Πανεπιστήμιο Κρήτης
Σχολή Θετικών Επιστημών και Τεχνολογίας
Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

Σχεδόν Πλήρως Μη Γραμμικές Συναρτήσεις (Almost Perfect Nonlinear Functions)

Μεταπτυχιακή Εργασία

Αναστασία Πανουή

Επιβλέπων καθηγητής: Θ. Γαρεφαλάκης

Ευχαριστίες

Ξεκινώντας, θα ήθελα να ευχαριστήσω τους ανθρώπους εκείνους, που με μοναδικό τρόπο ο καθένας, βοήθησαν στην πραγματοποίηση της παρούσας εργασίας.

Ευχαριστώ θερμά τους καθηγητές Ν.Τζανάκη και Ι.Αντωνιάδη για τα σημαντικά σχόλια, τις προτάσεις αλλά και συμβουλές τους για την επίτευξη του καλύτερου δυνατού αποτελέσματος. Τις ευχαριστίες μου εκφράζω στον καθηγητή J.F.Dillon για την ευγενική παραχώρηση μαθηματικού υλικού αλλά και για την προσφορά οποιασδήποτε βοήθειας στη μαθηματική μου έρευνα. Ιδιαίτερα, θα ήθελα να ευχαριστήσω τον δάσκαλό μου Επίκουρο καθηγητή Θ.Γαρεφαλάκη. Η καθοδήγηση, τα σχόλια και οι παρατηρήσεις του, η υπομονή και εμπιστοσύνη που μου έδειξε, με οδήγησαν να κατανοήσω τί σημαίνει μαθηματική έρευνα και με προετοίμασαν για αυτό το συναρπαστικό ταξίδι. Τέλος, ευχαριστώ από καρδιάς την οικογένειά μου και τους φίλους μου, ιδιαιτέρως τον Β.Καπετανάκη, για τη διαρκή υποστήριξη και αγάπη τους.

Κεφάλαιο 1

Εισαγωγή

Το σύστημα κτυπτογράφησης DES (Data Encryption Standard), εμφανίστηκε τη δεκαετία 1970 και πολύ σύντομα έγινε το πρότυπο σύστημα για τις ποικίλες διατραπεζικές συναλλαγές. Για τα επόμενα 20 περίπου χρόνια το DES συνέχιζε να προσφέρει ασφαλείς συναλλαγές, ώσπου το 1990 η διαρκώς εξελισσόμενη τεχνολογία οδήγησε στην αντικατάστασή του από το AES (Advanced Encryption Standard).

Η αποτελεσματικότητα του DES οφείλεται στη χρήση συναρτήσεων επανάληψης (round functions) και παράλληλων μετασχηματισμών αντικατάστασης (Substitution boxes). Η αύξηση του αριθμού των επαναλήψεων και του μεγέθους των S-boxes, προσφέρει μεγάλη ασφάλεια σε διαφορικές επιθέσεις (differential attacks). Στις επιθέσεις αυτού του τύπου, ελέγχονται ζευγάρια κρυπτογραφημένου κειμένου σε εκείνα τα σημεία, όπου στο κανονικό κείμενο παρατηρούνται διαφορές. Αν κάποιες διαφορές στο αρχικό κείμενο έχουν μεταφερθεί στο κρυπτογραφημένο, τότε με την παραπάνω επίθεση είναι δυνατόν να αποκαλυφθεί η δομή του κρυφού κλειδιού. Η μεταφορά ή όχι των διαφορών του αρχικού κειμένου στο τελικό, εξαρτάται από τις συναρτήσεις επανάληψης και τα S-boxes. Απαραίτητη προϋπόθεση για την αποτελεσματικότητα αυτών των δύο βασικών στοιχείων του DES, είναι η μη γραμμικότητα, δηλαδή η ύπαρξη όσο το δυνατόν μεγαλύτερης απόστασης από το σύνολο των αφινικών συναρτήσεων.

Το 1994, η Kaisa Nyberg [10] εισήγαγε τον όρο **σχεδόν πλήρως μη γραμμικές συναρτήσεις (Alomost Perfect Nonlinear functions)**. Στη συνέχεια, οι Claude Carlet, Pascale Charpin και Victor Zinoviev παρουσίασαν μια σχέση ισοδυναμίας (CCZ equivalence), η οποία οδήγησε στην ταξινόμηση των συναρτήσεων APN. Το 1998 η ίδια ερευνητική ομάδα, μετέφρασε τις συναρτήσεις APN στη γλώσσα της κωδικοποίησης και τις αντιστοίχισε με γραμμικούς κώδικες [5]. Έτσι, η ταξινόμηση των APN μπορεί να πραγματοποιηθεί με χρήση γραμμικών κωδίκων. Το γεγονός ότι οι νέες συναρτήσεις APN που ανακαλύπτονται είναι ισοδύναμες με μονώνυμα, δημιούργησε την εικασία ότι ίσως όλες οι APN είναι ισοδύναμες με μονώνυμα. Όμως, η έρευνα των Yves Edel, Gohar Kyureghyan και Alexander Pott σε συνδυασμό με την χρήση ηλεκτρονικού υπολογιστή, οδήγησε στην ανακάλυψη μιας νέας συνάρτησης APN πάνω από το

$\mathbb{F}_{2^{10}}$, η οποία δεν είναι μονώνυμο και δεν είναι ισοδύναμη με καμία απο τις ήδη γνωστές APN [6]. Το 2006, η ερευνητική ομάδα του J.F. Dillon, χρησιμοποιώντας τους γραμμικούς κώδικες καθώς και άλλες αναλλοίωτες, όπως το φάσμα Fourier, παρουσίασε καινούρια πολυώνυμα APN σε πεπερασμένα σώματα μικρής διάστασης, τα οποία είναι ισοδύναμα με μονώνυμα, αυξάνοντας έτσι τον αριθμό των στοιχείων που ανήκουν σε κάθε κλάση [2].

Η παρούσα εργασία μελετά τη σχέση των συναρτήσεων APN με τους γραμμικούς κώδικες. Αρχικά, δίνονται οι απαραίτητοι ορισμοί και οι ιδιότητες των APN, ενώ στη συνέχεια παρουσιάζονται κάποια βασικά χαρακτηριστικά των γραμμικών κωδίκων. Τέλος, αναφέρεται και αποδεικνύεται το θεώρημα που συνδέει τις APN με τους γραμμικούς κώδικες, καθώς και κάποια παραδείγματα-εφαρμογές του θεωρηματος.

Περιεχόμενα

Κεφάλαιο 2

Ορισμοί

2.1 APN συναρτήσεις πάνω από το F_q

Έστω $f : \mathbb{F}_q \to \mathbb{F}_q$, όπου q είναι δύναμη πρώτου. Τότε ορίζουμε για $a, b \in \mathbb{F}_q$, με $a \neq 0$

$$N_f(a,b) = |\{x \in \mathbb{F}_q \,/\, f(x+a) - f(x) = b\}|$$

δηλαδή το πλήθος των λύσεων της εξίσωσης

$$f(x+a) - f(x) = b$$

Επίσης ορίζουμε Δ_f να είναι η μέγιστη τιμή του $N_f(a,b)$:

$$\Delta_f = \max\{\, N_f(a,b) \,/\, a, b \in \mathbb{F}_q, a \neq 0\}$$

Αν η συνάρτηση f είναι γραμμική, δηλαδή $f(x+y) = f(x) + f(y)$ τότε

$$\begin{aligned} f(x+a) - f(x) &= b \Leftrightarrow \\ \Leftrightarrow\ f(x) + f(a) - f(x) &= b \Leftrightarrow \\ \Leftrightarrow\ f(a) &= b \end{aligned}$$

Δηλαδή $\Delta_f = N_f(a, f(a)) = q$. Άρα η παράμετρος Δ_f είναι ένα μέτρο του κατά πόσο η συνάρτηση f απέχει από το να είναι γραμμική.

Ορισμός 2.1.1 *Αν $\Delta_f = 1$ τότε η f λέγεται πλήρως μη γραμμική (Perfect Nonlinear), ενώ αν $\Delta_f = 2$ σχεδόν πλήρως μη γραμμική, (Almost Perfect Nonlinear).*

Στο παρακάτω Θεώρημα αναφέρονται κάποιες περιπτώσεις, όπου ανάλογα σε ποιο σώμα βρισκόμαστε, η συνάρτηση $f(x) - x^d$ έχει διαφορετικό Δ_f. Η απόδειξη βρίσκεται στο [7].

Θεώρημα 2.1.1 *Έστω $d = p^n - 3$ και $f(x) - x^d$ απεικόνιση από το $\mathbb{F}_{p^n}$ στον εαυτό της.*

1. *Αν $p = 2$, τότε $\Delta_f = 2$ για n περιττό και $\Delta_f = 4$ για n άρτιο.*
2. *Αν p είναι περιττός πρώτος, τότε $1 \leq \Delta \leq 5$.*
3. *Αν $n > 1$ περιττός και $p = 3$, τότε $\Delta_f = 2$*

2.2 Η περίπτωση $q = 2^n$

Σε σώμα χαρακτηριστικής 2, η εξίσωση $f(x+a) - f(x) = b$ μετατρέπεται στην

$$f(x+a) + f(x) = b \tag{2.1}$$

Έστω $x \in \mathbb{F}_{2^n}$ μια λύση της εξίσωσης (2.1), τότε και η $x + a \in \mathbb{F}_{2^n}$ είναι επίσης λύση:

$$f(x+a+a) + f(x+a) = f(x) + f(x+a) = b$$

Επίσης παρατηρούμε ότι θα υπάρχουν πάντα $a, b \in \mathbb{F}_{2^m}$ για τα οποία η εξίσωση (2.1) έχει λύση. Για παράδειγμα, αν επιλέξουμε τη συνάρτηση $f(x) = x^3$ πάνω από το $\mathbb{F}_{2^3}$, τότε για $a = 1$ και $x = 1$ έχουμε

$$f(1+1) + f(1) = f(0) + f(1) = 0 + 1 = 1$$

Δηλαδή για $b = 1$, η εξίσωση

$$f(x+1) + f(x) = 1$$

έχει λύσεις τις $x = 1, x + 1 = 0$.

Είδαμε ότι οι λύσεις της (2.1) είναι ζευγάρια. Επομένως, όταν βρισκόμαστε σε σώμα χαρακτηριστικής 2, η μικρότερη τιμή που μπορεί να πάρει το Δ_f είναι 2.

Πρόταση 2.2.1 *Έστω $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Τα εξής είναι ισοδύναμα:*

(i) $\Delta_f = 2$

(ii) $|H_a| = \frac{1}{2}|\mathbb{F}_{2^n}| = 2^{n-1}, \quad \forall a \in \mathbb{F}_{2^n}^*$, *όπου* $H_a = \{\, f(x+a) + f(x) \,/\, x \in \mathbb{F}_{2^n} \}$

(iii) το σύστημα

$$\begin{cases} x + y = a \\ f(x) + f(y) = b \end{cases} \tag{2.2}$$

έχει 0 ή 2 λύσεις

Απόδειξη

$(i) \Rightarrow (ii)$ $\Delta_f = 2 \Leftrightarrow |H_a| = 2^{n-1}$

Θεωρούμε την απεικόνιση

$$\begin{array}{rcl} \theta : \mathbb{F}_{2^n} & \longrightarrow & H_a \\ x & \longmapsto & f(x+a)+f(x) \end{array}$$

τότε

$$|\mathbb{F}_{2^n}| = 2^n = \sum_{b \in H_a} 1 \sum_{\theta(x)=b} 1$$

$(\Rightarrow)$ Υποθέτουμε ότι $\Delta_f = 2$. Τότε για κάθε $b \in H_a$ υπάρχουν ακριβώς δύο $x \in \mathbb{F}_{2^n}$ που ικανοποιούν την (2.1):

$$\left\{ \begin{array}{l} f(x_1+a)+f(x_1) = b, \quad x_1 \in \mathbb{F}_{2^n} \\ f(x_2+a)+f(x_2) = b, \quad x_2 \in \mathbb{F}_{2^n} \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \theta(x_1) = b \\ \theta(x_2) = b \end{array} \right.$$

άρα

$$2^n = 2 \sum_{b \in H_a} 1 \quad \Rightarrow \quad 2^n = 2\,|H_a| \quad \Rightarrow \quad |H_a| = 2^{n-1}$$

$(\Leftarrow)$ Αν $|H_a| = 2^{n-1}$ τότε για κάθε $b \in H_a$,

$$2^n = 2^{n-1} \sum_{\theta(x)=b} 1 \;\Rightarrow\; \sum_{\theta(x)=b} 1 = 2 \;\Rightarrow\; N_f(a,b) = 2 \;\Rightarrow\; \Delta_f = 2$$

$(i) \Rightarrow (iii)$ $\Delta_f = 2 \Leftrightarrow$ " το σύστημα (2.2) έχει 0 ή 2 λύσεις"

$(\Rightarrow)$ Υποθέτουμε ότι $\Delta_f = 2$, δηλαδή

$$\begin{array}{rcl} \max\{N_f(a,b) \,/\, a,b \in \mathbb{F}_{2^n}, a \neq 0\} & = & 2 \quad \Rightarrow \\ \Rightarrow \quad N_f(a,b) = |\{x \in \mathbb{F}_{2^n} \,/\, f(x+a)+f(x) = b\}| & = & 0 \quad \acute{\eta} \quad 2 \end{array}$$

Αν $N_f(a,b) = 0$ τότε $\nexists\, x \in \mathbb{F}_{2^n}$ τέτοιο ώστε $f(x+a)+f(x) = b$, δηλαδή το σύστημα

$$\left\{ \begin{array}{l} y = x + a \\ f(y)+f(x) = b \end{array} \right.$$

δεν έχει λύση.

Αν $N_f(a,b) = 2$ τότε $\exists\, x, y \in \mathbb{F}_{2^n}$, με $y = x + a$ τέτοια ώστε το (2.2) να έχει 2 λύσεις, τις $(x, x+a)$, $(y, y+a)$.

($\Rightarrow$) Υποθέτουμε ότι το (2.2) έχει 2 λύσεις (x_1, x_2), (y_1, y_2), $x_1, x_2, y_1, y_2 \in \mathbb{F}_{2^n}$, δηλαδή για $x_2 = x_1 + a$ και $y_2 = y_1 + a$ έχουμε

$$\begin{cases} f(x_1 + a) + f(x_1) = b \\ \qquad \kappa\alpha\iota \\ f(y_1 + a) + f(y_1) = b \end{cases}$$

άρα $N_f(a,b) = 2$ και συνεπώς $\Delta_f = 2$

Παρατηρούμε ότι αν x_0 είναι λύση της εξίσωσης

$$f(x + a) + f(x) = b, \quad a, b \in \mathbb{F}_{2^n}, a \neq 0$$

τότε το x_0 είναι επίσης λύση του συστήματος (2.2). Αντίστροφα, αν $(x_0, x_0 + a)$ είναι λύση του (2.2), τότε το x_0 είναι λύση της παραπάνω εξίσωσης. Δηλαδή υπάρχει μια "$1-1$" αντιστοιχία μεταξύ των λύσεων του συστήματος (2.2), με τις λύσεις της εξίσωσης. Άρα, αν το σύστημα δεν έχει λύση αυτό σημαίνει ότι η εξίσωση δεν έχει λύση. Όμως κάτι τέτοιο δεν μπορεί να συμβαίνει για όλα τα $a, b \in \mathbb{F}_{2^m}$, ακριβώς διότι $|H_a| = 2^{n-1}$. Άρα, σύμφωνα με την πρώτη ισοδυναμία, $\Delta_f = 2$.

Ορισμός 2.2.1 *Αν ισχύει ένα από τα $(i), (ii), (iii)$ της παραπάνω πρότασης, τότε η f λέγεται APN.*

Σύμφωνα λοιπόν με τους παραπάνω ορισμούς, η συνάρτηση f είναι APN αν για $a, b \in \mathbb{F}_{2^m}$ με $a \neq 0$, οι λύσεις της $f(x+a) + f(x) = b$ είναι ζευγάρια της μορφής $\{x, x+a\}$. Συνεπώς, η f δεν είναι APN αν και μόνο αν για κάποια $a, b \in \mathbb{F}_{2^m}$ με $a \neq 0$, υπάρχουν διαφορετικά μεταξύ τους $x, y, x', y' \in \mathbb{F}_{2^m}$, τέτοια ώστε

$$x + y = a = x' + y'$$

$$f(x) + f(y) = b = f(x') + f(y')$$

Η άρνηση της παραπάνω πρότασης δίνει ακόμη έναν τρόπο ορισμού των συναρτήσεων APN.

Πρόταση 2.2.2 *Μία συνάρτηση f είναι APN αν και μόνο αν για κάθε $x, y, x', y' \in \mathbb{F}_{2^m}$, διαφορετικά μεταξύ τους, ισχύει:*

$$x + y + x' + y' = 0 \quad \Rightarrow \quad f(x) + f(y) + f(x') + f(y') \neq 0$$

2.3 Σχέσεις ισοδυναμίας - Ισοδύναμες Συναρτήσεις

Έστω $f(x) \in \mathbb{F}_2[x]$ ανάγωγο πολυώνυμο βαθμού ν και $\alpha \in \mathbb{F}_{2^n}$ μια ρίζα του f. Τότε το σύνολο $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ αποτελεί βάση του $\mathbb{F}_{2^n}$ πάνω από το $\mathbb{F}_2$. Αν θεωρήσουμε τον ισομορφισμό

$$\begin{array}{rcl} \phi : \mathbb{F}_{2^n} & \longrightarrow & \mathbb{F}_2^n \\ c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + \ldots + c_1\alpha + c_0 & \longmapsto & (c_{n-1}, c_{n-2}, \ldots, c_1, c_0) \end{array}$$

τότε οι χώροι $\mathbb{F}_{2^n}$ και $\mathbb{F}_2^n$ είναι ισόμορφοι μέσω του παραπάνω ισομορφισμού ϕ. Συνεπώς οι ορισμοί των APN συναρτήσεων πάνω από το $\mathbb{F}_{2^n}$ μπορούν να μεταφερθούν στο διανυσματικό χώρο $\mathbb{F}_2^n$. Στο εξής, συχνά θα γίνεται ταύτιση των $\mathbb{F}_{2^n}$ και $\mathbb{F}_2^n$.

Ορισμός 2.3.1 *Δύο συναρτήσεις $f, f' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ λέγονται αφινικά ισοδύναμες (affine equivalent - AE) αν υπάρχουν $L_1, L_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ αντιστρέψιμες αφινικές απεικονίσεις τέτοιες ώστε*

$$f'(x) = L_1(f(L_2(x)))$$

Αν επιπλέον υπάρχει αφινική απεικόνιση $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ ώστε

$$f'(x) = L_1(f(L_2(x))) + L(x)$$

τότε οι f, f' είναι extended - affine ισοδύναμες (extended affine equivalent - EA)

Η σχέση Affine Equivalence προκύπτει από την Extended Affine Equivalence για $L(x) = 0$.

Πρόταση 2.3.1 *Η σχέση Extended Affine Equivalence (EA) είναι σχέση ισοδυναμίας.*

Απόδειξη

ανακλαστική $\mathbf{f \sim f}$

$$f(x) = L_1(f(L_2(x))) + L(x)$$

όπου
$L_1(x) = L_2(x) = x$, η ταυτοτική απεικόνιση
$L(x) = 0$

συμμετρική $\mathbf{f \sim g \Leftrightarrow g \sim f}$

$$\begin{array}{rcl} f \sim g & \Rightarrow & g(x) = L_1(f(L_2(x))) + L(x) \quad \Rightarrow \\ & \Rightarrow & L_1(f(L_2(x))) = g(x) - L(x) \end{array}$$

Η συνάρτηση L_1 είναι αφινική, άρα και η αντίστροφή της θα είναι αφινική. Έστω $L_1^{-1}(x) = N(x) + c$, με $N(x)$ γραμμική και c μια σταθερά. Τότε

$$\begin{aligned}
& f(L_2(x)) = L_1^{-1}(g(x) - L(x)) \quad \Rightarrow \\
\Rightarrow \quad & f(L_2(x)) = N(g(x) - L(x)) + c \quad \Rightarrow \\
\Rightarrow \quad & f(L_2(x)) = N(g(x) - N(L(x)) + c \quad \Rightarrow \\
\Rightarrow \quad & f(y) = N(g(L_2^{-1}(y))) - N(L(L_2^{-1}(y))) + c \quad \Rightarrow \\
\Rightarrow \quad & f(y) = L_1^{-1}(g(L_2^{-1}(y))) - N(L(L_2^{-1}(y))) \quad \Rightarrow \\
\Rightarrow \quad & f(x) = M_1(g(M_2(x))) + M(x) \quad \Rightarrow \\
\Rightarrow \quad & g \sim f
\end{aligned}$$

όπου
$M_1(x) = L_1^{-1}(x)$ (αντιστρέψιμη αφινική απεικόνιση)
$M_2(x) = L_2^{-1}(x)$ (αντιστρέψιμη αφινική απεικόνιση)
$M(x) = -N(L(L_2^{-1}(x)))$ (αφινική απεικόνιση)

μεταβατική $\left.\begin{array}{l} \mathbf{f} \sim \mathbf{g} \\ \mathbf{g} \sim \mathbf{h} \end{array}\right\} \Rightarrow \mathbf{f} \sim \mathbf{h}$

$$\mathbf{f} \sim \mathbf{g} \quad \Rightarrow \quad g(x) = L_1(f(L_2(x))) + L(x) \tag{2.3}$$
$$\mathbf{g} \sim \mathbf{h} \quad \Rightarrow \quad h(x) = M_1(g(M_2(x))) + M(x) \tag{2.4}$$

άρα, αν $M_1(x) = N_1(x) + c$, με $N_1(x)$ γραμμική και c μια σταθερά, τότε

$$\begin{aligned}
h(x) &= M_1(g(M_2(x))) + M(x) = \\
&\overset{(2.3)}{=} M_1(L_1(f(L_2(M_2(x)))) + L(M_2(x))) + M(x) = \\
&= N_1(L_1(f(L_2(M_2(x))))) + N_1(L(M_2(x))) + c + M(x) = \\
&= M_1(L_1(f(L_2(M_2(x))))) + N_1(L(M_2(x))) + M(x) = \\
&= K_1(f(K_2(x))) + K(x)
\end{aligned}$$

όπου
$K_1(x) = M_1(L_1(x))$ (αντιστρέψιμη αφινική απεικόνιση)
$K_2(x) = L_2(M_2(x))$ (αντιστρέψιμη αφινική απεικόνιση)
$K(x) = M_1(L(M_2(x))) + M(x)$ (αφινική απεικόνιση)

Άρα η EA-ισοδυναμία είναι σχέση ισοδυναμίας. ■

Πρόταση 2.3.2 *Αν $\mathcal{A}$ είναι μία αφινική απεικόνιση από το $\mathbb{F}_2^{2n}$ στον εαυτό της, τότε η $\mathcal{A}$ έχει τη μορφή*

$$\mathcal{A}(x, y) = (L_1(x, y) + c_1, L_2(x, y) + c_2)$$

όπου L_1, L_2 *γραμμικές συναρτήσεις από το* $\mathbb{F}_2^{2n}$ *στο* $\mathbb{F}_2^n$ *και* c_1, c_2 *κατάλληλες σταθερές.*

Αν ορίσουμε συναρτήσεις f_1, $f_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *με*

$$\begin{cases} f_1(x) = L_1(x, y) + c_1 \\ f_2(x) = L_2(x, y) + c_2 \end{cases}$$

τότε

$$\mathcal{A}(x, y) = (f_1(x), f_2(x)).$$

Έστω $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, τότε το γράφημά της είναι το σύνολο

$$\Gamma_f = \{(x, f(x)) \, : \, x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^{2n}$$

Ορισμός 2.3.2 *Δύο συναρτήσεις* $f, f' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *είναι Carlet-Charpin-Zinoviev ισοδύναμες (CCZ-ισοδύναμες), αν υπάρχει αντιστρέψιμη αφινική απεικόνιση* $\mathcal{L} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ *τέτοια ώστε* $\mathcal{L}(\Gamma_f) = \Gamma_{f'}$

Έστω

$$\Gamma_f = \{(x, f(x)) \, : \, x \in \mathbb{F}_2^n\}$$

το γράφημα μιας συνάρτησης $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Αν $\mathcal{L}$ μια αφινική απεικόνιση του $\mathbb{F}_2^{2n}$, τότε σύμφωνα με την Πρόταση 2.3.2:

$$\begin{aligned} \mathcal{L}(\Gamma_f) &= \{\mathcal{L}(x, f(x)) \, : \, x \in \mathbb{F}_2^n\} \\ &= \{(L_1(x, f(x)) + c_1, L_2(x, f(x)) + c_2) \, : \, x \in \mathbb{F}_2^n\} \\ &= \{(f_1(x), f_2(x)) \, : \, x \in \mathbb{F}_2^n\} \end{aligned}$$

Πρόταση 2.3.3 *Η σχέση CCZ είναι σχέση ισοδυναμίας.*

Απόδειξη

ανακλαστική $\mathbf{f \sim f}$

$$\mathcal{L}(\Gamma_f) = \Gamma_f$$

όπου $\mathcal{L}$ η ταυτοτική απεικόνιση.

συμμετρική $\mathbf{f \sim g \Leftrightarrow g \sim f}$

$$f \sim g \;\Rightarrow\; \mathcal{L}(\Gamma_f) = \Gamma_g \;\Rightarrow\; \mathcal{L}^{-1}(\Gamma_g) = \Gamma_f \;\Rightarrow\; \mathcal{M}(\Gamma_g) = \Gamma_f \;\Rightarrow g \sim f$$

όπου $\mathcal{M} = \mathcal{L}^{-1}$ η αντίστροφη απεικόνιση της $\mathcal{L}$, η οποία είναι επίσης αφινική.

$$\textbf{μεταβατική} \quad \left.\begin{array}{l} \mathbf{f \sim g} \\ \mathbf{g \sim h} \end{array}\right\} \Rightarrow \mathbf{f \sim h}$$

Αν

$$\begin{cases} \mathcal{L}(\Gamma_f) = \Gamma_g \\ \mathcal{M}(\Gamma_g) = \Gamma_h \end{cases}$$

τότε

$$\Gamma_h = \mathcal{M}(\Gamma_g) = \mathcal{M}(\mathcal{L}(\Gamma_f)) = \mathcal{K}(\Gamma_f)$$

όπου $\mathcal{K} = \mathcal{M} \circ \mathcal{L}$ αφινική, ως σύνθεση αφινικών απεικονίσεων. ■

Πρόταση 2.3.4 *Το σύνολο $\mathcal{L}(\Gamma_f)$ αποτελεί γράφημα μιας συνάρτησης f', δηλαδή $\mathcal{L}(\Gamma_f) = \Gamma_{f'}$, αν και μόνο αν η συνάρτηση f_1 είναι αντιστρέψιμη και τότε $f' = f_2 \circ f_1^{-1}$.*

Απόδειξη

($\Rightarrow$)

Το σύνολο $\mathcal{L}(\Gamma_f)$ είναι γράφημα μιας συνάρτησης f' συνεπώς $\mathcal{L}(\Gamma_f) = \Gamma_{f'}$, δηλαδή

$\forall x \in \mathbb{F}_2^n \quad \exists y \in \mathbb{F}_2^n$ τέτοιο ώστε $f_1(x) = y$ και $f_2(x) = f'(y)$

και

$\forall y \in \mathbb{F}_2^n \quad \exists x \in \mathbb{F}_2^n$ τέτοιο ώστε $f'(y) = f_2(x)$ και $y = f_1(x)$

δηλαδή η συνάρτηση f_1 είναι επί του $\mathbb{F}_2^n$ και επειδή το πεπερασμένο σύνολο τιμών $\mathbb{F}_2^n$ ταυτίζεται με το πεδίο ορισμού, η f_1 είναι "$1-1$". Άρα η f_1 είναι αντιστρέψιμη.
Επίσης

$$f'(y) = f_2(x) = f_2(f_1^{-1}(y)) \Rightarrow f'(y) = f_2 \circ f_1^{-1}(y)$$

($\Leftarrow$)

Η f_1 είναι επί του $\mathbb{F}_2^n$, δηλαδή

$\forall y \in \mathbb{F}_2^n \quad \exists x \in \mathbb{F}_2^n$ τέτοιο ώστε $y = f_1(x)$

Για να είναι το σύνολο $\mathcal{L}(\Gamma_f)$ γράφημα της f' πρέπει επιπλέον να ισχύει

$\forall x \in \mathbb{F}_2^n \quad \exists y \in \mathbb{F}_2^n$ τέτοιο ώστε $f_1(x) = y$ και $f_2(x) = f'(y)$

Η f_1 είναι αντιστρέψιμη, συνεπώς είναι "$1-1$", δηλαδή $\forall x \in \mathbb{F}_2^n$ υπάρχει η f_1^{-1}. Άρα

$$\forall x \in \mathbb{F}_2^n \quad \exists y \in \mathbb{F}_2^n \text{ τέτοιο ώστε } f_2(x) = (f_2(f_1^{-1}(y))) \Rightarrow f_2(x) = f'(y)$$

Άρα το σύνολο $\mathcal{L}(\Gamma_f)$ είναι το γράφημα της συνάρτησης $f' = f_2 \circ f_1^{-1}$

Από τους παραπάνω ορισμούς και τις σχέσεις ισοδυναμίας προκύπτουν τα εξής συμπεράσματα:

Πόρισμα 2.3.1 *Αν δύο συναρτήσεις $f, f' : \mathbb{F}_2^n \to \mathbb{F}_2^n$ είναι EA ισοδύναμες, τότε είναι και CCZ ισοδύναμες.*

Απόδειξη

Οι f, f' είναι EA ισοδύναμες, δηλαδή υπαρχουν αντιστρέψιμες αφινικές απεικονίσεις $L_1, L_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ και αφινική ακεικόνιση $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ έτσι ώστε

$$f'(x) = L_1 \circ f \circ L_2(x) + L(x)$$

Για να αποδείξουμε ότι οι f, f' είναι CCZ ισοδύναμες αρκεί να δείξουμε ότι αν $\Gamma_f = \{(y, f(y)) : y \in \mathbb{F}_2^n\}$ και $\Gamma_{f'} = \{(x, f'(x)) : x \in \mathbb{F}_2^n\}$ τα γραφήματα των f, f' αντίστοιχα, τότε υπάρχει αντιστρέψιμη αφινική απεικόνιση $\mathcal{L}$ τέτοια ώστε

$$\mathcal{L}(\Gamma_{f'}) = \Gamma_f \quad \Leftrightarrow \quad \mathcal{L}(x, f'(x)) = (y, f(y))$$

Από την EA ισοδυναμία των f, f' έχουμε

$$\begin{aligned} f'(x) &= L_1(f(L_2(x))) + L(x) \Rightarrow \\ \Rightarrow L_1(f(L_2(x))) &= f'(x) - L(x) \end{aligned}$$

εφαρμόζοντας την αντίστροφη απεικόνιση της L_1, έστω $L_1^{-1}(x) = M(x) + c$, όπου $M(x)$ γραμμική και c σταθερά, παίρνουμε

$$\begin{aligned} f(L_2(x)) &= L_1^{-1}(f'(x) - L(x)) \quad \Rightarrow \\ \Rightarrow \quad f(L_2(x)) &= M(f'(x)) - M(L(x)) + c \\ \Rightarrow \quad f(L_2(x)) &= L_1^{-1}(f'(x)) - M(L(x)) \end{aligned}$$

Αν ορίσουμε την αφινική συνάρτηση $\mathcal{L}(x, y) = (L_2(x),\, L_1^{-1}(y) - M(L(x)))$, τότε

$$\begin{aligned} \mathcal{L}(x, f'(x)) &= (L_2(x),\, L_1^{-1}(f'(x)) - M(L(x))) = \\ &= (L_2(x),\, f(L_2(x))) = \\ &= (y, f(y)) \end{aligned}$$

Για να ολοκληρωθεί η απόδειξη θα πρέπει να δείξουμε ότι η αφινική απεικόνιση $\mathcal{L}$ είναι αντιστρέψιμη:

έστω $x_1, x_2, y_1, y_2 \in \mathbb{F}_{2^n}$, τότε

$$\mathcal{L}(x_1, y_1) = \mathcal{L}(x_2, y_2) \Rightarrow \begin{cases} L_2(x_1) = L_2(x_2) \\ L_1^{-1}(y_1) - M(L(x_1)) = L_1^{-1}(y_2) - M(L(x_2)) \end{cases}$$

- $L_2(x_1) = L_2(x_2) \overset{L_2 \text{"1-1"}}{\Longrightarrow} x_1 = x_2$

- $L_1^{-1}(y_1) - M(L(x_1)) = L_1^{-1}(y_2) - M(L(x_2)) \Rightarrow$

  $L_1^{-1}(y_1) - M(L(x_1)) = L_1^{-1}(y_2) - M(L(x_1)) \Rightarrow$

  $L_1^{-1}(y_1) = L_1^{-1}(y_2) \overset{L_1^{-1} \text{"1-1"}}{\Longrightarrow} y_1 = y_2$

δηλαδή η $\mathcal{L}$ είναι "$1-1$" και επειδή το πεδίο ορισμού ταυτίζεται με το σύνολο τιμών, είναι και επί. Άρα η $\mathcal{L}$ είναι μια αφινική, αντιστρέψιμη απεικόνιση. ■

Πόρισμα 2.3.2 *Αν η συνάρτηση f είναι ισομορφισμός τότε η f είναι CCZ ισοδύναμη με την αντίστροφή της, f^{-1}.*

Απόδειξη

Για να αποδείξουμε ότι $f \overset{ccz}{\sim} f^{-1}$, αρκεί να δείξουμε ότι υπάρχει $\mathcal{L}$ αντιστρέψιμη αφινική απεικόνιση, τέτοια ώστε

$$\mathcal{L}(\Gamma_f) = \Gamma_{f^{-1}} \Rightarrow (f_1(x), f_2(x)) = (y, f^{-1}(y)) \Rightarrow (f_1(x), f_2(x)) = (y, f_2 \circ f_1^{-1}(y))$$

Εάν επιλέξουμε

$$\begin{cases} f_1(x) = f(x) \\ f_2(x) = x \end{cases}$$

τότε έχουμε $f^{-1}(x) = f_2(f_1^{-1}(x)) = f_1^{-1}(x) = f^{-1}(x)$. ■

Πόρισμα 2.3.3 *Αν $f \overset{ccz}{\sim} f'$ και η συνάρτηση f' είναι APN, τότε και η f είναι APN.*

Απόδειξη

Αρκεί να αποδείξουμε ότι για κάθε $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, υπάρχουν $a', b' \in \mathbb{F}_{2^n}$ με $a' \neq 0$ τέτοια ώστε $N_f(a,b) = N_{f'}(a',b')$, όπου $N_f(a,b), N_{f'}(a',b')$ το πλήθος λύσεων των $f(x+a)+f(x)=b$ και $f'(x+a')+f'(x)=b'$ αντίστοιχα.

Επίσης, θεωρούμε την αφινική απεικόνιση $\mathcal{A} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ με

$$\mathcal{A}(x,y) = (L_1(x,y) + c_1, L_2(x,y) + c_2)$$

με L_1, L_2 γραμμικές απεικονίσεις. Θέτοντας $x = y = 0$ παίρνουμε $\mathcal{A}(0,0) = (c_1, c_2)$, άρα

$$\mathcal{A}(x,y) = \mathcal{L}(x,y) + \mathcal{A}(0,0)$$

όπου $\mathcal{L}$ γραμμική απεικόνιση.

Έχουμε

$$\begin{aligned}
N_f(a,b) &= |\{x \in \mathbb{F}_2^n : f(x+a)+f(x)=b\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : (x,f(x))+(y,f(y))=(a,b)\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : \mathcal{A}((x,f(x))+(y,f(y)))=\mathcal{A}(a,b)\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : \mathcal{L}(x,f(x))+\mathcal{L}(y,f(y))+\mathcal{A}(0,0)=\mathcal{L}(a,b)+\mathcal{A}(0,0)\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : \mathcal{A}(x,f(x))-\mathcal{A}(0,0)+\mathcal{A}(y,f(y))-\mathcal{A}(0,0)+\mathcal{A}(0,0)=\mathcal{L}(a,b)+\mathcal{A}(0,0)\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : \mathcal{A}(x,f(x))+\mathcal{A}(y,f(y))=\mathcal{L}(a,b)\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : (f_1(x),f_2(x))+(f_1(y),f_2(y))=\mathcal{L}(a,b)\}| \\
&\overset{f\sim f'}{=} |\{(x,y) \in \mathbb{F}_2^{2n} : (x,f_2(f_1^{-1}(x))+(y,f_2(f_1^{-1}(y))=\mathcal{L}(a,b)\}| \\
&= |\{(x,y) \in \mathbb{F}_2^{2n} : (x,f'(x))+(y,f'(y))=\mathcal{L}(a,b)\}| \\
&= N_{f'}(\mathcal{L}(a,b)) \\
&= N_{f'}(a',b')
\end{aligned}$$

Αν $a' \neq 0$, τότε επειδή η f' είναι APN και $N_f(a,b) = N_{f'}(a',b') \leq 2$, είναι και η f APN.

Αν $a' = 0$, τότε $N_{f'}(0,b') = 0 \leq 2$, εκτός από την περίπτωση όπου $b' = 0$. Όμως, όταν $a' = b' = 0$ έχουμε

$$\mathcal{L}(a,b) = (0,0)$$

κάτι που είναι αδύνατο, διότι η $\mathcal{L}$ είναι αντιστρέψιμη και $a \neq 0$. ■

Κεφάλαιο 3

APN συναρτήσεις και κώδικες

3.1 Γραμμικοί δυαδικοί κώδικες

Ορισμός 3.1.1 *Έστω $A = \{\alpha_1, \ldots, \alpha_q\}$ ένα σύνολο με q στοιχεία, το οποίο θα ονομάζουμε αλφάβητο.*

(i) Μια λέξη μήκους n πάνω από το αλφάβητο A είναι μια ακολουθία $w = w_1 w_2 \ldots w_n$, όπου $w_i \in A$ για κάθε i. Η λέξη w μπορεί επίσης να θεωρηθεί διάνυσμα $(w_1, w_2, \ldots, w_n)$.

(ii) Ένας κώδικας μήκους n πάνω από το A είναι ένα υποσύνολο του A^n.

(iii) Το πλήθος των λέξεων του κώδικα C ονομάζεται μέγεθος του C.

Ορισμός 3.1.2 *Ένας γραμμικός κώδικας C μήκους n πάνω από το $\mathbb{F}_q$ είναι ένας υπόχωρος του $\mathbb{F}_q^n$.*

Για τον πλήρη χαρακτηρισμό ενός κώδικα είναι απαραίτητο να γνωρίζουμε, εκτός από το μήκος του n, τη διάστασή του και την απόσταση *Hamming*.

Ορισμός 3.1.3 *Η διάσταση του γραμμικού κώδικα C είναι η διάσταση του C ως διανυσματικού χώρου πάνω από το $\mathbb{F}_q$*

Ορισμός 3.1.4 *(Hamming distance) Έστω $\mathbf{x}, \mathbf{y}$ λέξεις μήκους n ενός αλφαβήτου A. Η απόσταση Hamming από το $\mathbf{x}$ στο $\mathbf{y}$, η οποία συμβολίζεται με $d(\mathbf{x}, \mathbf{y})$, ορίζεται να είναι ο αριθμός των γραμμάτων όπου οι λέξεις $\mathbf{x}, \mathbf{y}$ διαφέρουν. Αν $\mathbf{x} = x_1 x_2 \ldots x_n$ και $\mathbf{y} = y_1 y_2 \ldots y_n$ τότε*

$$d(\mathbf{x}, \mathbf{y}) = d(x_1, y_1) + d(x_2, y_2) + \ldots + d(x_n, y_n)$$

όπου

$$d(x_i, y_i) = \begin{cases} 1, & \text{αν } x_i \neq y_i \\ 0, & \text{αν } x_i = y_i. \end{cases}$$

Ορισμός 3.1.5 *Σε κώδικα C που περιέχει τουλάχιστον δύο λέξεις, ορίζουμε*

$$d(C) = min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C,\ \mathbf{x} \neq \mathbf{y}\}$$

να είναι η ελάχιστη απόσταση του C.

Το μήκος n, η διάσταση k και η απόσταση d ονομάζονται παράμετροι του γραμμικού κώδικα C, ο οποίος συμβολίζεται με $[n, k, d]$.

Ορισμός 3.1.6 *(Hamming weight) Έστω x μια λέξη του $\mathbb{F}_q^n$. Το βάρος Hamming της x, το οποίο συμβολίζεται με $wt(x)$, ορίζεται να είναι το πλήθος των μη μηδενικών συνιστωσών της λέξης x:*

$$wt(x) = d(x, 0)$$

Παράδειγμα 3.1.1 Έστω $C = \{00000, 00111, 11111\}$ ένας δυαδικός γραμμικός κώδικας μήκους 5, τότε:

$$d(00000, 00111) = 3$$
$$d(00000, 11111) = 5$$
$$d(00111, 11111) = 2$$

Άρα $d(C) = 2$, δηλαδή ο C είναι ένας $[5, 3, 2]$-κώδικας. Επίσης,

$$wt(00111) = 3$$
$$wt(11111) = 5$$

3.2 Ο δυικός κώδικας

Ορισμός 3.2.1 *Ο δυικός κώδικας του C, ο οποίος συμβολίζεται με $C^\perp$, είναι το ορθογώνιο συμπλήρωμα του C, δηλαδή*

$$C^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{v} \cdot \mathbf{s} = \mathbf{0} \quad \forall\, \mathbf{s} \in C\}$$

Θεώρημα 3.2.1 *Έστω C γραμμικός κώδικας μήκους n πάνω από το $\mathbb{F}_q$. Τότε*

(i) ο $C^\perp$ είναι γραμμικός κώδικας και

$$dim(C) + dim(C^\perp) = n$$

(ii) $(C^\perp)^\perp = C$

Απόδειξη

(*i*) Από τον ορισμό του $C^\perp$ και από το γεγονός ότι ο C είναι υπόχωρος του $\mathbb{F}_q^n$ προκύπτει ότι ο $C^\perp$ είναι επίσης υποσύνολο του $\mathbb{F}_q^n$.

Έστω $\mathbf{v}, \mathbf{w} \in C^\perp$ και $\lambda, \mu \in \mathbb{F}_q$, τότε $\forall\, \mathbf{s} \in C$ έχουμε:

$$(\lambda\mathbf{v} + \mu\mathbf{w}) \cdot \mathbf{s} = \lambda(\mathbf{v} \cdot \mathbf{s}) + \mu(\mathbf{w} \cdot \mathbf{s}) = 0$$

Συνεπώς ο $C^\perp$ είναι υπόχωρος του $\mathbb{F}_q^n$.

Για $C = \{0\}$ η σχέση $dim(C) + dim(C^\perp) = n$ είναι αληθής. Έστω $dim(C) = k \geq 1$ και έστω $\{v_1, \ldots, v_k\}$ μια βάση του C. Θα δείξουμε ότι $dim(C^\perp) = n - k$.

Έχουμε

$$\mathbf{x} \in C^\perp \;\Leftrightarrow\; v_1 \cdot \mathbf{x} = \ldots = v_k \cdot \mathbf{x} = 0 \;\Leftrightarrow\; A\mathbf{x}^T = 0$$

όπου A είναι ο $k \times k$ πίνακας με γραμμές τα διανύσματα $v_1, \ldots, v_k$. Οι γραμμές του πίνακα A είναι γραμμικώς ανεξάρτητες, επομένως το $A\mathbf{x}^T = 0$ είναι ένα γραμμικό σύστημα με k γραμμικές εξισώσεις n μεταβλητών. Από τη γραμμική άλγεβρα γνωρίζουμε ότι μια βάση του χώρου λύσεων αποτελείται από $n-k$ διανύσματα, δηλαδή $dim(C^\perp) = n-k$.

(*ii*) Αντικαθιστώντας το C με $C^\perp$ στην παραπάνω σχέση προκύπτει:

$$dim(C^\perp) + dim(C^\perp)^\perp = n$$

και μαζί με την $dim(C) + dim(C^\perp) = n$ παίρνουμε

$$dim(C) = dim(C^\perp)^\perp$$

Επομένως για να δείξουμε ότι $(C^\perp)^\perp = C$ αρκεί $C \subseteq (C^\perp)^\perp$.

Ένα διάνυσμα $\mathbf{v} \in \mathbb{F}_q^n$ είναι στοιχείο του $(C^\perp)^\perp$ αν και μόνο αν $\mathbf{v} \cdot \mathbf{x} = \mathbf{0}$, $\forall\, \mathbf{x} \in C^\perp$. Έστω $\mathbf{c} \in C$, τότε εξ ορισμού του $C^\perp$ ισχύει

$$\mathbf{c} \cdot \mathbf{x} = \mathbf{0}\,, \quad \forall\, \mathbf{x} \in C^\perp$$

άρα $\mathbf{c} \in (C^\perp)^\perp$ ■

Πρόταση 3.2.1 *Αν V, W διανυσματικοί χώροι, τότε*

$$V \leq W \quad \Leftrightarrow \quad W^\perp \leq V^\perp$$

Απόδειξη

($\Rightarrow$) Υποθέτουμε ότι $V \leq W$.
Έστω $b \in W^{\perp}$, τότε για κάθε $w \in W$ έχουμε

$$b \cdot w = 0$$

Αν $v \in V$, τότε $v \in W$, άρα

$$\forall v \in V \quad b \cdot v = 0 \Rightarrow b \in V^{\perp}$$

($\Leftarrow$) Υποθέτουμε ότι $W^{\perp} \leq V^{\perp}$. Τότε από το ευθύ έχουμε

$$W^{\perp} \leq V^{\perp} \Rightarrow (V^{\perp})^{\perp} \leq (W^{\perp})^{\perp} \Rightarrow V \leq W$$

3.3 Πίνακες βάσης και πίνακες ελέγχου

Ορισμός 3.3.1 (*i*) *Ο πίνακας βάσης (generator matrix) ενός γραμμικού κώδικα C είναι ένας πίνακας G, του οποίου οι γραμμές αποτελούν βάση του C.*

(*i*) *Ο πίνακας ελέγχου (parity-check matrix) ενός γραμμικού κώδικα C είναι ο πίνακας βάσης του δυικού κώδικα $C^{\perp}$.*

Επομένως αν C είναι ένας $[n, k]$ γραμμικός κώδικας, τότε ο πίνακας βάσης G θα έχει διάσταση $k \times n$, ενώ ο πίνακας ελέγχου $(n-k) \times n$.

Για να αποδείξουμε ότι ένας $k \times n$ πίνακας είναι πίνακας βάσης ενός $[n, k]$ γραμμικού κώδικα C, αρκεί να δείξουμε ότι οι γραμμές του G είναι γραμμικώς ανεξάρτητες και παράγουν τον C. Όμοια εργαζόμαστε για να αποδείξουμε ότι ένας πίνακας $(n-k) \times n$ είναι πίνακας ελέγχου του C.

Λήμμα 3.3.1 *Έστω C ένας $[n, k]$ γραμμικός κώδικας πάνω από το $\mathbb{F}_q$ με πίνακα βάσης G. Τότε ένα στοιχείο $\mathbf{v}$ του $\mathbb{F}_q^n$ ανήκει στον $C^{\perp}$ αν και μόνο αν είναι ορθογώνιο σε κάθε γραμμή του G, δηλαδή*

$$\mathbf{v} \in C^{\perp} \Leftrightarrow \mathbf{v} \cdot G^T = 0$$

Ειδικότερα, δεδομένου ενός $(n-k) \times n$ πίνακα H, ο H είναι πίνακας ελέγχου του C αν και μόνο αν οι γραμμές του H είναι γραμμικώς ανεξάρτητες και $HG^T = 0$.

Απόδειξη

Έστω $\mathbf{r}_i$ τυχαία γραμμή του G, τότε κάθε στοιχείο του C γράφεται στη μορφή

$$\mathbf{c} = \lambda_1 \mathbf{r}_1 + \ldots + \lambda_k \mathbf{r}_k$$

όπου $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q$.

Αν $\mathbf{v} \in C^\perp$, τότε $\mathbf{v} \cdot \mathbf{c} = \mathbf{0} \quad \forall c \in C$, δηλαδή το $\mathbf{v}$ είναι ορθογώνιο στο $\mathbf{r}_i$, $i = 1, \ldots, k$, επομένως $\mathbf{v}G^T = 0$.

Αντίστροφα, αν $\mathbf{v} \cdot \mathbf{r}_i = 0,\ i = 1, \ldots, k$ τότε για $\mathbf{c} = \lambda_1\mathbf{r}_1 + \ldots + \lambda_k\mathbf{r}_k$ έχουμε:

$$\mathbf{v} \cdot \mathbf{c} = \lambda_1(\mathbf{v}\mathbf{r}_1) + \ldots + \lambda_k(\mathbf{v}\mathbf{r}_k) = 0$$

Για το δεύτερο μέρος του Λήμματος, αν Η είναι ο πίνακας ελέγχου του C, τότε εξ ορισμού οι γραμμές του, $\mathbf{h}_i,\ i = 1, \ldots, n-k$, είναι γραμμικώς ανεξάρτητες. Επίσης οι γραμμές αποτελούν λέξεις του $C^\perp$, επομένως σύμφωνα με τα παραπάνω:

$$\left.\begin{array}{l} \mathbf{h}_1 G^T = 0 \\ \mathbf{h}_2 G^T = 0 \\ \quad \vdots \\ \mathbf{h}_{n-k} G^T = 0 \end{array}\right\} \Rightarrow HG^T = 0$$

Αντίστροφα, αν $HG^T = 0$, τότε σύμφωνα με το πρώτο μέρος του Λήμματος, οι γραμμές του Η, άρα και ο χώρος γραμμών του Η, περιέχονται στον $C^\perp$. Επίσης, από το γεγονός ότι ο πίνακας Η έχει γραμμικώς ανεξάρτητες γραμμές προκύπτει ότι η διάσταση του χώρου γραμμών είναι $n-k$, δηλαδή ο $C^\perp$ ταυτίζεται με τον χώρο γραμμών του Η, άρα ο Η είναι ο πίνακας ελέγχου του C. ■

Πρόταση 3.3.1 *Έστω C ένας γραμμικός κώδικας και H ο αντίστοιχος πίνακας ελέγχου. Τότε τα παρακάτω είναι ισοδύναμα:*

(i) ο C έχει ελάχιστη απόσταση d

(ii) οποιεσδήποτε $d-1$ στήλες του H είναι γραμμικώς ανεξάρτητες και υπάρχουν d γραμμικώς εξαρτημένες στήλες.

Παράδειγμα 3.3.1 Έστω C ένας δυαδικός γραμμικός κώδικας με πίνακα ελέγχου

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

Αν παρατηρήσυμε τις στήλες του Η, θα δούμε ότι καμία δεν είναι η μηδενική και ανά δύο δεν αθροίζουν στο $\mathbf{0}^T$. Άρα κάθε δύο στήλες είναι γραμμικώς ανεξάρτητες. Επίσης, υπάρχουν τρείς στήλες, οι 1,3 και 4, οι οποίες είναι γραμμικώς εξαρτημένες. Συνεπώς, η απόσταση του κώδικα C είναι $d = 3$.

3.4 Ο επεκτεταμένος κώδικας του C

Ορισμός 3.4.1 *Για κάθε κώδικα C πάνω από το $\mathbb{F}_q$, ο επεκτεταμένος κώδικας (extended code) του C συμβολίζεται με $\widetilde{C}$ και ορίζεται να είναι το σύνολο:*

$$\widetilde{C} = \{(-\sum_{i=1}^{n} \mathbf{c}_i, \mathbf{c}_1, \ldots, \mathbf{c}_n) : (\mathbf{c}_1, \ldots, \mathbf{c}_n) \in C\}$$

Για $q = 2$ η επιπρόσθετη συνιστώσα $-\sum_{i=1}^{n} \mathbf{c}_i = \sum_{i=1}^{n} \mathbf{c}_i$ ονομάζεται συνιστώσα ελέγχου.

Θεώρημα 3.4.1 *Αν C είναι ένας $[n, k, d]$-γραμμικός κώδικας πάνω από το $\mathbf{F}_q$, τότε ο $\widetilde{C}$ είναι ένας $[n+1, k, d']$-γραμμικός κώδικας του $\mathbf{F}_q$ με*

$$d' = \begin{cases} d, & d \text{ άρτιος} \\ d+1, & d \text{ περιττός} \end{cases}$$

και πίνακα ελέγχου

$$\widetilde{H} = \left[\begin{array}{c|ccc} 1 & 1 & \ldots & 1 \\ \hline 0 & & & \\ \vdots & & H & \\ 0 & & & \end{array}\right]$$

όπου H ο πίνακας ελέγχου του C.

Απόδειξη

Εξ ορισμού ο $\widetilde{C}$ έχει μια επιπλέον συνιστώσα, επομένως το μήκος του κώδικα αυξάνεται κατά μια μονάδα και από n γίνεται $n+1$.

Όσον αφορά στη δεύτερη παράμετρο, η διάσταση k δεν αλλάζει, διότι δεν μεταβλήθηκε το πλήθος των διανυσμάτων, αλλά το μήκος τους.

Στη συνέχεια διακρίνουμε περιπτώσεις για την απόσταση d του C.

1^{η} περίπτωση: d περιττός

Για τον πίνακα H γνωρίζουμε ότι οποιεσδήποτε $d-1$ στήλες είναι γραμμικώς ανεξάρτητες και ότι υπάρχουν d στήλες γραμμικώς εξαρτημένες. Οι $d-1$ γραμμικώς ανεξάρτητες παραμένουν τέτοιες, ακόμη και μετά την προσθήκη της επιπλέον συνιστώσας του $\widetilde{H}$, '1'.

Αν συμβολίσουμε με h_i τις στήλες του H, τότε για τις d γραμμικώς εξαρτημένες έχουμε:

$$\begin{pmatrix} 1 \\ h_1 \end{pmatrix} + \begin{pmatrix} 1 \\ h_2 \end{pmatrix} + \ldots + \begin{pmatrix} 1 \\ h_d \end{pmatrix} = \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix} \tag{3.1}$$

που σημαίνει ότι είναι γραμμικώς ανεξέρτητες.

Εάν επιλέξουμε $d-1$ στήλες του H, προσθέσουμε την επιπλέον συνιστώσα,'1' και τις αθροίσουμε μαζί με την επιπρόσθετη στήλη του $\widetilde{H}$, προκύπτει η παρακάτω σχέση:

$$\begin{pmatrix} 1 \\ h_1 \end{pmatrix} + \begin{pmatrix} 1 \\ h_2 \end{pmatrix} + \ldots + \begin{pmatrix} 1 \\ h_{d-1} \end{pmatrix} + \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix} \neq \begin{pmatrix} 0 \\ \mathbf{0} \end{pmatrix} \tag{3.2}$$

δηλαδή οι παραπάνω d στήλες είναι γραμμικώς ανεξάρτητες.

Επίσης, υπάρχουν $d+1$ γραμικώς εξαρτημένες στήλες:

$$\begin{pmatrix} 1 \\ h_1 \end{pmatrix} + \begin{pmatrix} 1 \\ h_2 \end{pmatrix} + \ldots + \begin{pmatrix} 1 \\ h_d \end{pmatrix} + \begin{pmatrix} 1 \\ \mathbf{0} \end{pmatrix} = \begin{pmatrix} 0 \\ \mathbf{0} \end{pmatrix} \tag{3.3}$$

Από τις (3.1), (3.2) προκύπτει ότι οποιεσδήποτε d στήλες του $\widetilde{H}$ είναι γραμμικώς ανεξάρτητες, ενώ η (3.3) δηλώνει την ύπαρξη $d+1$ γραμμικώς εξαρτημένων στηλών. Επομένως η απόσταση του $\widetilde{C}$ είναι $d+1$.

2^{η} περίπτωση: d άρτιος

Εφαρμόζοντας την ίδια διαδικασία με παραπάνω έχουμε:

$$\begin{pmatrix} 1 \\ h_1 \end{pmatrix} + \begin{pmatrix} 1 \\ h_2 \end{pmatrix} + \ldots + \begin{pmatrix} 1 \\ h_{d-1} \end{pmatrix} \neq \begin{pmatrix} 0 \\ \mathbf{0} \end{pmatrix} \tag{3.4}$$

και

$$\begin{pmatrix} 1 \\ h_1 \end{pmatrix} + \begin{pmatrix} 1 \\ h_2 \end{pmatrix} + \ldots + \begin{pmatrix} 1 \\ h_d \end{pmatrix} = \begin{pmatrix} 0 \\ \mathbf{0} \end{pmatrix} \tag{3.5}$$

Άρα οποιεσδήποτε $d-1$ στήλες είναι γραμμικώς ανεξέρτητες και υπάρχουν d γραμμικώς εξαρτημένες. Συνεπώς $d(\widetilde{C}) = d$ ■

3.5 Ισοδυναμία γραμμικών κωδίκων

Ορισμός 3.5.1 *Δύο γραμμικοί κώδικες πάνω από το $\mathbb{F}_q$ ονομάζονται ισοδύναμοι αν ο ένας προκύπτει από τον άλλο με συνδυασμό των παρακάτω πράξεων:*

(A) *μετάθεση των γραμμάτων των λέξεων του κώδικα,*

(B) *πολλαπλασιασμό γραμμάτων σε συγκεκριμένες θέσεις με μη μηδενική σταθερά.*

Θεώρημα 3.5.1 *Δύο $k \times n$ πίνακες παράγουν ίσους κώδικες, αν ο ένας προκύπτει από τον άλλο με εφαρμογή μιας ή περισσοτέρων από τις παρακάτω πράξεις:*

R1 *μετάθεση γραμμών*

R2 *πολλαπλασιασμό γραμμής με μη μηδενική σταθερά*

R3 *πρόσθεση ενός πολλαπλασίου γραμμής σε μία άλλη,*

ενώ παράγουν ισοδύναμους κώδικες, με εφαρμογή των πράξεων

C1 *μετάθεση στηλών*

C2 *πολλαπλασιασμό στήλης με μη μηδενική σταθερά.*

Ορισμός 3.5.2 *(i) Ένας πίνακας βάσης της μορφής $[I_k|X]$ θεωρείται ότι βρίσκεται σε κανονική μορφή (standard form)*

(ii) Ένας πίνακας ελέγχου της μορφής $[Y|I_{n-k}]$ θεωρείται ότι βρίσκεται σε κανονική μορφή.

Θεώρημα 3.5.2 *Κάθε γραμμικός κώδικας C είναι ισοδύναμος με έναν κώδικα C', του οποίου ο πίνακας βάσης βρίσκεται σε κανονική μορφή.*

3.5.1 Ισοδυναμία δυαδικών γραμμικών κωδίκων

Όταν το αλφάβητο του κώδικα είναι το $\mathbb{F}_2$, οι πράξεις των πινάκων που παράγουν ισοδύναμους κώδικες είναι οι $R1, C1$, ενώ η $R3$ μετατρέπεται σε 'πρόσθεση γραμμών'. Πιο συγκεκριμένα, δύο πίνακες G_1, G_2 παράγουν τον ίδιο κώδικα αν συνδέονται με τη σχέση:

$$G_2 = MG_1$$

όπου M είναι ένας $k \times k$ αντιστρέψιμος πίνακας. Ουσιαστικά ο πίνακας M μεταθέτει ή/και προσθέτει γραμμές. Με άλλα λόγια, υπάρχει μία αντιστρέψιμη γραμμική απεικόνιση $\mathcal{L}$, με πίνακα τον M, η οποία αντιστοιχίζει την $j-$οστή στήλη του G_1 στην $j-$οστή στήλη του G_2.

Πρόταση 3.5.1 *Έστω C_1, C_2 $[n, k, d]$ γραμμικοί κώδικες και G_1, G_2 οι αντίστοιχοι πίνακες βάσης. Τότε, ο C_1 είναι ισοδύναμος με τον C_2 αν και μόνο αν υπάρχει αντιστρέψιμη γραμμική απεικόνιση $\mathcal{L}$ του $\mathbb{F}_2^k$, η οποία αντιστοιχίζει τις στήλες του G_1 στις στήλες του G_2.*

Παράδειγμα 3.5.1 Έστω

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

ο πίνακας βάσης που αντιστοιχεί στον κώδικα C_1 και

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

ένας αντιστρέψιμος πίνακας. Τότε ο πίνακας $G_2 = MG_1$ θα είναι ο

$$G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

του οποίου η πρώτη γραμμή είναι το άθροισμα της πρώτης γραμμής του G_1 με την τρίτη. Σύνεπώς ο κώδικας C_2 που παράγει ο G_2, είναι τελικά ο C_1.

Επίσης, εάν ο πίνακας G_2 προκύπτει από τη σχέση $G_2 = G_1P$, για κάποιον πίνακα μετάθεσης P, τότε οι αντίστοιχοι κώδικες C_1, C_2 είναι ισοδύναμοι. Ο πίνακας P ουσιαστικά μεταθέτει τις στήλες του G_1.

Παράδειγμα 3.5.2 Αν πολλαπλασιάσουμε από δεξιά τον πίνακα G_1 του προηγούμενου παραδείγματος με τον πίνακα μετάθεσης

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

έχουμε:

$$G_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Παρατηρώντας το αποτέλεσμα του γινομένου βλέπουμε ότι έχουν μετατεθεί οι στήλες 1 και 4 του G_1. Επομένως οι κώδικες που αντιστοιχούν στους G_1, G_2 είναι ισοδύναμοι.

Γενικά, οι κώδικες C_1, C_2 με αντίστοιχους πίνακες βάσης G_1, G_2 είναι ισοδύναμοι, αν $G_2P = MG_1$, για κάποιον αντιστρέψιμο πίνακα M και πίνακα μετάθεσης P. Επιπλέον, δύο κώδικες C_1, C_2 είναι ισοδύναμοι αν και μόνο αν οι αντίστοιχοι δυϊκοί είναι ισοδύναμοι. Αυτό ισχύει διότι οι μεταθέσεις των γραμμών-στηλών με τις οποίες ο G_2 παράγεται από τον G_1 διατηρούνται και στους πίνακες ελέγχου H_1, H_2.

Παράδειγμα 3.5.3 Έστω G_1, G_2 οι πίνακες βάσης του προηγουμενου παραδείγματος, όπου ο G_2 είναι ο G_1 με μετάθεση της πρώτης με την τέταρτη στήλη, και

$$H_1 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

ο πίνακας ελέγχου του C_2. Ονομάζουμε H_2 τον πίνακα που προκύπτει από τον H_1 με εναλλαγή της πρώτης με την τέταρτη στήλη:

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Υπολογίζουμε το γινόμενο

$$H_2 G_2^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = 0$$

δηλαδή ο H_2 είναι πίνακας ελέγχου του G_2.

3.6 APN και κώδικες

Στο πρώτο κεφάλαιο έγινε αναφορά στις συναρτήσεις APN, δόθηκαν οι απαραίτητοι ορισμοί και κάποιες ιδιότητές τους. Το δεύτερο κεφάλαιο ασχολείται με τη θεωρία κωδικοποίησης, όπου αναφέρονται τα στοιχεία εκείνα, που χαρακτηρίζουν τους γραμμικούς κώδικες και συγκεκριμένα, τους δυαδικούς γραμμικούς κώδικες.

Το γεγονός ότι κάθε γραμμικός κώδικας αντιστοιχίζεται με έναν πίνακα και ότι η μελέτη των πινάκων είναι σαφώς πιο εύκολη, σε σχέση με την μελέτη των συναρτήσεων, οδήγησε τους μαθηματικούς στην εύρεση συνδετικών κρίκων ανάμεσα στις συναρτήσεις APN και τους γραμμικούς κώδικες. Σε αυτό το κεφάλαιο γίνεται μελέτη αυτής της σχέσης των γραμμικών κωδίκων και των APN και παρουσιάζεται ένα Θεώρημα από τη μη δημοσιευμένη εργασία της ερευνητικής ομάδας του J.F.Dillon [2], το οποίο δίνει ακόμη έναν τρόπο ταξινόμησης των συναρτήσεων APN.

Ορισμός 3.6.1 *Ένας $[n, d, w]$ δυαδικός κώδικας σταθερού βάρους, είναι ένας δυαδικός κώδικας μήκους n και ελάχιστης απόστασης d, του οποίου όλες οι κωδικές λέξεις αποτελούνται από w άσσους. Επίσης, ορίζουμε $A(n, d, w)$ να είναι ο μέγιστος αριθμός λέξεων δυαδικού κώδικα μήκους n, ελάχιστης απόστασης d και σταθερού βάρους w.*

Από το [11], γνωρίζουμε ότι ισχύουν τα παρακάτω φράγματα για την παράμετρο $A(n, d, w)$:

Πρόταση 3.6.1 *Αν $[n, d, w]$ είναι ένας δυαδικός κώδικας σταθερού βάρους, τότε*

- $A(n, 2w, w) \leq \left\lfloor \frac{n}{w} \right\rfloor$
- $A(n, 2\delta, w) \leq \frac{\binom{n}{t}}{\binom{w}{t}}$ *για* $t = w - \delta + 1$.

Θεώρημα 3.6.1 *Δεν υπάρχει γραμμικός κώδικας με παραμέτρους* $[2^t - 2, 2^t - 2t - 1, 5]$, *για* $t > 3$

Απόδειξη

Έστω C ένας κώδικας πάνω από το $\mathbb{F}_q$ μήκους n και ελάχιστης απόστασης d. Για κάθε σημείο c του C θεωρούμε τη συνάρτηση S_c από το $\mathbb{F}_q^n$ στο $\mathbb{R}$ με τις εξής ιδιότητες:

(i) $S_c(x) \geq 0$, $\forall x \in \mathbb{F}_q^n$

(ii) $\sum_{c \in C} S_c(x) \leq 1$, $\forall x \in \mathbb{F}_q^n$

(iii) $|S_c| \geq s$, όπου $|S_c| = \sum_{x \in \mathbb{F}_q^n} S(x)$ και $s \in \mathbb{R}$

Τότε:

$$\sum_{x \in \mathbb{F}_q^n} \sum_{c \in C} S_c(x) \leq \sum_{x \in \mathbb{F}_q^n} 1 = q^n \tag{3.6}$$

και

$$\sum_{c \in C} \sum_{x \in \mathbb{F}_q^n} S_c(x) = \sum_{c \in C} |S_c| \geq \sum_{c \in C} s = |C|s \tag{3.7}$$

Συνδυάζοντας τις (3.6) και (3.7) προκύπτει η σχέση

$$|C| \leq \frac{q^n}{s} \tag{3.8}$$

η οποία είναι γνωστή ως το φράγμα του Johnson.

Έστω $d = 2e + 1 > 1$. Αν ορίσουμε τη χαρακτηριστική συνάρτηση

$$S_c(x) = \begin{cases} 1, & d(c, x) \leq e \\ 0, & d(c, x) > e \end{cases}$$

τότε από το φράγμα του Johnson παίρνουμε το φράγμα sphere packing [9]. Ορίζουμε B_x να είναι το σύνολο των λέξεων του κώδικα C που απέχουν από το $x \in \mathbb{F}_q^n$ απόσταση $e + 1$ και επιπλέον $d(x, C) = e + 1$. Δηλαδή

$$B_x = \{c \in C \, : \, d(x, c) = d(x, C) = e + 1\}$$

και θέτουμε $m = \max_{x\in\mathbb{F}_q^n} |B_x|$. Τότε, αν μαζί με τα σημεία που βρίσκονται μέσα στη σφαίρα ακτίνας e γύρω από το c επιλέξουμε και το $1/m$ των σημείων σε ακτίνα $e+1$, τα οποία απέχουν επίσης $e+1$ από τον C, τότε μπορούμε να βελτιώσουμε το παραπάνω φράγμα. Έτσι, η χαρακτηριστική συνάρτηση θα έχει τη μορφή:

$$S_c(x) = \begin{cases} 1, & d(c,x) \le e \\ \frac{1}{m}, & d(c,x) = e+1,\ d(C,x) = e+1 \end{cases}$$

Επίσης ορίζουμε

$$N_d(c) = \{c' \in C \,:\, d(c,c') = d\}$$

με

$$a_d(c) = |N_d(c)|$$

Επιπλέον, θέτουμε a_d να είναι ο μέσος όρος των σημείων που απέχουν απόσταση d μεταξύ τους, δηλαδή

$$a_d = \frac{1}{|C|}\sum_{c\in C} a_d(c)$$

Ας μελετήσουμε τα $x \in \mathbb{F}_q^n$, τα οποία απέχουν από τη λέξη $c \in C$ απόσταση $e+1$. Επιπλέον ισχύει $d(x,C) = e$ ή $e+1$. Γνωρίζουμε ότι το πλήθος των λέξεων με $d(x,c) = e+1$ είναι $\binom{n}{e+1}(q-1)^{e+1}$. Από αυτές, θα πρέπει λοιπόν να αφαιρέσουμε εκείνες για τις οποίες $d(x,C) = e$. Εφόσον λοιπόν $d(x,C) = e$, για κάθε $x \in \mathbb{F}_q^n$ υπάρχει μοναδικό $c' \in C$, τέτοιο ώστε $d(x,c') = e$. Τότε φυσικά ισχύει $d(c,c') = 2e+1$.

Αντίστροφα, για κάθε $c' \in C$ θα υπολογίσουμε το πλήθος των $x \in \mathbb{F}_q^n$ για τα οποία $d(c,x) = e$ και $d(x,c) = e+1$. Έστω

$$\begin{aligned} c &= (c_1, c_2, \ldots, c_n) \\ c' &= (c'_1, c'_2, \ldots, c'_n) \\ x &= (x_1, x_2, \ldots, x_n) \end{aligned}$$

και εφόσον $d(c,c') = d$, ας υποθέσουμε ότι $c_j \neq c'_j$, $1 \le j \le d$ και $c_i = c'_i$, $i = d+1, \ldots, n$, δηλαδή

$$\begin{aligned} c &= (c_1, \ldots, c_d, c_{d+1}, \ldots, c_n) \\ c' &= (c'_1, \ldots, c'_d, c_{d+1}, \ldots, c_n) \end{aligned}$$

Θα δείξουμε ότι $x_i = c_i$, $i = d+1, \ldots, n$. Έστω ότι $x_k \neq c_k$ για κάποιο $d+1 \le k \le n$. Τότε, το πολύ e από τις $x_1, \ldots, x_d$ συνιστώσες διαφέρουν από τις αντίστοιχες $c_1, \ldots, c_d$, διότι $d(x,c) = e+1$. Άρα, τουλάχιστον $d - e = e+1$ συνιστώσες από τις $x_1, \ldots, x_d$ έχουν καθοριστεί. Με τον ίδιο τρόπο, η σχέση $d(x,c') = e$ καθορίζει τις $d-(e-1) = e+2$ συνιστώσες της x. Συνολικά έχουμε

$$(e+1) + (e+2) = 2e+3 > d$$

που σημαίνει ότι υπάρχει κάποια συνιστώσα x_j, $1 \leq j \leq d$ τέτοια ώστε $x_j = c_j = c'_j$. Όμως αυτό δεν μπορεί να συμβαίνει, διότι $d(c, c') = d$. Συνεπώς,

$$x = (x_1, \ldots, x_d, c_{d+1}, \ldots, c_n).$$

Από τις d πρώτες συντεταγμένες, μπορούμε να επιλέξουμε με $\binom{d}{e} = \binom{d}{e+1}$ τρόπους τις e συνιστώσες στις οποίες οι x, c ταυτίζονται. Οι υπόλοιπες $e+1$ συνιστώσες καθορίζονται από τη λέξη c'. Οι c' και x διαφέρουν σε e συνιστώσες, επομένως υπάρχουν $\binom{d}{e+1}$ τρόποι επιλογής για τις $e+1$ κοινές συνιστώσες. Τελικά, το πλήθος των x που θα πρέπει να αφαιρεθούν είναι $a_d(c)\binom{d}{e}$.

Συνδυάζοντας το παραπάνω αποτέλεσμα με το φράγμα του Johnson, έχουμε

$$\begin{aligned} q^n &\geq \sum_{c \in C} \sum_{x \in \mathbb{F}_q^n} S_c(x) \\ &= \sum_{c \in C} \left(1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{e}(q-1)^e + \frac{1}{m}\left(\binom{n}{e+1}(q-1)^{e+1} - a_d(c)\binom{d}{e}\right)\right) \\ &= |C|\left(1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{e}(q-1)^e + \frac{1}{m}\left(\binom{n}{e+1}(q-1)^{e+1} - a_d\binom{d}{e}\right)\right) \end{aligned}$$

δηλαδή

$$s = 1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{e}(q-1)^e + \frac{1}{m}\left(\binom{n}{e+1}(q-1)^{e+1} - a_d\binom{d}{e}\right)$$

Για να βελτιώσουμε το s αρκεί να βρούμε ένα πάνω φράγμα για το m και το a_d. Θα περιοριστούμε στους κώδικες πάνω από το $\mathbb{F}_2$.

- **Φράγμα για το m**

  Ορίζουμε

  $$C_x = \{c - x \,:\, c \in B_x\}$$

  τότε $|B_x| = |C_x|$. Επίσης παρατηρούμε, ότι όλες οι λέξεις του συνόλου C_x έχουν σταθερό βάρος:

  $$wt(c - x) = d(x, c) = e + 1$$

  και αν $c_1, c_2 \in B_x$, τότε

  $$d(c_1 - x, c_2 - x) = wt(c_1 - c_2) \geq d$$

  Σύμφωνα με την Πρόταση 3.6.1, $A_2(n, d, e+1)$ είναι ο μέγιστος αριθμός λέξεων δυαδικού κώδικα μήκους n, ελάχιστης απόστασης d και σταθερού βάρους $e+1$, τότε

  $$m \leq A_2(n, d, e+1)$$

Έστω c_1 λέξη ενός δυαδικού κώδικα σταθερού βάρους. Αν εναλλάξουμε r άσσους της c_1 με r μηδενικά και ονομάσουμε c_2 τη λέξη που προκύπτει, τότε

$$d(c_1, c_2) = r + r = 2r$$

δηλαδή η απόστασή τους θα είναι πάντα άρτιος αριθμός.

Επίσης, από την Πρόταση 3.6.1 γνωρίζουμε ότι

$$A_2(n, 2w, w) \leq \left\lfloor \frac{n}{w} \right\rfloor$$

Συνδυάζοντας τα παραπάνω αποτελέσματα έχουμε:

$$m \leq A_2(n, 2e+1, e+1) = A_2(n, 2e+2, e+1) \leq \left\lfloor \frac{n}{e+1} \right\rfloor$$

- **Φράγμα για το α_d**

Αρχικά θα αποδείξουμε ότι

$$a_d(c) \leq \frac{\lfloor \frac{n-e}{e+1} \rfloor \binom{n}{e}}{\binom{d}{e}}$$

Όπως έχει προαναφερθεί, το σύνολο $N_d(c)$ αποτελείται από όλες τις λέξεις του κώδικα C, οι οποίες απέχουν από την c απόσταση $d = 2e + 1$. Επίσης, είναι γνωστό ότι η απόσταση του κώδικα είναι d, το οποίο συνεπάγεται ότι κάθε δύο λέξεις απέχουν τουλάχιστον d η μία από την άλλη. Ας ονομάσουμε w, w' τις λέξεις του κώδικα με τις παραπάνω ιδιότητες, δηλαδή

- $d(c, w) = d$ με $\begin{cases} c_i \neq w_i & 1 \leq i \leq d \\ c_i = w_i & d+1 \leq i \leq n \end{cases}$
- $d(c, w') = d$ με $\begin{cases} c_i \neq w_i & 1 \leq i \leq e,\ d+e+2 \leq i \leq n \\ c_i = w_i & e+1 \leq i \leq d+e+1 \end{cases}$
- $d(w, w') \geq d$

Παρατηρούμε ότι υπάρχουν e το πλήθος συνιστώσες, συκγεκριμένα στις θέσεις $e+1$ έως d, για τις οποίες ισχύει:

$$w_i \neq c_i \quad \text{και} \quad w'_i \neq c_i$$

Επομένως, αν διαλέξουμε $w_i = w'_i$ για $e+1 \leq i \leq d$, τότε οι αποστάσεις διατηρούνται. Αν όμως επιλέξουμε παραπάνω από e συνιστώσες οι οποίες θα είναι κοινές στις w, w' αλλά διαφορετικές στην c, τότε οι αποστάσεις αλλάζουν.

Έστω λοιπόν ότι $w_i = w'_i$ για $e \leq i \leq d$, δηλαδή οι w, w' μοιράζονται $d-e = e+1$ συνιστώσες. Τότε, η συνιστώσα στη θέση e είναι κοινή και στις τρείς λέξεις:

$$\left.\begin{array}{ll} c_i \neq w_i,\ 1 \leq i \leq d & \rightarrow c_e \neq w_e \\ c_i = w'_i,\ 1 \leq i \leq e & \rightarrow c_e = w'_e \end{array}\right\} \overset{w_e = w'_e}{\Rightarrow} c_e = w_e = w'_e$$

Όμως η παραπάνω ισότητα οδηγεί στη μείωση της απόστασης μεταξύ των c, w, η οποία γίνεται $d-1$. Αντίστοιχα, αν επιλέξουμε την επιπλέον συνιστώσα από την αντίθετη πλευρά, δηλαδή $w_i = w'_i$ για $e+1 \leq i \leq d+1$, τότε θα μειωθεί η απόσταση των c, w'. Επομένως, το μεγαλύτερο πλήθος κοινών συνιστωσών ανάμεσα στις c, w, w' είναι e.

Ας ονομάσουμε $a_{d,e}$ το πλήθος των λέξεων του κώδικα C, οι οποίες έχουν κοινές τις e συνιστώσες που περιέχονται στο d κομμάτι. Οι λέξεις με αυτή την ιδιότητα είναι το πολύ $\lfloor \frac{n-e}{e+1} \rfloor$, άρα

$$a_{d,e} \leq \left\lfloor \frac{n-e}{e+1} \right\rfloor \tag{3.9}$$

Επιπλέον, οι τρόποι με τους οποίους μπορούν να επιλεγούν αυτές οι συνιστώσες είναι $\binom{n}{e}/\binom{2e+1}{e}$. Άρα, για κάθε λέξη του κώδικα ισχύει:

$$a_d(c) \leq \frac{\lfloor \frac{n-e}{e+1} \rfloor \binom{n}{e}}{\binom{2e+1}{e}} \tag{3.10}$$

Σύμφωνα με την παραπάνω ανισότητα, σε κάθε λέξη $c \in C$ αντιστοιχεί πεπερασμένος αριθμός λέξεων που βρίσκονται σε απόσταση d. Άρα, θα υπάρχει τουλάχιστον μία λέξη, ας την ονομάσουμε c', η οποία έχει το μέγιστο $a_d(c')$. Επιπλέον, από το φράγμα του Johnson γνωρίζουμε ότι ο κώδικας C έχει πεπερασμένο πλήθος λέξεων. Επομένως, υπάρχει τουλάχιστον μία λέξη του κώδικα, η c', για την οποία ισχύει

$$a_d \leq a_d(c') \quad \overset{(3.10)}{\Rightarrow} \quad a_d \leq \frac{\lfloor \frac{n-e}{e+1} \rfloor \binom{n}{e}}{\binom{2e+1}{e}}$$

Στη συνέχεια, θα βελτιώσουμε το φράγμα για την ποσότητα $a_{d,e}$. Θέτουμε $a = \lfloor \frac{n-e}{e+1} \rfloor$ και χρησιμοποιώντας την ιδιότητα του ακέραιου μέρους προκύπτει

$$\left\lfloor \frac{n-e}{e+1} \right\rfloor \leq \frac{n-e}{e+1} \quad \Rightarrow \quad a(e+1) \leq n-e$$
$$\Rightarrow \quad n-e = a(e+1)+b, \quad 0 \leq b \leq e$$

Ας υποθέσουμε ότι το $a_{d,e}$ παίρνει τη μέγιστη δυνατή τιμή, δηλαδή $a_{d,e} = a$.

Περίπτωση 1^{η}: α περιττός

Αν προσθέσουμε όλες τις a λέξεις, θα προκύψει λέξη βάρους $a(e+1)+e = n-b$, διότι ανά δύο τα e κομμάτια εξουδετερώνονται και μένει μόνο ένα.

Αν $b = 0$, προκύπτει λέξη βάρους n, δηλαδή ο κώδικας περιέχει τη λέξη $\mathbf{1} = (11\ldots1)$. Αν η λέξη $\mathbf{1}$ ανήκε στο σύνολο των λέξεων με e κοινό κομμάτι, τότε θα έπρεπε σε όλες τις λέξεις το e κομμάτι να αποτελείται αποκλειστικά από άσσους. Επομένως, θα περιοριστούμε στην περίπτωση όπου $b \neq 0$. Αν λοιπόν $1 \leq b \leq e$, τότε η λέξη που προκύπτει ανήκει στις λέξεις με e κοινές συνιστώσες. Σε αυτή την περίπτωση, μπορούμε να βρούμε κώδικα ίδιας διάστασης και ίδιας ελάχιστης απόστασης, χωρίς τη λέξη με βάρος $n-b$. Αυτό μπορεί να επιτευχθεί με πρόσθεση μιας συνιστώσας ελέγχου (parity-check), αλλάζοντας έτσι το μήκος. Επιπλέον, η λέξη θα έχει βάρος $n-b+1$. Στη συνέχεια, μειώνουμε το μήκος και την ελάχιστη απόσταση αλλάζοντας τις συνιστώσες που δεν ανήκουν στο κοινό κομμάτι e, το βάρος θα παραμείνει $n-b+1$ [9]. Άρα, στη γενική περίπρωση όπου $a_{d,e} \leq a$, όταν το a είναι περιττό και $b \neq 0$, ισχύει $a_{d,e} \leq a-1$.

Επίσης, γνωρίζουμε ότι ισχύει η σχέση

$$\left\lfloor \frac{n-e}{e+1} - 1 \right\rfloor \leq \left\lfloor \frac{n-e}{e+1} \right\rfloor$$

συνεπώς

$$\frac{\lfloor \frac{n-e}{e+1} - 1 \rfloor \binom{n}{e}}{\binom{d}{e}} \leq \frac{\lfloor \frac{n-e}{e+1} \rfloor \binom{n}{e}}{\binom{d}{e}}$$

Άρα, δείξαμε ότι

$$a_d \leq \frac{\lfloor \frac{n-e}{e+1} - 1 \rfloor \binom{n}{e}}{\binom{d}{e}}$$

Επίσης, αποδείξαμε ότι $a_{d,e} \leq \lfloor \frac{n-e}{e+1} \rfloor - 1$, επομένως ισχύει η παρακάτω ανίσωση:

$$a_d \leq a_{d,e} \frac{\binom{n}{e}}{\binom{d}{e}} \leq \left(\left\lfloor \frac{n-e}{e+1} \right\rfloor - 1 \right) \frac{\binom{n}{e}}{\binom{d}{e}}$$

δηλαδή

$$a_d \leq \left(\left\lfloor \frac{n-e}{e+1} \right\rfloor - 1 \right) \frac{\binom{n}{e}}{\binom{d}{e}}$$

Θα αποδείξουμε ότι $\lfloor \frac{n-e}{e+1} \rfloor - 1 \leq \lfloor \frac{n-e}{e+1} - 1 \rfloor$. Για την απλοποίηση της απόδειξης θέτουμε $\lfloor \frac{n-e}{e+1} \rfloor = z$. Από τον ορισμό του ακέραιου μέρους έχουμε:

$$\lfloor z \rfloor \leq z < \lfloor z \rfloor + 1 \tag{3.11}$$

Άρα

$$\begin{aligned}
& \lfloor z \rfloor \leq z \\
\Rightarrow \quad & \lfloor z \rfloor - 1 \leq z - 1 \\
\Rightarrow \quad & \lfloor z \rfloor - 1 \leq z - 1 \overset{(3.11)}{<} \lfloor z - 1 \rfloor + 1 \\
\Rightarrow \quad & \lfloor z \rfloor - 1 < \lfloor z - 1 \rfloor + 1 \\
\Rightarrow \quad & \lfloor z \rfloor \leq \lfloor z - 1 \rfloor + 1 \\
\Rightarrow \quad & \lfloor z \rfloor - 1 \leq \lfloor z - 1 \rfloor
\end{aligned}$$

Τελικά έχουμε

$$\left\lfloor \frac{n-e}{e+1} \right\rfloor - 1 \leq \left\lfloor \frac{n-e}{e+1} - 1 \right\rfloor \leq \left\lfloor \frac{n-e}{e+1} \right\rfloor$$

Συνεπώς,

$$a_d \leq \frac{\lfloor \frac{n-e}{e+1} - 1 \rfloor \binom{n}{e}}{\binom{d}{e}} = \frac{\lfloor \frac{n-d}{e+1} \rfloor \binom{n}{e}}{\binom{d}{e}}$$

Αν χρησιμοποιήσουμε τα φράγματα που υπολογίσαμε για τα m, a_d, η παράμετρος s γίνεται:

$$\begin{aligned}
s \geq\ & 1 + \binom{n}{1}(q-1) + \ldots + \binom{n}{e}(q-1)^e \\
& + \left\lfloor \frac{n}{e+1} \right\rfloor \left(\binom{n}{e+1}(q-1)^{e+1} - \left\lfloor \frac{n-d}{e+1} \right\rfloor \binom{n}{e} \right)
\end{aligned} \tag{3.12}$$

Επανερχόμαστε στον αρχικό κώδικα C με παραμέτρους $[n, 2^t - 2t - 1, 5]$. Από την απόσταση $d = 5$ συνεπάγεται ότι $e = 2$. Επίσης, $a = (n-3)/3$, $b = 1$, $a_5 \leq n(n-1)(n-6)/60$ και $m \leq n/3$. Αν το t είναι περιττός, αντικαθιστώντας αυτές τις τιμές στην παραπάνω ανίσωση έχουμε:

$$s \geq 1 + n + \frac{1}{2}n(n-1) + 2(n-1) = 2^{2t-1} + 2^{t-1} - 4 > 2^{2t-1}$$

Σύμφωνα με το φράγμα του Johnson πρέπει

$$2^{2^t-2t-1} \leq \frac{2^{2^t-2}}{s}$$

όμως

$$\frac{2^{2t-2}}{s} < 2^{2^t-2}2^{2t-1} = 2^{2^t-2t-1}$$

Άρα δεν υπάρχει κώδικας C με παραμέτρους $[n, 2^t-2t-1, 5]$ και t περιττό.

Περίπτωση 2^η: α άρτιος

Προσθέτοντας τις a λέξεις με την ιδιότητα να μοιράζονται e συνιστώσες, προκύπτει λέξη βάρους $a(e+1) = n-b-e$, η οποία δεν έχει την παραπάνω ιδιότητα. Αυτό μπορεί να συμβεί το πολύ $a_{n-b-e}\binom{b+e}{e}$ φορές, όπου a_{n-b-e} ο μέσος όρος των λέξεων βάρους $n-b-e$. Επιπλέον, τα υπόλοιπα σύνολα που περιέχουν λέξεις οι οποίες μοιράζονται e συνιστώσες, αποτελούνται από το πολύ $a-1$ λέξεις βάρους d.

Συνολικά έχουμε

$$\begin{pmatrix} d \\ e \end{pmatrix} a_d \leq (a-1)\begin{pmatrix} n \\ e \end{pmatrix} + a_{n-b-e}\begin{pmatrix} b+e \\ e \end{pmatrix}$$

Επίσης, για το a_{n-b-e} ισχύει

$$a_{n-b-e} \leq A_2(n,d,n-b-e) = A_2(n,d,b+e) = A(n,2d,b+e) \leq \frac{\binom{n}{b}}{\binom{b+e}{b}}$$

όπου η τελευταία ανίσωση ισχύει λόγω της Πρότασης 3.6.1.

Ας επανέλθουμε στον κώδικα με παραμέτρους $[2^t-2, 2^t-2t-1, 5]$ και t άρτιο. Τότε $e=2$, $a=(n-2)/3$, $b=0$, $a_{n-2} \leq 1$, $10a_5 \leq n(n-1)(n-5)/6$ και $m \leq (n-2)/3$. Αν αντικαταστήσουμε αυτές τις παραμέτρους στην ανίσωση (3.12), υπολογίζουμε το s :

$$s \geq 1+n+\frac{1}{2}n(n-1)+\frac{3}{2}(n+1) = 2^{2t-1}+\frac{1}{2} > 2^{2t-1}$$

Όπως και στην περίπτωση όπου το a είναι περιττός, έτσι κι εδώ η παραπάνω ανίσωση του s δεν συμφωνεί με το φράγμα του Johnson. Σε κάθε περίπτωση ο κώδικας C με παραμέτρους $[2^t-2, 2^t-2t-1, 5]$ δεν υπάρχει. ■

Ορισμός 3.6.2 *Έστω $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. Αν $n = 2^m - 1$, τότε ορίζουμε C_f να είναι ο $[n, k, d]$ γραμμικός κώδικας, του οποίου ο δυϊκός κώδικας παράγεται από τις γραμμές του πίνακα*

$$H_f = \begin{bmatrix} 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ f(1) & f(\omega) & f(\omega^2) & \dots & f(\omega^{n-1}) \end{bmatrix}$$

όπου ω είναι μία πρωταρχική ρίζα του $\mathbb{F}_{2^m}^*$ και τα στοιχεία ω^i, $f(\omega^i)$ του $\mathbb{F}_{2^m}$ τα βλέπουμε ως διανύσματα του $\mathbb{F}_2^m$ (βλ. §2.3).

Θεώρημα 3.6.2 *Έστω $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ με $f(0) = 0$ και C_f ο κώδικας όπως ορίζεται στον παραπάνω ορισμό. Τότε:*

(i) ο κώδικας C_f έχει ελάχιστη απόσταση $3 \leq d \leq 5$

(ii) η f είναι APN αν και μόνο αν $d = 5$.

(iii) αν η f είναι APN, τότε η διάσταση του C_f είναι $k = 2^m - 1 - 2m$

Απόδειξη

(i) Σύμφωνα με τα παραπάνω ο H_f έχει $2m$ το πλήθος γραμμές, άρα ισχύει

$$n - k \leq 2m \Rightarrow k \geq n - 2m \Rightarrow k \geq 2^m - 2m - 1$$

Επίσης παρατηρούμε ότι οι στήλες του H_f είναι όλες διαφορετικές μεταξύ τους, διότι τα διανύσματα που αντιστοιχούν στα ω^j, $i = 0, \dots, n-1$, είναι όλα τα στοιχεία του $\mathbb{F}_2^m$. Άρα οποιεσδήποτε δύο στήλες είναι γραμμικώς ανεξέρτητες, δηλαδή η ελάχιστη απόσταση του C_f, με παραμέτρους $[2^m - 1, k, d]$, $k \geq 2^m - 2m - 1$, είναι $d \geq 3$. Υποθέτουμε ότι $d \geq 6$. Από την θεωρία κωδικοποίησης η ύπαρξη κώδικα με παραμέτρους $[n, k, d]$, συνεπάγεται την ύπαρξη ενός $[n-r, k, d-r]$ ([9] Θεώρημα 6.1.1 (iii)). Άρα από τον κώδικα $[2^m - 1, k, 6]$ προκύπτει ο $[2^m - 2, k, 5]$, με $k \geq 2^m - 2m - 1$. Όμως σύμφωνα με το Θεώρημα 3.6.1 δεν υπάρχει κώδικας με αυτές τις παραμέτρους. Επαγωγικα, χρησιμοποιώντας το (iv) του Θεωρήματος 6.1.1 από το [9], κατασκευάζουμε κώδικες παραμέτρων $[2^m - 1, k, d]$, με $k \geq 2^m - 2m - 1$, $d \geq 7$, οι οποίοι σύμφωνα με το Θεώρημα 3.6.1 δεν υπάρχουν. Επομένως η ελάχιστη απόσταση του κώδικα C_f με μήκος $2^m - 1$ και διάσταση $k \geq 2^m - 2m - 1$, είναι $d \leq 5$.

(ii) Έστω $c = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_2$. Τότε το c είναι στοιχείο του C_f αν και μόνο αν ικανοποιεί την

$$cH_f^T = 0 \quad \Rightarrow \quad \begin{cases} \sum_{i=0}^{n-1} c_i \omega^i = 0 \\ \\ \sum_{i=0}^{n-1} c_i f(\omega^i) = 0 \end{cases}$$

Αν υπάρχουν τέσσερα στοιχεία $x, y, x', y' \in \mathbb{F}_{2^m}$ διαφορετικά μεταξύ τους τέτοια ώστε $x + y + x' + y' = 0$ και $f(x) + f(y) + f(x') + f(y') = 0$ τότε ο κώδικας C_f έχει ελάχιστη απόσταση $d = 4$, ενώ αν κάποιο από τα στοιχεία είναι μηδέν, η απόσταση είναι 3. Σε αυτή την περίπτωση, σύμφωνα με την πρόταση (2.2.2), η συνάρτηση f δεν είναι APN. Επομένως, η f είναι APN αν και μόνο αν η απόσταση του κώδικα είναι $d \geq 5$. Συνδυάζοντας αυτό το αποτέλεσμα με το (i) προκύπτει ότι $d = 5$.

(iii) Έστω f μια συνάρτηση APN. Τότε σύμφωνα με τα παραπάνω, ο αντίστοιχος κώδικας C_f έχει παραμέτρους $[2^m - 1, k, 5]$. Σύμφωνα με το Θεώρημα 3.2.1 $dim(C^{\perp}) = n - k$. Το πλήθος των γραμμών του H_f είναι $2m$. Επειδή γενικά δεν γνωρίζουμε αν οι γραμμές του H_f είναι γραμμικώς ανεξάρτητες, ισχύει

$$n - k \leq 2m \Rightarrow k \geq 2^m - 1 - 2m$$

Έστω $k = 2^m - 2m$, τότε ο C_f είναι ένας $[2^m - 1, 2^m - 2m, 5]$ κώδικας, ο οποίος σύμφωνα με το Θεώρημα 3.6.1 δεν υπάρχει. Άρα η διάσταση του κώδικα είναι $k = 2^m - 2m - 1$. ■

Συνοψίζοντας, αν μία συνάρτηση f είναι APN, τότε ο αντίστοιχος κώδικας C_f έχει παραμέτρους $[2^m - 1, 2^m - 1 - 2m, 5]$, ενώ ο επεκτεταμένος κώδικας $\widetilde{C}_f$, $[2^m, 2^m - 1 - 2m, 6]$.

Ορισμός 3.6.3 *Έστω $F = \mathbb{F}_{q^m}$ πεπερασμένη επέκταση του $K = \mathbb{F}_q$ και $\alpha \in F$, τότε το ίχνος $Tr(\alpha)$ ορίζεται να είναι*

$$Tr(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$

Θεώρημα 3.6.3 *Έστω $K = \mathbb{F}_q$ και $F = \mathbb{F}_{q^m}$. Τότε*

(i) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta), \quad \forall \alpha, \beta \in F$

(ii) $Tr(c\alpha) = cTr(\alpha), \quad \forall c \in K, \alpha \in F$

(iii) *αν θεωρήσουμε ως K-διανυσματικούς χώρους τα F, K τότε το ίχνος $Tr(\alpha)$ είναι γραμμική απεικόνιση από το F επί του K*

(iv) $Tr(\alpha^q) = Tr(\alpha), \quad \forall \alpha \in F$

(v) *αν $\alpha \in F$, τότε $Tr(\alpha) = 0$ αν και μόνο αν $\alpha = \beta^q - \beta$ για κάποιο $\beta \in F$.*

Απόδειξη

(i) Για $\alpha, \beta \in F$ έχουμε

$$\begin{aligned} Tr(\alpha+\beta) &= (\alpha+\beta)+(\alpha+\beta)^q+\ldots+(\alpha+\beta)^{q^{m-1}} \\ &= \alpha+\beta+\alpha^q+\beta^q+\ldots+\alpha^{q^{m-1}}+\beta^{q^{m-1}} \\ &= Tr(\alpha)+Tr(\beta) \end{aligned}$$

(ii) Αν $c \in K$ τότε $c^{q^j} = c$, $\forall j \geq 0$. Συνεπώς, για $\alpha \in F$

$$\begin{aligned} Tr(c\,\alpha) &= c\,\alpha + c^q\,\alpha^q + \ldots + c^{q^{m-1}}\,\alpha^{q^{m-1}} \\ &= c\,\alpha + c\,\alpha^q + \ldots + c\,\alpha^{q^{m-1}} \\ &= c\,Tr(\alpha) \end{aligned}$$

(iii) Από τα $(i), (ii)$ και το γεγονός ότι $Tr(\alpha) \in K$ συνεπάγεται ότι το ίχνος Tr είναι γραμμική απεικόνιση από το F στο K. Απομένει να δείξουμε ότι η απεικόνιση είναι επί του K, δηλαδή την ύπαρξη ενός στοιχείου $\alpha \in F$, για το οποίο $Tr(\alpha) \neq 0$. Έστω $Tr(\alpha) = 0$, τότε το α είναι ρίζα του πολυωνύμου $x^{q^{m-1}}+\ldots+x^q+x \in K[x]$ στο F, το οποίο μπορεί να έχει το πολύ q^{m-1} το πλήθος ρίζες στο F. Όμως, το F έχει q^m στοιχεία, άρα υπάρχει στοιχείο $\alpha \in F$ τέτοιο ώστε $Tr(\alpha) \neq 0$.

(iv) Για $\alpha \in F$ έχουμε $\alpha^{q^m} = \alpha$, συνεπώς

$$Tr(\alpha^q) = \alpha^q + \alpha^{g^2} + \ldots + \alpha^{q^m} = Tr(\alpha)$$

(v) $(\Rightarrow)$

Υποθέτουμε ότι $Tr(\alpha) = 0$ για $\alpha \in F$. Έστω β μια ρίζα του πολυωνύμου $x^q = x - \alpha$ σε κάποια επέκταση του F. Τότε $\alpha = \beta^q - \beta$ και

$$\begin{aligned} 0 &= Tr(\alpha) \\ &= \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}} \\ &= (\beta^q - \beta) + (\beta^{2q} - \beta^q) + \ldots + (\beta^{q^m} - \beta^{q^{m-1}}) \\ &= \beta^{q^m} - \beta \end{aligned}$$

δηλαδή $\beta \in F$.

$(\Leftarrow)$

Έστω $\alpha = \beta^q - \beta$ με $\alpha, \beta \in F$. Τότε από το (iv) έχουμε

$$Tr(\alpha) = Tr(\beta^q - \beta) = Tr(\beta^q) - Tr(\beta) \overset{\beta \in F}{=} Tr(\beta) - Tr(\beta) = 0 \qquad \blacksquare$$

Θεώρημα 3.6.4 *Έστω $F = \mathbb{F}_{q^m}$ πεπερασμένη επέκταση του $K = \mathbb{F}_q$. Αν θεωρήσουμε ως διανυσματικούς χώρους τα F, K, τότε οι γραμμικές απεικονίσεις από το F στο K είναι ακριβώς οι απεικονίσεις L_β, $\beta \in F$, όπου $L_\beta(\alpha) = Tr(\beta\alpha)$ για κάθε $\alpha \in F$. Επιπλέον, $L_\beta \neq L_\gamma$ για διαφορετικά $\beta, \gamma \in F$.*

Απόδειξη

Σύμφωνα με το (iii) του προηγούμενου Θεωρήματος, κάθε απεικόνιση L_β είναι γραμμικός μετασχηματισμός από το F στο K. Για $\beta \neq \gamma$ έχουμε:

$$L_\beta(\alpha) - L_\gamma(\alpha) = Tr(\beta\alpha) - Tr(\gamma\alpha) = Tr((\beta - \gamma)\alpha) \neq 0$$

για κατάλληλο $\alpha \in F$. Άρα για διαφορετικά β, γ οι αντίστοιχοι μετασχηματισμοί L_β, L_γ είναι επίσης διαφορετικοί.

Αν $F = \mathbb{F}_{q^m}, K = \mathbb{F}_q$, τότε σύμφωνα με τα παραπάνω υπάρχουν q^m διαφορετικοί μετασχηματισμοί από το F στο K. Επίσης, κάθε γραμμικός μετασχηματισμός μπορεί να δημιουργηθεί αντιστοιχίζοντας αυθαίρετα στοιχεία του K, σε m στοιχεία δοσμένης βάσης του F. Αυτό μπορεί να πραγματοποιηθεί με q^m διαφορετικούς τρόπους, επομένως οι απεικονίσεις L_β είναι όλοι οι γραμμικοί μετασχηματισμοί από το F στο K.

■

Λήμμα 3.6.1 *Αν $\mathcal{L}$ είναι μία γραμμική απεικόνιση από το $\mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ στον εαυτό της, τότε η $\mathcal{L}$ έχει τη μορφή*

$$\mathcal{L}(z, x, y) = (bz + Tr(\alpha x) + Tr(\beta y), L_1(x, y) + c_1 z, L_2(x, y) + c_2 z)$$

για κάποια $\alpha, \beta, c_1, c_2 \in \mathbb{F}_{2^m}$ και $b \in \mathbb{F}_2$.

Απόδειξη

Για την απόδειξη του Λήμματος αρκεί να μελετήσουμε τις προβολές της $\mathcal{L}$ σε καθέναν από τους χώρους $\mathbb{F}_2, \mathbb{F}_{2^m}$.

Αρχικά, γράφουμε το διάνυσμα (z, x, y) στη μορφή:

$$(z, x, y) = (z, 0, 0) + (0, x, y) = (z, 0, 0) + (0, x, 0) + (0, 0, y)$$

- προβολή στο $\mathbb{F}_2$: $\mathcal{L}_1 : \mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$

$$\begin{aligned} \mathcal{L}_1(z, x, y) &= \mathcal{L}_1(z, 0, 0) + \mathcal{L}_1(0, x, 0) + \mathcal{L}_1(0, 0, y) \\ &\overset{z \in \mathbb{F}_2}{=} z\mathcal{L}_1(1, 0, 0) + L_1(x) + L_2(y) \\ &= bz + Tr(\alpha x) + Tr(\beta y) \end{aligned}$$

με $b \in \mathbb{F}_2$, $\alpha, \beta \in \mathbb{F}_{2^m}$. Η τελευταία ισότητα προκύπτει άμεσα απο Θεώρημα 3.6.4 για $F = \mathbb{F}_{2^m}$ και $K = \mathbb{F}_2$.

- προβολή στο $\mathbb{F}_{2^m}$: $\mathcal{L}_2 : \mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$

$$\begin{aligned} \mathcal{L}_2(z,x,y) &= \mathcal{L}_2(z,0,0) + \mathcal{L}_2(0,x,y) \\ &\overset{z\in\mathbb{F}_2}{=} z\mathcal{L}_2(1,0,0) + L(x,y) \\ &= cz + L(x,y) \end{aligned}$$

όπου $c \in \mathbb{F}_{2^m}$ και $L : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ γραμμική απεικόνιση.

Τελικά, η $\mathcal{L}$ έχει τη μορφή:

$$\begin{aligned} \mathcal{L}(z,x,y) &= (\mathcal{L}_1(z,x,y),\, \mathcal{L}_2(z,x,y),\, \mathcal{L}_2(z,x,y)) \\ &= (bz + Tr(\alpha x) + Tr(\beta y),\, L_1(x,y) + c_1 z,\, L_2(x,y) + c_2 z) \end{aligned}$$

για κάποια $\alpha, \beta, c_1, c_2 \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_2$ και L_1, L_2 γραμμικές απεικονίσεις από το $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ στο $\mathbb{F}_{2^m}$. ■

Θεώρημα 3.6.5 *Έστω $f, g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ συναρτήσεις APN.*

1. *Αν $f(0) = 0$ και $g(0) = 0$, τότε οι κώδικες C_f, C_g είναι ισοδύναμοι αν και μόνο αν υπάρχει αντιστρέψιμη γραμμική απεικόνιση $\mathcal{L} : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ τέτοια ώστε $\Gamma_g = \mathcal{L}(\Gamma_f)$*

2. *Η f είναι CCZ ισοδύναμη με την g αν και μόνο αν οι επεκταμένοι κώδικες $\widetilde{C}_f, \widetilde{C}_g$ είναι ισοδύναμοι.*

Απόδειξη

1. Έστω f, g APN συναρτήσεις με $f(0) = 0$, $g(0) = 0$, οι οποίες αντιστοιχούν στους κώδικες C_f, C_g. Τότε

$$C_f \sim C_g \Leftrightarrow C_f^{\perp} \sim C_g^{\perp}$$

το οποίο ισχύει αν και μόνο αν υπάρχει αντιστρέψιμη γραμμική απεικόνιση $\mathcal{L}$ που αντιστοιχίζει τις στήλες του H_f στις στήλες του H_g. Όμως οι στήλες του H_f είναι ακριβώς τα μη μηδενικά στοιχεία του συνόλου $\{(x, f(x)) : x \in \mathbb{F}_{2^m}\}$, το οποίο είναι το γράφημα Γ_f, της f. Επίσης, $\mathcal{L}(0,0) = (0,0)$ επομένως ισχύει $\Gamma_g = \mathcal{L}(\Gamma_f)$.

2. ($\Rightarrow$) Υποθέτουμε ότι οι f, g είναι CCZ ισοδύναμες και θα δείξουμε ότι $C_f^{\perp} \sim C_g^{\perp}$.

Κάθε αφινική απεικόνιση από το $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ στον εαυτό της είναι της μορφής:

$$\mathcal{A}(x, y) = (L_1(x, y) + c_1, L_2(x, y) + c_2) \tag{3.13}$$

όπου L_1, L_2 γραμμικές και $c_1, c_2 \in \mathbb{F}_{2^m}$. Η συνάρτηση f είναι APN, συνεπώς ο επεκτεταμένος κώδικας $\widetilde{C}_f$ έχει πίνακα ελέγχου

$$\widetilde{H}_f = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \mathbf{0} & 1 & \dots & \omega^{2^m-2} \\ \mathbf{0} & f(1) & \dots & f(\omega^{2^m-2}) \end{bmatrix}$$

Οι στήλες του $\widetilde{H}_f$ είναι ακριβώς τα σημεία του χώρου $\mathcal{P} = \mathbb{F}_2 \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Ας ονομάσουμε το σύνολο αυτών των σημείων $\widetilde{\Gamma}_f$, δηλαδή

$$\widetilde{\Gamma}_f = \{(1, x, f(x)) : x \in \mathbb{F}_{2^m}\}$$

Εξ υποθέσεως οι APN συναρτήσεις f, g είναι CCZ ισοδύναμες, επομένως $\Gamma_g = \mathcal{A}(\Gamma_f)$ για κάποια αντιστρέψιμη αφινική απεικόνιση $\mathcal{A}$, που δίνεται από την (3.13). Αντίστοιχα, στον χώρο $\mathcal{P}$ θα έχουμε $\widetilde{\Gamma}_g = \mathcal{T}(\widetilde{\Gamma}_f)$, με $\mathcal{T}$ τη γραμμική απεικόνιση

$$\mathcal{T}(z, x, y) = (z, L_1(x, y) + c_1 z, L_2(x, y) + c_2 z)$$

Για να είναι οι επεκτεταμένοι κώδικες $\widetilde{C}_f, \widetilde{C}_g$ είναι ισοδύναμοι, θα πρέπει σύμφωνα με την Πρόταση 3.5.1, η απεικόνιση $\mathcal{T}$ να είναι αντιστρέψιμη.

Έστω $x_1, y_1, x_2, y_2 \in \mathbb{F}_{2^m}$ και $z \in \mathbb{F}_2$, με $\mathcal{T}(z, x_1, y_1) = \mathcal{T}(z, x_2, y_2)$.

- αν $z = 0$, τότε

$$\begin{aligned} \mathcal{T}(z, x_1, y_1) = \mathcal{T}(z, x_2, y_2) \quad &\Rightarrow \quad \begin{cases} L_1(x_1, y_1) + c_1 0 = L_1(x_2, y_2) + c_1 0 \\ L_2(x_1, y_1) + c_2 0 = L_2(x_2, y_2) + c_2 0 \end{cases} \\ &\Rightarrow \quad \begin{cases} L_1(x_1, y_1) = L_1(x_2, y_2) \\ L_2(x_1, y_1) = L_2(x_2, y_2) \end{cases} \\ &\Rightarrow \quad \begin{cases} x_1 = x_2 \\ y_1 = y_2 \end{cases} \end{aligned}$$

- αν $z = 1$, τότε

$$\mathcal{T}(z, x_1, y_1) = \mathcal{T}(z, x_2, y_2) \Rightarrow \begin{cases} L_1(x_1, y_1) + c_1 = L_1(x_2, y_2) + c_1 \\ L_2(x_1, y_1) + c_2 = L_2(x_2, y_2) + c_2 \end{cases}$$

$$\Rightarrow \begin{cases} L_1(x_1, y_1) = L_1(x_2, y_2) \\ L_2(x_1, y_1) = L_2(x_2, y_2) \end{cases}$$

$$\Rightarrow \begin{cases} x_1 = x_2 \\ y_1 = y_2 \end{cases}$$

Δηλαδή η $\mathcal{T}$ είναι "$1-1$" και επειδή το πεδίο ορισμού ταυτίζεται με το σύνολο τιμών, είναι και επί. Άρα η $\mathcal{T}$ είναι μια αντιστρέψιμη γραμμική απεικόνιση.

($\Leftarrow$) Αντιστρόφως, υποθέτουμε ότι οι κώδικες $\widetilde{C}_f, \widetilde{C}_g$ είναι ισοδύναμοι. Τότε, υπάρχει αντιστρέψιμη γραμμική απεικόνιση $\mathcal{L}$ του χώρου $\mathcal{P}$, τέτοια ώστε $\widetilde{\Gamma}_g = \mathcal{L}(\widetilde{\Gamma}_f)$, η οποία σύμφωνα με το Λήμμα 3.6.1 έχει τη μορφή:

$$\mathcal{L}(z, x, y) = (bz + Tr(\alpha x) + Tr(\beta y),\ L_1(x, y) + c_1 z,\ L_2(x, y) + c_2 z)$$

με $b \in \mathbb{F}_2$ και $\alpha, \beta, c_1, c_2 \in \mathbb{F}_{2^m}$.

$$\begin{aligned} \widetilde{\Gamma}_g &= \{\mathcal{L}(1, x, f(x)) : x \in \mathbb{F}_{2^m}\} \\ &= \{(b + Tr(\alpha x) + Tr(\beta f(x)),\ L_1(x, f(x)) + c_1,\ L_2(x, f(x)) + c_2) : x \in \mathbb{F}_{2^m}\} \end{aligned}$$

δηλαδή

$$b + Tr(\alpha x) + Tr(\beta f(x)) = 1 \Rightarrow Tr(\alpha x + \beta f(x)) = 1 - b, \quad \forall x \in \mathbb{F}_{2^m} \quad (3.14)$$

Η συνάρτηση f είναι APN, συνεπώς ο κώδικας C_f έχει ελάχιστη απόσταση $d = 5$. Αυτό σημαίνει ότι υπάρχουν 5 γραμμικώς εξαρτημένες στήλες

$$\begin{pmatrix} x_1 \\ f(x_1) \end{pmatrix}, \ldots, \begin{pmatrix} x_5 \\ f(x_5) \end{pmatrix}$$

για τις οποίες ισχύει

$$\sum_{i=1}^{5} \begin{pmatrix} x_i \\ f(x_i) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \sum_{i=1}^{5} x_i = 0 \,\kappa\alpha\iota \sum_{i=1}^{5} f(x_i) = 0$$

Έχουμε

$$\begin{aligned} 0 &= Tr(\alpha \sum_{i=1}^{5} x_i + \beta \sum_{i=1}^{5} f(x_i)) \\ &= \sum_{i=1}^{5} Tr(\alpha x_i + \beta f(x_i)) \\ &\overset{(3.14)}{=} 5(1-b) \\ &= 1-b \end{aligned}$$

δηλαδή $b = 1$. Επομένως, για κάθε $x \in \mathbb{F}_{2^m}$ $Tr(\alpha x + \beta f(x)) = 0$. Επίσης, από το γεγονός ότι η f είναι APN συνεπάγεται ότι ο C_f έχει παραμέτρους $[2^m - 1, 2^m - 1 - 2m, 5]$ και από το Θεώρημα 3.2.1 έχουμε:

$$dim(C_f) + dim(C_f^{\perp}) = 2^m - 1 \quad \Rightarrow \quad dim(C_f^{\perp}) = 2m$$

Συνεπώς,

$$Span\left\{ \begin{pmatrix} x \\ f(x) \end{pmatrix} : x \in \mathbb{F}_{2^m} \right\} = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$$

άρα

$$\forall (x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \quad (x,y) = \sum_{i=1}^{2m} \lambda_i (x_i, f(x_i))$$

Χρησιμοποιώντας την παραπάνω σχέση παίρνουμε

$$\begin{aligned} Tr(\alpha x + \beta y) &= Tr(\alpha \sum_{i=1}^{2m} \lambda_i x_i + \beta \sum_{i-1}^{2m} \lambda_i f(x_i)) \\ &= \sum_{i=1}^{2m} \lambda_i Tr(\alpha x_i + \beta f(x_i)) \\ &= 0 \end{aligned}$$

Το παραπάνω αποτέλεσμα ισχύει για κάθε x, y στο $\mathbb{F}_{2^m}$, επομένως από το Θεώρημα 3.6.3 και θέτοντας $y = 0$, παίρνουμε

$$Tr(\alpha x) = \alpha x + \alpha^2 x^2 + \ldots + \alpha^{2^{m-1}} x^{2^{m-1}} = 0, \quad \forall x \in \mathbb{F}_{2^m}$$

Άρα πρέπει $\alpha = 0$. Όμοια, για $x = 0$ έχουμε $\beta = 0$.

Τελικά,

$$\{(1, x, g(x)) : x \in \mathbb{F}_{2^m}\} = \{(1, L_1(x, f(x)) + c_1, L_2(x, f(x)) + c_2\}$$

δηλαδή υπάρχει αντιστρέψιμη αφινική απεικόνιση $\mathcal{A}$ του $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, τέτοια ώστε $\Gamma_g = \mathcal{A}(\Gamma_f)$, που σημαίνει ότι οι συναρτήσεις f, g είναι CCZ ισοδύναμες.

■

3.7 Παραδείγματα

Στα παρακάτω παραδείγματα θα μελετηθούν συναρτήσεις πάνω από το σώμα $\mathbb{F}_{2^3} = \mathbb{F}_2/ < x^3 + x + 1 >$. Αν ω είναι μια πρωταρχική ρίζα του $\mathbb{F}_{2^3}^*$ και $f : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$ μια APN συνάρτηση, τότε μπορούμε να κατασκευάσουμε τον πίνακα ελέγχου

$$\widetilde{H}_f = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 0 & f(1) & f(\omega) & f(\omega^2) & \dots & f(\omega^{n-1}) \end{bmatrix}$$

Παράδειγμα 3.7.1 Έστω η APN συνάρτηση $f(x) = x^3$ πάνω από το $\mathbb{F}_{2^3}$, η οποία αντιστοιχεί στον κώδικα $\widetilde{C}_f$ με πίνακα ελέγχου

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

Ας θεωρήσουμε επίσης την αντιστρέψιμη αφινική απεικόνιση

$$\begin{aligned} \mathcal{A} : \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} &\longrightarrow \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \\ (x, y) &\longmapsto (x, y + x) \end{aligned}$$

Έχουμε

$$\mathcal{A}(x, f(x)) = \mathcal{A}(x, x^3) = (x, x^3 + x) = (x, g(x))$$

δηλαδή η συνάρτηση $g(x) = x^3 + x$ είναι CCZ ισοδύναμη με την f, άρα είναι επίσης APN. Ο πίνακας ελέγχου του κώδικα $\widetilde{C}_g$ είναι ο:

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

Εκ κατασκευής, οι 4 πρώτες γραμμές των πινάκων ταυτίζονται, διότι είναι οι δυνάμεις ενός πρωταρχικού στοιχείου ω του $\mathbb{F}_{2^3}$. Παρατηρώντας τους δύο πίνακες βλέπουμε ότι

η 5^η γραμμή του $\widetilde{H}_g$ είναι το άθροισμα της $2^{\eta\varsigma}$ και της $5^{\eta\varsigma}$ γραμμής του $\widetilde{H}_f$. Επίσης, η 3^η και η 6^η του $\widetilde{H}_f$ αθροίζουν στην 6^η του $\widetilde{H}_g$, ενώ η 7^η του $\widetilde{H}_g$ προκύπτει από τις 4 και 7. Επομένως, ο πίνακας μετάθεσης που αντιστοιχίζει τις στήλες του $\widetilde{H}_g$ στις στήλες του $\widetilde{H}_f$ είναι ο

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

Η σχέση που συνδέει τους δύο πίνακες είναι η

$$\widetilde{H}_g = M\widetilde{H}_f$$

δηλαδή

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

Παράδειγμα 3.7.2 Θεωρούμε τη συνάρτηση $g(x) = x^5+1$ και την APN συνάρτηση $f(x) = x^5$. Επίσης, θεωρούμε την αφινική απεικόνιση

$$\begin{aligned} \mathcal{A} : \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} &\longrightarrow \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \\ (x, y) &\longmapsto (x, y + 1) \end{aligned}$$

Προφανώς ισχύει ότι $\mathcal{A}(\Gamma_f) = \Gamma_g$, διότι

$$\{\mathcal{A}(x, x^5) : x \in \mathbb{F}_{2^3}\} = \{(x, x^5 + 1) : x \in \mathbb{F}_{2^3}\}$$

Άρα, οι συναρτήσεις f, g είναι CCZ ισοδύναμες και επειδή η f είναι APN, σύμφωνα με το Πόρισμα 2.3.3 και g θα είναι APN.

Ας κατασκευάσουμε τους πίνακες ελέγχου των $\widetilde{C}_f, \widetilde{C}_g$:

$$\widetilde{H}_f = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad \widetilde{H}_g = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Σύμφωνα με το Θεώρημα 3.5.2 οι παραπάνω πίνακες είναι ισοδύναμοι με τους

$$[I_7|X_f] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad [I_7|X_g] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Εφόσον οι f, g είναι CCZ ισοδύναμες, συνεπάγεται ότι και οι πίνακες $\widetilde{H}_f, \widetilde{H}_g$ είναι ισοδύναμοι και κατ'επέκταση, οι $[I_7|X_f]$, $[I_7|X_g]$ είναι ισοδύναμοι. Όμως, οι πίνακες X_f, X_g δεν είναι ισοδύναμοι:

$$X_f = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \neq \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = X_g$$

Το συμπέρασμα λοιπόν είναι ότι αν $[I_k|X_f]$, $[I_k|X_g]$ είναι οι κανονικές μορφές των πινάκων ελέγχου δύο γραμμικών κωδίκων $\widetilde{C}_f, \widetilde{C}_g$, οι οποίοι αντιστοιχούν στις APN συναρτήσεις f, g, τότε

- αν οι στήλες του X_f είναι μετάθεση των στηλών του X_g τότε οι f, g είναι CCZ ισοδύναμες, ενώ
- αν οι στήλες του X_f δεν είναι μετάθεση των στηλών του X_g, τότε δεν μπορούμε να καταλήξουμε σε κάποιο συμπέρασμα.

Παράδειγμα 3.7.3 Έστω οι APN συναρτήσεις $f(x) = x^3$ και $g(x) = x^5$. Με μια πρώτη ματιά οι f, g δεν φαίνεται να είναι CCZ ισοδύναμες. Κατασκευάζουμε τους αντίστοιχους πίνακες ελέγχου:

$$\widetilde{H}_f = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}, \quad \widetilde{H}_g = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

και τους μετατρέπουμε σε πίνακες κανονικής μορφής:

$$[I_7|X_f] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad [I_7|X_g] = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Παρατηρούμε ότι υποπίνακες X_f, X_g είναι ίδιοι, επομένως καταλήγουμε στο συμπέρασμα ότι οι f, g είναι CCZ ισοδύναμες.

Ένας εναλλακτικός τρόπος για να φτάσουμε στο ίδιο αποτέλεσμα είναι να βρούμε μια αφινική απεικόνιση $\mathcal{A}$, τέτοια ώστε $\mathcal{A}(\Gamma_f) = \Gamma_g$.

Από τον ενδομορφισμό F του Φροβενιυς και δεδομένου ότι βρισκόμαστε σε σώμα χαρακτηριστικής 2, ισχύει

$$\begin{aligned} F : \mathbb{F}_{2^3} &\to \mathbb{F}_{2^3} \\ x &\mapsto x^2 \end{aligned}$$

Επίσης παρατηρούμε ότι

$$\begin{cases} x^{10} = x^8 \cdot x^2 = x \cdot x^2 = x^3 \\ x^{10} = (x^5)^2 \end{cases} \quad \Rightarrow \quad x^3 = (x^5)^2$$

Άρα, αν θεωρήσουμε την απεικόνιση

$$\begin{aligned} \mathcal{A} : \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} &\longrightarrow \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \\ (x, y) &\longmapsto (x^2, y) \end{aligned}$$

τότε

$$\begin{aligned}\mathcal{A}(\Gamma_f) &= \{\mathcal{A}(x, x^3) : x \in \mathbb{F}_{2^3}\} \\ &= \{(x^2, x^3) : x \in \mathbb{F}_{2^3}\} \\ &= \{(x^2, x^{10}) : x \in \mathbb{F}_{2^3}\} \\ &= \{(x', x'^5) : x' \in \mathbb{F}_{2^3}\} \\ &= \Gamma_g\end{aligned}$$

δηλαδή, οι f, g είναι CCZ ισοδύναμες.

Βιβλιογραφία

[1] A. E. Brouwer and L.M.G.M. Tolhuizen, A Sharpening of the Johnson Bound for Binary Linear Codes, Designs, Codes and Cryptography, Vol. 3, No. 1 (1993) pp.95-98.

[2] K. A. Browning, J. F. Dillon, R. E. Kibler and M. T. McQuistan, *APN Polynomials and Related Codes*, preprint.

[3] Lilya Budaghyan, Claude Carlet, Patrick Felke and Gregor Leander, An infinite class of quadratic APN functions which are not equivalent to power mappings, preprint

[4] Lilya Budaghyan, The Equivalence of Almost Bent and Almost Perfect Nonlinear Functions and their Generalizations, dissertation, Otto-von-Guericke Universität Magdeburg, 2005.

[5] Claude Carlet, Pascale Charpin and Victor Zinoviev, Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems, Designs, Codes and Cryptography 15 (1998), pp. 125-156.

[6] Yves Edel, Gohar Kyureghyan and Alexander Pott, A new APN function which is not equivalent to a power mapping, preprint.

[7] T. Helleseth, C. Rong, D. Sandberg, New families of almost perfect nonlinear power mappings, IEEE Trans. Inform. Theory 45 (1999) 475-485.

[8] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications,* Vol. 20, Cambridge University Press, Cambridge (1983).

[9] San Ling, Chaoping Xing, Coding Theory, A First Course, Cambridge University Press, Cambridge (2004).

[10] K. Nyberg, Differentially uniform mappings for cryptology, Advances in Cryptology - EUROCRYPT93, LNCS (1994), Springer-Verlag, 55-64.

[11] Erik Agrell and Er Vardy and Kenneth Zeger, Upper bounds for constant-weight codes, IEEE Trans. Inform. Theory 46 (2000) 2373–2395.