θεώρημα 7.7

1. Ένας γεννήτορας πίνακας του R(1) είναι ο $R_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.

2. Αν R_m γεννήτορας πίνακας του κώδικα R(m) τότε ένας γεννήτορας πίνακας του κώδικα R(m + 1) είναι ο

$$R_{m+1} = \left[\begin{array}{c|c} 00\ldots0 & 11\ldots1 \\ \hline R_m & R_m \end{array}\right].$$

Παράδειγμα 7.8 Ένας γεννήτορας πίνακας του R(3) είναι

$$R_3 = \left[\begin{array}{cccc:cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hdashline 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$$

Θεώρημα 7.9 Ο πίνακας R_m μπορεί να περιγραφεί ως εξής:

- Πρώτη γραμμή: 2^{m-1} μηδενικά ακολουθούμενα από 2^{m-1} μονάδες.
- Δεύτερη γραμμή: Εναλλαγή από μπλοκς μηδενικών και μονάδων μήκους 2^{m-2} το καθένα

…

- i-στή γραμμή: Εναλλαγή από μπλοκς μηδενικών και μονάδων μήκους 2^{m-i} το καθένα

…

- m-στή γραμμή: Εναλλαγή από 0 και 1
- (m + 1)-στή γραμμή: Μόνο μονάδες

Αποκωδικοποίηση των Reed-Muller κωδίκων

Ο Reed-Muller κώδικας R(m) έχει ελάχιστη απόσταση $d = 2^{m-1}$. Επομένως, ο κώδικας διορθώνει το πολύ $\left[\frac{d-1}{2}\right] = \left[\frac{2^{m-1}-1}{2}\right] = 2^{m-2} - 1$ λάθη. Τα διανύσματα μήκους n στον $\mathbf{F}_2$ είναι $2^n = 2^{2^m}$ άρα έχουμε $\frac{2^{2^m}}{2^{m+1}} = 2^{2^m - m - 1}$ cosets.

Για παράδειγμα αν θέλουμε ο κώδικας να διορθώνει 7 λάθη θα πρέπει m = 5. Έχουμε επομένως, $2^{2^5 - 5 - 1} = 2^{26} = 67\ 108\ 864$ cosets. **Καταστροφή** ακόμα και για μικρό m όπως αυτό του Mariner. Άρα πρέπει να ψάξουμε για άλλους τρόπους αποκωδικοποίησης.

Reed – Muller αποκωδικοποίηση

Πρόκειται για ειδικό τύπο του majority logic decoding (αποκωδικοποίηση της πλειοψηφίας).

Ιδέα! Έστω C γραμμικός δυαδικός κώδικας με βάση $B = \{\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_k\}$. Υποθέτουμε ότι στείλαμε την κωδική λέξη $\underline{c} = c_1c_2\ldots c_n$. Αφού το σύνολο B είναι βάση υπάρχουν $a_1, a_2, \ldots, a_k \in \mathbf{F}_2$ τέτοια ώστε $\underline{c} = a_1\underline{b}_1 + \ldots + a_k\underline{b}_k$. Υποθέτουμε ότι μπορούμε να βρούμε διαφορετικούς τρόπους να υπολογίσουμε το a_i από το αντίστοιχο c_i, για παράδειγμα με τέσσερις διαφορετικούς μεταξύ τους, και ότι κάθε φορά χρησιμοποιούμε διαφορετικές συντεταγμένες.

Παράδειγμα 7.10 Υποθέτουμε ότι n = 8 και ότι στάλθηκε η κωδική λέξη $c = c_1c_2\ldots c_8$. Υποθέτουμε ότι το a_1 γράφεται στις μορφές:

$a_1 = c_1 + c_5$
$a_1 = c_2 + c_6$
$a_1 = c_3 + c_7$
$a_1 = c_4 + c_8$

Στη συνέχεια φανταζόμαστε ότι πήραμε, αντί του c που στάλθηκε, το διάνυσμα $x = x_1x_2\ldots x_8$ και υποθέτουμε ότι έχει το πολύ ένα λάθος.

Θα προσπαθήσουμε να υπολογίσουμε το a_1 χρησιμοποιώντας τις συντεταγμένες του διανύσματος x:

$a_1 = x_1 + x_5$
$a_1 = x_2 + x_6$
$a_1 = x_3 + x_7$
$a_1 = x_4 + x_8$

Επειδή στο x υποθέσαμε ότι υπάρχει το πολύ ένα λάθος έπεται ότι από τις 4 σχέσεις που μας δίνουν a_1 το πολύ μια δεν είναι σωστή. Εδώ η πλειοψηφία (majority) είναι τουλάχιστον 3 και μας δίνει την σωστή τιμή για το a_1.

Κάνουμε το ίδιο για όλα τα a_i για i = 1, 2, …, k και έτσι αποκωδικοποιούμε στην κωδική λέξη $\underline{c} = a_1\underline{b}_1 + \ldots + a_k\underline{b}_k$.

Αυτή η μέθοδος λέγεται majority logic decoding.

Στη συνέχεια θα μελετήσουμε τον γεννήτορα πίνακα R_m. Συμβολίζουμε τις γραμμές του R_m με $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_m, \ldots, \underline{b}_{m+1}$. Αυτές αποτελούν βάση του κώδικα R(m).

Υποθέτουμε ότι στάλθηκε το $\underline{c} = c_1c_2\ldots c_n$. Ισχύει ότι,

$$\underline{c} = a_1\underline{b}_1 + \ldots + a_m\underline{b}_m + a_{m+1}\underline{b}_{m+1}.$$

Επιθυμούμε να βρούμε όσο πιο πολλές εκφράσεις γίνεται των $a_i \in \mathbf{F}_2$ συναρτήσει των c_i για κάθε i = 1, …, k.

Υποθέτουμε ότι ένα διάνυσμα x_i είναι ορθογώνιο σε κάθε άλλη γραμμή πλην της $\underline{b}_i$ ενώ ισχύει $x_ib_i = 1$. Τότε $x_ic = x_i(a_1\underline{b}_1 + \ldots + a_m\underline{b}_m + a_{m+1}\underline{b}_{m+1}) = a_i(x_i\underline{b}_i) = a_i$.

Ερώτημα Πως θα βρούμε τέτοια διανύσματα x_i;

Γράφουμε τις συνιστώσες του διανύσματος $\underline{b}_i$. Έστω ότι $\underline{b}_i = b_{i1}b_{i2}\ldots,b_{in}$ και έστω $\underline{e}_\lambda = 0\ldots010\ldots0$ το διάνυσμα που έχει 1 στην λ-στη θέση και 0 οπουδήποτε αλλού. Ισχύει ότι $\underline{e}_\lambda\underline{b}_i = b_{i\lambda}$ και $(\underline{e}_\lambda + \underline{e}_\mu)b_i = b_{i\lambda} + b_{i\mu}$ (mod 2). Για να είναι το διάνυσμα $\underline{e}_\lambda + \underline{e}_\mu$ κάποιο υποψήφιο x_i θα πρέπει $(\underline{e}_\lambda + \underline{e}_\mu)\underline{b}_v = b_{v\lambda} + b_{v\mu}$ (mod 2) $= \begin{cases} 1 & v = i \\ 0 & v \neq i \end{cases}$.

Επειδή 2 bits έχουν άθροισμα 1 αν και μόνο αν είναι διαφορετικά μεταξύ τους, έπεται ότι το παραπάνω θα συμβεί ακριβώς τότε όταν η λ-στη στήλη του R_m και η μ-στη στήλη διαφέρουν στην i γραμμή και συμπίπτουν σε όλες τις άλλες θέσεις.

Παράδειγμα 7.11 Ας θεωρήσουμε τον πίνακα $R_3 = \left[\begin{array}{cccc:cccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$.

Αν πάρουμε i = 1 και εξετάσουμε ποια ζευγάρια στηλών μας δίνουν το x_1 θα δούμε ότι είναι τα (Σ1, Σ5), (Σ2, Σ6), (Σ3, Σ7), (Σ4, Σ8).

Συνεπώς, για κάθε γραμμή i θέλουμε ένα ζευγάρι στηλών του R_m τα οποία ταυτίζονται σε όλες τις θέσει εκτός της i-στής γραμμής. Τέτοια ζευγάρια θα λέγονται **καλά ζευγάρια** για την i-στή γραμμή. Μπορούμε τώρα, σύμφωνα με τα παραπάνω, να διατυπώσουμε το ακόλουθο

Λήμμα 7.12 Αν (λ, μ) είναι η θέση δύο στηλών του R_m οι οποίες αποτελούν καλό ζευγάρι για την i-στή γραμμή του πίνακα R_m, τότε για κάθε κωδική λέξη $\underline{c} = a_1\underline{b}_1 + \ldots + a_m\,\underline{b}_m + a_{m+1}\,\underline{b}_{m+1}$ και για κάθε δείκτη i = 1, …, m έχουμε ότι $a_i = (\underline{e}_\lambda + \underline{e}_\mu)\underline{c}$.

Παρατήρηση 7.13 Επειδή η τελευταία γραμμή του πίνακα R_m έχει παντού μονάδες, οποιοδήποτε ζευγάρι στηλών του R_m έχει μονάδα στην (m +1)-στή θέση. Δηλαδή, η τελευταία γραμμή δεν έχει καλά ζευγάρια.

Με την τελευταία γραμμή θα ασχοληθούμε λίγο παρακάτω. Ούτως ή άλλως η τελευταία γραμμή δεν μας δημιουργεί κανένα πρόβλημα στην εύρεση καλών ζευγαριών για τις άλλες γραμμές και μπορούμε, συνεπώς, να την αγνοήσουμε. Πράγματι, έστω R'_m ο πίνακας που προκύπτει από τον R_m με την αφαίρεση της τελευταίας του γραμμής. Ένα καλό ζευγάρι για την i-στή γραμμή έχει τη μορφή

$$\begin{bmatrix} \beta_1 \\ \vdots \\ \beta_{i-1} \\ 0 \\ \beta_{i+1} \\ \vdots \\ \beta_n \end{bmatrix} \quad \text{και} \quad \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_{i-1} \\ 1 \\ \beta_{i+1} \\ \vdots \\ \beta_n \end{bmatrix}.$$

Ονομάζουμε αντίστοιχα τις στήλες το «**0-μισό**» του καλού ζευγαριού και το «**1-μισό**» του καλού ζευγαριού. Σύμφωνα με το προηγούμενο θεώρημα που διατυπώσαμε χωρίς απόδειξη οι στήλες του R'_m αποτελούνται από τις δυαδικές παραστάσεις των αριθμών 0, 1, 2, $2^m - 1$ με την κανονική σειρά.

Επομένως, για κάθε τιμή β_i υπάρχουν πάντοτε δύο στήλες της παραπάνω μορφής. Επιπλέον, επειδή η στήλη «1-μισό» του ζευγαριού παριστά μεγαλύτερο δυαδικό αριθμό από αυτόν που παριστά η «0-μισό» έπεται ότι η στήλη «1-μισό» βρίσκεται δεξιότερα της στήλης «0-μισό». Το ερώτημα είναι πόσο δεξιότερα. Ο αριθμός που παριστά η στήλη «1-μισό» είναι 2^{m-i} μεγαλύτερος από τον αριθμό που παριστά η στήλη «0-μισό». Άρα η απόσταση του «1-μισό» από το «0-μισό» ως προς την i-γραμμή είναι 2^{m-i}.

Συμπέρασμα Όλα τα καλά ζευγάρια για την i-στη γραμμή τα παίρνουμε ως εξής: Θεωρούμε όλες τις στήλες του R_m που έχουν 0 στην i-στη θέση. Αν «0-μισό» είναι η στήλη j τότε η αντίστοιχη «1-μισό» στήλη του καλού ζευγαριού για τη γραμμή i είναι η στήλη $(j + 2^{m-i})$.

Για παράδειγμα, στον R_3 για να βρούμε τα καλά ζευγάρια για την πρώτη γραμμή βρίσκουμε τις στήλες που έχουν 0, δηλαδή τις 1, 2, 3 και 4, και στη συνέχεια από τον τύπο $j + 2^{m-i}$ βρίσκουμε το αντίστοιχο «1-μισό». Επομένως, τα καλά ζευγάρια για την πρώτη γραμμή είναι τα (Σ1, Σ5), (Σ2, Σ6), (Σ3, Σ7), (Σ4, Σ8), για την δεύτερη γραμμή ισχύει j = 1, 2, 5, 6 άρα τα καλά ζευγάρια είναι τα (Σ1, Σ3), (Σ2, Σ4), (Σ5, Σ7), (Σ6, Σ8). Για την τρίτη γραμμή ισχύει j = 1, 3, 5, 7 άρα τα καλά ζευγάρια είναι τα (Σ1, Σ2), (Σ3, Σ4), (Σ5, Σ6), (Σ7, Σ8). Η τέταρτη, όπως προείπαμε, προς το παρόν δεν μας ενδιαφέρει. Επομένως, οι μισές ακριβώς από τις στήλες του R_m μας δίνουν τα «0-μισά» των καλών ζευγαριών για οποιαδήποτε γραμμή i και οι άλλες μισές τα αντίστοιχα «1-μισά».

Συμπέρασμα Για κάθε γραμμή i = 1, 2, …, m υπάρχουν 2^{m-1} καλά ζευγάρια.

Αλγόριθμος αποκωδικοποίησης Reed-Muller κωδίκων

Υποθέτουμε ότι στάλθηκε η κωδική λέξη $\underline{c} = a_1\underline{b}_1 + \ldots + a_m \underline{b}_m + a_{m+1} \underline{b}_{m+1}$. Αν χρησιμοποιήσουμε τα 2^{m-1} καλά ζευγάρια, για την i-στή γραμμή ($i \le m$) θα έχουμε 2^{m-1} εκφράσεις του συντελεστή a_i μέσω διαφορετικών μεταξύ τους ζευγαριών συντεταγμένων του $\underline{c}$. Για παράδειγμα, αν (Σλ, Σμ) καλό ζευγάρι για την i-στή γραμμή τότε $a_i = (\underline{e}_\lambda + \underline{e}_\mu)\ \underline{c} = c_\lambda + c_\mu$. Επομένως, αν δεν έχουμε περισσότερα από $2^{m-1} - 1$ λάθη τότε το πολύ $2^{m-2} - 1$ συνιστώσες του $\underline{x} = x_1x_2\ldots x_n$ που θα πάρουμε θα είναι λάθος. Συνεπώς, τουλάχιστον $2^{m-1} - (2^{m-2} - 1) = 2^{m-2} - 1$ εκφράσεις για το a_i, δηλαδή η πλειοψηφία, είναι σωστές. Οπότε, υπολογίζουμε τις 2^{m-1} εκφράσεις για το a_i και αποκωδικοποιούμε στην πλειοψηφούσα τιμή.

Τελικό βήμα Υπολογίζουμε τον συντελεστή a_{m+1}. Αν τα λάθη κατά την μεταφορά είναι $2^{m-1} - 1$ και υποθέσουμε ότι πήραμε το διάνυσμα $\underline{x}$ τότε το λάθος είναι το διάνυσμα $\underline{e} = \underline{x} - \underline{c}$ το οποίο έχει βάρος το πολύ $2^{m-1} - 1$. Αν θέσουμε $\underline{\delta} = a_1\underline{b}_1 + \ldots + a_m \underline{b}_m$ έχουμε $\underline{x} - \underline{\delta} = \underline{e} + \underline{c} - \underline{\delta} = \underline{e} + a_{m+1} \underline{b}_{m+1} = a_{m+1}\underline{1} + \underline{e}$, όπου $\underline{1} = 11\ldots1$. Υπάρχουν δύο δυνατότητες:

(i) Αν $a_{m+1} = 0$ τότε $\underline{e} = \underline{x} - \underline{\delta}$.

(ii) Αν $a_{m+1} = 1$ τότε $\underline{e} = (\underline{x} - \underline{\delta})^c$.

Συμπέρασμα
Αν $w(x - \delta) \leq 2^{m-2} - 1$ αποκωδικοποιούμε το a_{m+1} στο μηδέν.
Αν $w((x - \delta)^c) \leq 2^{m-2} - 1$ αποκωδικοποιούμε το a_{m+1} στο ένα.

Παρατήρηση 7.14 Αποδείξαμε ότι μπορούμε να διορθώσουμε το πολύ $2^{m-2} - 1$ λάθη. Άρα ο κώδικας έχει ελάχιστη απόσταση $d = 2^{m-1}$.

Παράδειγμα 7.15 Υποθέτουμε ότι η, άγνωστη σ' εμάς, κωδική λέξη c = 11 00 11 00 στάλθηκε μέσω ενός (8, 16, 4) Reed-Muller κώδικα R(3) αλλά εμείς πήραμε $x = x_1x_2\ldots x_8 = 11\ 01\ 11\ 00$. Επομένως, αν $\underline{c} = c_1c_2\ldots c_8 = a_1\underline{b}_1 + a_2\underline{b}_2 + a_3\underline{b}_3 + a_4\underline{b}_4$ όπου $\underline{b}_1, \underline{b}_2, \underline{b}_3, \underline{b}_4$ οι γραμμές του πίνακα R_3 τότε έχουμε ότι $a_1 = c_1 + c_5 = c_2 + c_6 = c_3 + c_7 = c_4 + c_8$.

Υπολογίζουμε το a_1:

$a_1 = x_1 + x_5 = 0$
$a_1 = x_2 + x_6 = 0$
$a_1 = x_3 + x_7 = 0$
$a_1 = x_4 + x_8 = 1$

Συνεπώς, αποκωδικοποιούμε στο $a_1 = 0$. Ομοίως για το a_2:

$a_2 = x_1 + x_3 = 1$
$a_2 = x_2 + x_4 = 0$
$a_2 = x_5 + x_7 = 1$
$a_2 = x_6 + x_8 = 1$

Συνεπώς, αποκωδικοποιούμε στο $a_2 = 1$. Ομοίως για το a_3:

$a_3 = x_1 + x_2 = 0$
$a_3 = x_3 + x_4 = 1$
$a_3 = x_5 + x_6 = 0$
$a_3 = x_7 + x_8 = 0$

Συνεπώς, αποκωδικοποιούμε στο $a_3 = 0$.

Στη συνέχεια, υπολογίζουμε το $\underline{x} - \underline{\delta} = \underline{x} - a_1\underline{b}_1 - a_2\underline{b}_2 - a_3\underline{b}_3 = 11011100 - 00110011 = 11\ 10\ 11\ 11$. Άρα, $w(\underline{x} - \underline{\delta}) = 7 > 1 = 2^{3-2} - 1$, ενώ $(\underline{x} - \underline{\delta})^c = 00\ 01\ 00\ 00$ και $w((\underline{x} - \underline{\delta})^c) = 1 \leq 1$. Συνεπώς, αποκωδικοποιούμε $a_4 = 1$. Τελικά, $\underline{c} = \underline{b}_2 + \underline{1} = 00\ 11\ 00\ 11 + 11\ 11\ 11\ 11 = 11\ 00\ 11\ 00$.

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.

9. MDS κώδικες

Έστω C ένας γραμμικός (n, k, d)-κώδικας. Υπενθυμίζουμε το φράγμα του Singleton: $k \leq n - d + 1$. Επίσης, είχαμε ορίσει ως MDS-κώδικα έναν γραμμικό κώδικα για τον οποίο ισχύει η ισότητα στο φράγμα του Singleton. Δηλαδή, $k = n - d + 1$ ή αλλιώς $d = m + 1$ όπου $m = n - k$.

Συμβολισμός 9.1 $V(m, q) = (\mathbf{F}_q)^n$

Ορισμός 9.2 Ένα (n, s)-σύνολο του V(m, q) είναι ένα σύνολο από n διανύσματα του V(m, q) τέτοιο ώστε s οποιαδήποτε από αυτά να είναι γραμμικά ανεξάρτητα.

Έχουμε ήδη αναφέρει την

Πρόταση 9.3 Υπάρχει κώδικας C τύπου (n, n – m, d) στο $\mathbf{F}_q$ ακριβώς τότε όταν υπάρχει ένα (n, d – 1) σύνολο του V(m, q).

Συμβολισμός 9.4 Το $\max_s(m, q)$ θα συμβολίζει τη μέγιστη τιμή του n για την οποία υπάρχει ένα (n, s)-σύνολο του V(m, q). Ένα τέτοιο n θα λέγεται βέλτιστο.

Άμεση συνέπεια της πρότασης 9.3 είναι το

Πόρισμα 9.5 Αν μας δοθούν τα q, d και m τότε η μεγαλύτερη τιμή για το n έτσι ώστε να υπάρχει ένας (n, n – m, d) κώδικας στο $\mathbf{F}_q$ είναι $\max_{d-1}(m, q)$.

Αν έχουμε τώρα έναν MDS-κώδικα (n, n – m, d) στο $\mathbf{F}_q$ τότε το μέγιστο μήκος n του κώδικα σύμφωνα με το πόρισμα 9.5 είναι $\max_m(m, q)$. Δηλαδή, το μέγιστο μήκος ενός (n, m)-συνόλου στο V(m, q).

Γνωστά αποτελέσματα υποβάλλουν την ανάγκη διατύπωσης της ακόλουθης εικασίας.

Εικασία 9.6 Έστω m με $2 \leq m \leq q$, $m \neq 3$. Ισχύει: $\max_m(m, q) = q + 1$.

Για m = 3 έχει αποδειχθεί ότι ισχύει $\max_3(3, q) = q + 2$.

Θα αποδείξουμε την εικασία κατ' αρχήν για m = 2. Θα αποδείξουμε δηλαδή ότι ισχύει:

$$\max_2(2, q) = q + 1. \quad (1)$$

Γενικότερα ισχύει η

Πρόταση 9.10 Δίδεται το m. Το μέγιστο μήκος n τέτοιο ώστε να υπάρχει (n, n – m, 3)-κώδικας ως προς το σώμα $\mathbf{F}_q$ είναι $n = \frac{q^m - 1}{q - 1}$.

Σημείωση 9.11 Αυτό σημαίνει ότι $\max_2(m, q) = \frac{q^m - 1}{q - 1}$.

Ειδικά για m = 2 έχουμε $\max_2(2, q) = \frac{q^2 - 1}{q - 1} = q + 1$ δηλαδή την (1).

Απόδειξη Σύμφωνα με το πόρισμα 9.5, αρκεί να αποδείξουμε ότι το n είναι η μεγαλύτερη τιμή ύπαρξης ενός (n, 2) – συνόλου στο V(m, g).

Ένα σύνολο S διανυσμάτων του V(m, g) είναι ένα (n, 2) – σύνολο τότε και μόνο τότε όταν δεν υπάρχει διάνυσμα στο S το οποίο να είναι scalar πολλαπλάσιο οποιουδήποτε άλλου διανύσματος του S. Τώρα θυμόμαστε, όταν γράφουμε τον τύπο … κωδίκων Hamming ότι εκεί τα $(q^m - 1)$ – μη μηδενικά διανύσματα του V(m, q) διαμερίζονται σε $\frac{q^m - 1}{q - 1}$ - κλάσεις, όπου κάθε κλάση περιέχει (q – 1) – διανύσματα τα οποία είναι scalar πολλαπλάσια το ένα του άλλου. Επομένως ένα (n, 2) – σύνολο μέγιστου μήκους – είναι ένα σύνολο $\frac{q^m - 1}{q - 1}$ διανυσμάτων. Παίρνουμε ένα από κάθε κλάση.

Ερώτημα Γιατί ξεκινάμε από m = 2;

Για m = 0 το V(n, q) είναι ένας (n, n – 1)-κώδικας για οποιοδήποτε n.

Για m = 1 ο πίνακας $\left[\begin{array}{c|c} I_{n-1} & \begin{matrix}1\\1\\\vdots\\1\end{matrix} \end{array}\right]$ είναι γεννήτορας ενός (n, n – 1, 2)-κώδικα για οποιοδήποτε n.

Εντελώς φυσικά προκύπτει και το επόμενο

Ερώτημα Τι γίνεται όταν m > q;

Απάντηση σ’ αυτό το ερώτημα δίνει η ακόλουθη

Πρόταση 9.12 Αν $m \geq q$ τότε $\max_m(m, q) = m + 1$ και κάθε MDS-κώδικας με $m \geq q$ είναι ισοδύναμος με κάποιον κώδικα επανάληψης μήκους m + 1.

Απόδειξη Ο κώδικας επανάληψης μήκους (m + 1) είναι του τύπου (m + 1, 1, m + 1) και έχει πίνακα γεννήτορα τον [11…1]. Επομένως, $\max_m(m, q) \geq m + 1$. Επίσης είναι σαφές ότι κάθε (m + 1, 1, m + 1) – κώδικας είναι ισοδύναμος με κάποιο κώδικα επανάληψης. Υποθέτουμε ότι $m \geq q$ και ότι $\max_m(m, q) \geq m + 2$. Τότε, σύμφωνα με τα προηγούμενα υπάρχει ένας (m + 2, 2, m + 1) – κώδικας C ως προς το σώμα $\mathbf{F}_q$. Ο κώδικας αυτός θα πρέπει να είναι ισοδύναμος με έναν κώδικα με γεννήτορα πίνακα της μορφής

$$G = \left[\begin{array}{cc|cccc} 1 & 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & a_1 & a_2 & \dots & a_m \end{array}\right]$$

Για να έχει κάθε γραμμικός συνδυασμός των γραμμών του πίνακα G βάρος τουλάχιστον (m + 1) θα πρέπει τα a_i να είναι διαφορετικά του μηδενός και διαφορετικά μεταξύ τους ανά δύο, στοιχεία του $\mathbf{F}_q$ από όπου έπεται ότι $m \leq q - 1$, άτοπο.

Άμεση συνέπεια της πρότασης 9.12 αλλά και άλλων στοιχείων στα οποία εμείς δεν αναφερθήκαμε είναι η ακόλουθη ταξινόμηση:

Οι μοναδικοί δυαδικοί MDS-κώδικες είναι:

- Ο $V(n, 2) = (\mathbf{F}_2)^n$, δηλαδή όλος ο χώρος.
- Ο κώδικας όλων των διανυσμάτων άρτιου βάρους του V(n, 2)
- Οι κώδικες επανάληψης

Χωρίς απόδειξη αναφέρουμε την

Πρόταση 9.13 Έστω m με $2 \leq m \leq q$ και $\mathbf{F}_q^* = \{\alpha_1, \alpha_2, \ldots, \alpha_{q-1}\}$. Ο πίνακας

$$H = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{q-1} & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{m-1} & \alpha_2^{m-1} & \ldots & \alpha_{q-1}^{m-1} & 0 & 1 \end{bmatrix}$$

είναι πίνακας ελέγχου ισοτιμίας ενός MDS-κώδικα τύπου (q +1, q – 1 – m, m + 1)

Πόρισμα 9.14 Για m με $2 \leq m \leq q$ ισχύει $\max_m(m, q) \leq q + 1$.
Τέλος ισχύουν,

1. Ο δυικός MDS-κώδικα είναι επίσης MDS.
2. Υπάρχει MDS κώδικας τύπου (n, n – m) ως προς το σώμα $\mathbf{F}_q$ ακριβώς τότε όταν υπάρχει MDS κώδικας τύπου (n, m).
3. Αν $q = 2^t$, $t > 1$ τότε υπάρχει (q + 2, 3, q)-κώδικας ως προς το σώμα $\mathbf{F}_q$.

10. Τροποποίηση κωδίκων

Όταν έχουμε έναν καλό κώδικα, ως προς κάποια συμπεριφορά, επιθυμούμε και ελπίζουμε να παράγουμε άλλο κώδικα επίσης αρκετά καλό με τροποποίηση του αρχικού.

Κάθε κώδικας έχει τρεις θεμελιώδης παραμέτρους

- το μήκος n
- τη διάσταση k
- το m = n – k

Θα αναφερθούμε σε 6 + 1 τεχνικές τροποποίησης κωδίκων. Πάντοτε μια παράμετρος παραμένει σταθερή και αυξομειώνονται οι άλλες δύο.

Όνομα	Σταθερό	Αυξάνεται	Μειώνεται
augmenting	n	k	m
expurgating	n	m	k
extending	k	n, m	-
puncturing	k	-	n, m
lengthening	m	n, k	-
shortening	m	-	n, k

Augmenting θα πει ότι προσθέτουμε κωδικές λέξεις στον C. Αυτό μπορεί να προκαλέσει μείωση της ελάχιστης απόστασης.
Expurgating θα πει ότι αφαιρούμε κωδικές λέξεις από τον C. Αυτό μπορεί να προκαλέσει αύξηση της ελάχιστης απόστασης.

Σε γραμμικό κώδικα επιτυγχάνουμε το augmenting προσθέτοντας γραμμές στον γεννήτορα πίνακα. Συνήθως, προσθέτουμε μια γραμμή, την $\underline{1} = (1\ 1\ \ldots\ 1)$ όταν αυτή δεν υπάρχει. Το expurgating το επιτυγχάνουμε σβήνοντας γραμμές από τον γεννήτορα πίνακα.

Extending επιτυγχάνουμε προσθέτοντας σύμβολα ελέγχου. Αν ο κώδικας είναι γραμμικός προσθέτουμε στήλες στον γεννήτορα πίνακα.

Puncturing επιτυγχάνουμε αφαιρώντας σύμβολα ελέγχου. Αν ο κώδικας είναι γραμμικός αφαιρούμε στήλες από τον γεννήτορα πίνακα.

Lengthening επιτυγχάνουμε αυξάνοντας το μήκος και προσθέτοντας και άλλες κωδικές λέξεις. Αν ο κώδικας είναι γραμμικός προσθέτουμε κάποιον αριθμό νέων γραμμών στον γεννήτορα πίνακα και τον ίδιο αριθμό στηλών.

Shortening επιτυγχάνουμε διαγράφοντας συντεταγμένες και κωδικές λέξεις.

Concatenation (περιπλοκή κωδίκων)

Πρόκειται για κατασκευή πολύ συνηθισμένη στην πράξη. Π.χ. η NASA συχνά χρησιμοποιεί έναν κώδικα ο οποίος αποτελεί περιπλοκή ενός Reed – Solomon και ενός convolutional (non – block) κώδικα. Θεωρούμε μια k_1k_2 – άδα από το σώμα $\mathbf{F}_2$

την οποία συμβολίζουμε με α. Ομαδοποιούμε το α σε k_1 – το πλήθος k_2 – άδες α_i όπου i = 0, 1, …, $k_1 - 1$. Δηλαδή, έχουμε ότι $\alpha = \alpha_0 \alpha_1 \dots \alpha_{k_1-1}$ όπου φανταζόμαστε κάθε k_2 – άδα σαν ένα στοιχείο του σώματος $\mathbf{F}_{2^{k_2}}$. Στη συνέχεια υποθέτουμε ότι έχουμε έναν (n_1, k_1, d_1) – κώδικα c_1 ως προς το σώμα $\mathbf{F}_{2^{k_2}}$. Θα τον ονομάζουμε **εσωτερικό κώδικα**. Το α κωδικοποιείται μέσω του c_1 στο $c = c_0c_1\dots c_{n_1-1}$ ως προς το σώμα $\mathbf{F}_{2^{k_2}}$.

Στη συνέχεια σε κάθε μια από τις n_1 στο πλήθος «συλλαβές» του $\mathbf{F}_{2^{k_2}}$ κωδικοποιείται, χρησιμοποιώντας έναν (n_2, k_2, d_2) – κώδικα c_2, ο οποίος λέγεται **εξωτερικός κώδικας**.

Η λέξη d που προέκυψε έχει μήκος n_1n_2. Η διαδικασία κωδικοποίησης των δύο βημάτων λέγεται και <u>υπερκωδικοποίηση.</u>

Ξεκινάμε με μια k_1k_2 – άδα και καταλήγουμε σε μια n_1n_2 – άδα. Ο καινούριος κώδικας έχει τύπο (n, k, d_{min}) όπου $n = n_1n_2$, $k = k_1k_2$ και $d = d_{min}(C) \geq d_1d_2$ (άσκηση)