ΠΟΛΥΩΝΥΜΑ ΜΕΤΑΘΕΣΗΣ ΠΑΝΩ ΑΠΟ ΠΕΠΕΡΑΣΜΕΝΑ ΣΩΜΑΤΑ

Ευλιάτης Αναστάσιος,
Τμήμα Μαθηματικών,
Επιβλέπων Καθηγητής: Γαρεφαλάκης Θεόδουλος,
Πανεπιστήμιο Κρήτης, Ηράκλειο,

2012

Πρόλογος

Ο στόχος αυτής της εργασίας είναι η ανάλυση κυρίων αποτελεσμάτων για πολυωνυμικές συναρτήσεις από ένα πεπερασμένο σώμα στον εαυτό του. Στίς ακόλουθες σελίδες, αναπτύσουμε μια εισαγωγή στα πολυώνυμα μετάθεσης. Έτσι, καλούνται τα πολυώνυμα που απεικονίζουν το σωμα στον εαυτό του. Συγκεκριμένα η δομή της εργασίας είναι η ακόλουθη:

- Στο κεφάλαιο 1, δίνουμε απαντήσεις στο πότε ένα πολυώνυμο αποτελεί πολυώνυμο μετάθεσης πάνω απο κάποιο πεπερασμένο σώμα.
- Στο κεφάλαιο 2, παρουσιάζουμε αποτελέσματα που σχετίζοντα με ειδικές περιπτώσεις τέτοιου είδους πολυωνύμων.
- Στο κεφάλαιο 3, μελετάμε τις εργασίες των Wan-Lidl και Amir Akbary-Qiang Wang που αναφέρονται σε πολυώνυμα της μορφής $\mathrm{x^r f(x^{(q-1)/l})}$.
- Στο κεφάλαιο 4, παρουσιάζουμε μία διεξοδίκη αρίθμηση πολυωνύμων βαθμού $q-2$ πάνω από το $\mathbb{F}_q$ που οφείλεται σε εργασία των Konyagin-Papalardi.

Στα δύο πρώτα κεφάλαια ακολουθούμε το βιβλίο [1].

Ευχαριστίες

Πρώτα απ'όλα, θέλω να ευχαριστήσω τον καθηγητή μου Γαρεφαλάκη Θεόδουλο για την αφοσίωση του και τις χρήσιμες υποδείξεις του που οδήγησαν στην επιτυχημένη έκβαση αυτής της εργασίας.
Αυτή η εργασία είναι αφιερωμένη στην οικογένεια μου, που με στηρίζει και με ενθαρύνει σε οποιαδήποτε επιλογή της ζωής μου.
Επίσης, θα ήταν μεγάλη μου παράβλεψη αν σε αυτό το σημείο δεν ευχαριστούσα τους Χρήστο, Γιώργο και Σάκη που με βοήθησαν στην εργασία.
Τέλος, θέλω να ευχαριστήσω τους φίλους μου για τις πολύ όμορφες στιγμές που περάσαμε μαζί κατά τη διάρκεια των σπουδών μου.

Κεφάλαιο 1

ΚΡΙΤΗΡΙΑ ΓΙΑ ΠΟΛΥΩΝΥΜΑ ΜΕΤΑΘΕΣΗΣ

1.1 Βασικά Κριτήρια

Έστω $\mathbb{F}_q$ ένα πεπερασμένο σώμα με q στοιχεία όπου $q = p^m$ με p πρώτο αριθμό και $m \in \mathbb{N}$. Ένα πολυώνυμο $f \in \mathbb{F}_q[x]$ καλείται πολυώνυμο μετάθεσης στο $\mathbb{F}_q$ αν η πολυωνυμική συνάρτηση

$$f : \mathbb{F}_q \longrightarrow \mathbb{F}_q,$$

είναι μετάθεση του $\mathbb{F}_q$. Προφανώς, αν το f είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$, τότε η εξίσωση $f(x) = a$ έχει ακριβώς μία λύση στο $\mathbb{F}_q$ για κάθε $a \in \mathbb{F}_q$. Επειδή το $\mathbb{F}_q$ είναι πεπερασμένο, ο ορισμός του πολυωνύμου μετάθεσης μπορεί να εκφραστεί με διάφορους τρόπους. Χρήσιμο θα ειναι για την συνέχεια το επόμενο λήμμα που η απόδειξη του ειναι προφανής.

Λήμμα 1.1.1. *Το πολυώνυμο $f \in \mathbb{F}_q[x]$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μόνο αν ισχύουν τα ακολουθα:*

(i) η συνάρτηση $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ είναι επί,

(ii) η συνάρτηση $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ είναι ένα-προς-ένα,

(iii) η εξίσωση $f(x) = a$ έχει λύση στο $\mathbb{F}_q$ για κάθε $a \in \mathbb{F}_q$,

(iv) η εξίσωση $f(x) = a$ έχει μια μοναδική λύση στο $\mathbb{F}_q$ για κάθε $a \in \mathbb{F}_q$.

Αν $\phi : \mathbb{F}_q \to \mathbb{F}_q$ είναι αυθαίρετη συνάρτηση τότε υπάρχει μοναδικό πολυώνυμο $g \in \mathbb{F}_q[x]$ με $deg(g) < q$ που αντιπροσωπεύει την ϕ, δηλαδή τέτοιο ώστε $g(c) = \phi(c)$ για όλα $c \in \mathbb{F}_q$. Το πολυώνυμο g προκύπτει άμεσα από το πολυώνυμο παρεμβολής Lagrange για τη δοσμένη συνάρτηση ϕ και συγκεκριμένα δίνεται από:

$$g(x) = \sum_{c \in \mathbb{F}_q} \phi(c)(1 - (x-c)^{q-1}).$$

Άν η f είναι ένα πολυώνυμο, ας πούμε ότι η f απεικονίζει το c στο $f(c) \in \mathbb{F}_q$, τότε η g μπορεί να προκύψει από την f με αναγωγή $\mod (x^q - x)$, σύμφωνα με το ακόλουθο λήμμα:

Λήμμμα 1.1.2. *Για $f, g \in \mathbb{F}_q[x]$, έχουμε*

$$f(c) = g(c) \ \ \forall c \in \mathbb{F}_q \iff f(x) \equiv g(x) \mod (x^q - x), \ \forall x \in \mathbb{F}_q.$$

Απόδειξη. Η Ευκλείδεια διαίρεση του $f(x) - g(x)$ με το $x^q - x$ οδηγεί στην εξίσωση $f(x) - g(x) = h(x)(x^q - x) + r(x)$ με $h, r \in \mathbb{F}_q[x]$ και $deg(r) < q$. Για $x = c \in \mathbb{F}_q$, έχουμε $f(c) - g(c) = h(c)(c^q - c) + r(c)$, όμως αφού $c^q = c$ για όλα τα $c \in \mathbb{F}_q$ συμπεραίνουμε ότι $f(c) = g(c)$ αν και μόνο αν $r(c) = 0$ για όλα τα $c \in \mathbb{F}_q$. Η τελευταία συνθήκη είναι ισοδύναμη με το ότι $r = 0$ δηλαδή $f(x) \equiv g(x) \mod (x^q - x)$. □

Επίσης χρήσιμο για την συνέχεια είναι το επόμενο λήμμα.

Λήμμμα 1.1.3. *Έστω $a_0, a_1, ..., a_{q-1}$ στοιχεία του $\mathbb{F}_q$. Τότε, τα στοιχεία $a_0, a_1, ..., a_{q-1}$ είναι διακριτά αν και μόνο αν*

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{για } t = 0, 1, ..., q-2 \\ -1 & \text{για } t = q-1 \end{cases} \tag{1.1}$$

Απόδειξη. Για σταθερό i με $0 \leq i \leq q-1$, θεωρούμε το πολυώνυμο

$$g_i(x) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} x^j.$$

Υπολογίζουμε,

$$g_i(a_i) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} a^j = 1 - \sum_{j=0}^{q-1} a_i^{q-1} = 1,$$

ενώ, για $b \in \mathbb{F}_q$ και $b \neq a_i$, έχουμε

$$g_i(b) = 1 - \sum_{j=0}^{q-1} a_i^{q-1-j} b^j = 1 - a_i^{q-1} \sum_{j=0}^{q-1} \frac{b^j}{a_i^j} = 0, \ \text{ εφόσον } \ a_i \neq 0$$

Αν $a_i = 0$, τότε $g_i(x) = 1 - x^{q-1}$ και $g_i(b) = 0$, εφόσον $b \neq a_i$ Έτσι το πολυώνυμο

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = -\sum_{i=0}^{q-1} \Big(\sum_{j=0}^{q-1} a_i^{q-1-j} \Big) x^j,$$

αν $\{a_0, ..., a_{q-1}\} = \mathbb{F}_q$ απεικονίζει κάθε στοιχείο του $\mathbb{F}_q$ στο 1. Από τη στιγμή που $deg(g) < q$, από το αμέσως προηγούμενο λήμμα, παίρνουμε ότι το πολυώνυμο g απεικονίζει όλα τα στοιχεία του $\mathbb{F}_q$ στο 1 αν $g(x) = 1$, αφού η $f(x) = 1$ είναι συνάρτηση από το $\mathbb{F}_q$ στο 1 με $degf(x) < q$ και έχει την ιδιότητα $f(c) = g(c)$. Επομένως,

$$g(x) = 1 \Longrightarrow -\sum_{j=0}^{q-1} \Big(\sum_{j=0}^{q-1} a_i^{q-1-j} \Big) x^j = 1.$$

Αν εξισώσουμε τους συντελεστές οδηγούμαστε στην δεύτερη συνθήκη. Από την άλλη, αν η δεύτερη συνθήκη ίσχυε, δηλαδή

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{για } t = 0, 1, ..., q-2 \\ -1 & \text{για } t = q-1 \end{cases}$$

Τότε το πολυώνυμο μας θα ήταν το $g(x) = 1$ και άρα $\{a_0, ..., a_{q-1}\} = \mathbb{F}_q$. □

Θεώρημα 1.1.4. *(Κριτήριο Hermite)*
Έστω $\mathbb{F}_q$ ένα σώμα χαρακτηριστικής p. Τότε, το $f \in \mathbb{F}_q[x]$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μονο αν

(i) Το f έχει ακριβώς μια ρίζα στο $\mathbb{F}_q$ και

(ii) για κάθε ακέραιο t με $1 \leq t \leq q-2$ και $t \neq 0 \mod p$, το

$$f(x)^t \mod (x^q - x)$$

έχει βαθμό $\leq q-2$.

Απόδειξη. Έστω ότι το f είναι πολυώνυμο μετάθεσης στο $\mathbb{F}_q$. Τότε, το (i) προκύπτει άμεσα γιατί αλλιώς το πολυώνυμο θα είχε περισσότερες από μία διαφορετικές θέσεις μηδενισμου και δεν θα ήταν ένα-προς-ένα. Για το (ii),το $f(x)^t \mod (x^q - x)$ είναι κάποιο πολυώνυμο της μορφής $\sum_{j=0}^{q-1} b_j^{(t)} x^j$. Από τον τύπο παρεμβόλης Lagrange για κάθε $x \in \mathbb{F}_q$

$$f(x)^t = \sum_{c \in \mathbb{F}_q} f(c)^t (1 - (x-c)^{q-1}).$$

Αφού αναπτύξουμε όπως φαίνεται παρακάτω

$$f(x)^t = \sum_{c\in\mathbb{F}_q} f(c)^t(1-(x-c)^{q-1}) \\ = \sum_{c\in\mathbb{F}_q} f(c)^t(1-x^{q-1}+...) = -\sum_{c\in\mathbb{F}_q} f(c)^t x^{q-1}+...$$

παρατηρούμε ότι ο μεγιστοβάθμιος όρος του $f(x)^t$ είναι $b_{q-1}^{(t)} = -\sum_{c\in\mathbb{F}_q} f(c)^t$. Αφού όμως η $f(x)^t$ είναι ένα-προς-ένα και η εικόνα της είναι όλο το $\mathbb{F}_q$, με τη βοήθεια του λήμματος 1.1.3 συμπεραίνουμε ότι για $t = 1, 2, ..., q-2$ το $b_{q-1}^{(t)} = 0$. Έτσι το (ii) ισχύει.

Αντίστροφα, έστω ότι οι (i) και (ii) ισχύουν. Το $f(c)^{q-1}$ μπορεί να πάρει τις τιμές 0 ή 1. Από την (i) έχουμε ότι μόνο ένα από τα $f(c)$ κάνει 0. Επομένως, $\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = q-1 = -1 \mod p$. Από την (ii) για το $f^t(x) = \sum_{i=0}^{q-2} b_i^{(t)} x^i$ έχουμε ότι $\sum_{c\in\mathbb{F}_q} f(c) = \sum_{i=0}^{q-2} b_i(\sum_{c\in\mathbb{F}_q} c^i) = 0$ για $t \not\equiv 0 \mod p$, όπως προκύπτει από το λήμμα 1.1.3. Επίσης αφού το σώμα είναι χαρακτηριστικής p, ισχύει

$$\sum_{c\in\mathbb{F}_q} f(c)^{tp^j} = (\sum_{c\in\mathbb{F}_q} f(c)^t)^{p^j}.$$

Έτσι έχουμε $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ για $1 \le t \le q-2$ και από το λήμμα 1.1.3 συμπεραίνουμε ότι το f πολυώνυμο μετάθεσης. □

Πόρισμα 1.1.5. *Αν $d > 1$ ένας διαιρέτης του $q-1$, τότε δεν υπάρχει πολυώνυμο μετάθεσης του $\mathbb{F}_q$ βαθμού d.*

Απόδειξη. Αν το $f \in \mathbb{F}_q[x]$ έχει $deg(f) = d$, τότε $deg(f^{\frac{q-1}{d}}) = q-1$ κάτι το οποίο αντιφάσκει με τη δεύτερη συνθήκη του κριτηρίου Hermite για $t = (q-1)/d$. Είναι εμφανές από την απόδειξη του παραπάνω θεωρήματος ότι αν η f είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ τότε η συνθήκη (ii) του κριτηρίου Hermite ισχύει χωρίς τον περιορισμό $t \not\equiv 0 \mod p$. □

Η συνθήκη (i) του κριτήριου του Hermite μπορεί να αντικατασταθεί από άλλες συνθήκες όπως οι ακόλουθες:

Θεώρημα 1.1.6. *Έστω $\mathbb{F}_q$ ένα σώμα χαρακτηριστικής p. Τότε το $f \in \mathbb{F}_q[x]$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μόνο αν ισχύουν οι δύο ακόλουθες συνθήκες:*

(i) Το $f(x)^{q-1} \mod (x^q - x)$ έχει βαθμό $q-1$,

(ii) Για κάθε ακέραιο t *με* $1 \leq t \leq q-2$ *και* $t \not\equiv 0 \mod p$, *το*

$$f(x)^t \mod (x^q - x)$$

έχει βαθμό $\leq q-2$.

Απόδειξη. Έστω ότι το $f(x)$ είναι πολυώνυμο μετάθεσης. Το (ii) ισχύει από το κρίτηριο Hermite. Σε εκείνη την απόδειξη είχαμε ότι

$$b_{q-1}^{(q-1)} = -\sum_{c \in \mathbb{F}_q} f(c)^{q-1}.$$

Αλλά αφού το $f(x)$ είναι πολυώνυμο μετάθεσης και απο το λήμμα 1.1.3, έχουμε ότι $b_{q-1}^{(q-1)} = -(-1) = 1$, ο μεγιστοβάθμιος όρος υπάρχει, οπότε το $f(x)^{q-1} \mod (x^q - x)$ έχει βαθμό $q-1$. Αντίστροφα, έστω ότι ισχύουν τα (i) και (ii). Από την (ii) για το $f(x) = \sum_{i=0}^{q-2} b_i x^i$ έχουμε ότι $\sum_{c \in \mathbb{F}_q} f(c) = \sum_{i=0}^{q-2} b_i (\sum_{c \in \mathbb{F}_q} c^i) = 0$ για $t \neq 0 \mod p$, όπως προκύπτει από το λήμμα 1.1.3. Επίσης αφού το σώμα είναι χαρακτηριστικής p, ισχύει

$$\sum_{c \in \mathbb{F}_q} f(c)^{tp^j} = (\sum_{c \in \mathbb{F}_q} f(c)^t)^{p^j}.$$

Έτσι έχουμε $\sum_{c \in \mathbb{F}_q} f(c)^t = 0$ για $1 \leq t \leq q-2$ και από το λήμμα 1.1.3 . Επομένως, το πολυώνυμο

$$g(x) = -\sum_{j=0}^{q-1} \Big(\sum_{c \in \mathbb{F}_q} f(c)^{q-1-j} \Big) x^j$$

είναι μία μη μηδενική σταθερά. Αν τώρα, το $f(x)$ δεν ήταν πολυώνυμο μετάθεσης του $\mathbb{F}_q$, τότε το επιχείρημα του 1.1.3 θα έδειχνε ότι υπάρχει $b \in \mathbb{F}_q$ με $g(b) = 0$, το οποίο είναι άτοπο. □

Κεφάλαιο 2

ΕΙΔΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΠΟΛΥΩΝΥΜΩΝ ΜΕΤΑΘΕΣΗΣ

Σε αύτο το κεφάλαιο θα αναλύσουμε πολλές ειδικές περιπτώσεις πολυωνύμων μετάθεσης που έχουν ιδιαίτερο ενδιαφέρον. Ιδιαίτερα το θεωρημα 2.2.6 θα το εξετάσουμε διεξοδικά στο επόμενο κεφάλαιο.

2.1 Εισαγωγή

Θα ξεκινήσουμε αυτό το κεφάλαιο εξετάζοντας τις απλούστερες περιπτώσεις πολυωνύμων μετάθεσης.

2.2 Ειδικές Περιπτώσεις

Θεώρημα 2.2.1. *Οι ακόλουθες περιπτώσεις αποτελούν πολυώνυμα μετάθεσης του* $\mathbb{F}_q$.

(i) Κάθε γραμμικό πολυώνυμο του $\mathbb{F}_q$,

(ii) Το μονώνυμο x^n *είναι πολυώνυμο μετάθεσης του* $\mathbb{F}_q$ *αν και μόνο αν* $ΜΚΔ(n, q-1) = 1$.

Απόδειξη. Το (i) ισχύει λόγω του ότι η απεικόνιση είναι ένα-προς-ένα.

Για το (ii) έχουμε ότι το x^n είναι πολυώνυμο μετάθεσης στο $\mathbb{F}_q$ αν και μόνο αν η συνάρτηση $g \mapsto g^n$ είναι επί, όπου g είναι κάποιο πρωταρχικό στοιχείο του $\mathbb{F}_q$, το οποίο ισχύει αν και μόνο αν το $|< g^n >|=|< g >|$, το οποίο ισχύει όταν ΜΚΔ$(n, q-1) = 1$.

□

Παράδειγμα 2.2.2. *Το* $P(x) = x + 2$ *είναι πολυώνυμο μετάθεσης του* $\mathbb{F}_3$ *με*

c	0	1	2
$P(c)$	2	0	1

Παράδειγμα 2.2.3. *Έστω x^2+x+1 ανάγωγο πάνω από το $\mathbb{F}_2$ και θ μια ρίζα του. Τότε $\mathbb{F}_4 = \{0, 1, \theta, \theta+1\}$.*

Το $P(x) = x^2$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_4$ αφού ΜΚΔ$(3, 2) = 1$. Οι τιμές του είναι

c	0	1	θ	$\theta+1$
$P(c)$	0	1	$\theta+1$	θ

Θεώρημα 2.2.4. *Έστω $\mathbb{F}_q$ σώμα χαρακτηριστικής p. Τότε, το p-πολυώνυμο*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x],$$

είναι πολυώνυμο μετάθεσης αν και μόνο αν το $L(x)$ έχει ρίζα το 0 του $\mathbb{F}_q$.

Απόδειξη. Αφού το $\mathbb{F}_q$ αποτελεί διανυσματικό χώρο πάνω από το $\mathbb{F}_p$, παρατηρούμε ότι η συνάρτηση $L : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ είναι γραμμικός τελεστής του $\mathbb{F}_q$ πάνω από το $\mathbb{F}_p$. Έτσι, η L είναι ένα-προς-ένα αν και μόνο αν το πολυώνυμο $L(x)$ έχει μοναδική ρίζα το 0 στο $\mathbb{F}_q$. □

Παράδειγμα 2.2.5. *Έστω το πολυώνυμο x^2+x+2 που είναι ανάγωγο πάνω από το $\mathbb{F}_3$ και έστω ξ μία ρίζα του. Τότε,*

$$\mathbb{F}_9 = \{0, 1, 2, \xi, \xi+1, \xi+2, 2\xi, 2\xi+1, 2\xi+2\}.$$

Θεωρούμε το $L(x) = x + \xi x^3 \in \mathbb{F}_9[x]$. Μια βάση του $\mathbb{F}_9$ πάνω από το $\mathbb{F}_3$ είναι $\{1, \xi\}$. Έχουμε,

$$L(1) = 1 + \xi,$$
$$L(\xi) = \xi + \xi^4 = 2 + \xi.$$

Έτσι, ο πίνακας που αναπαριστά την γραμμική απεικόνιση L δίνεται από

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

Παρατηρούμε ότι $detA = -1 \neq 0$ άρα η L σαν απεικόνιση είναι ένα-προς-ένα. Πράγματι,

c	0	1	2	ξ	$\xi+1$	$\xi+2$	2ξ	$2\xi+1$	$2\xi+2$
$P(c)$	0	$\xi+1$	$2\xi+2$	$\xi+2$	2ξ	1	$2\xi+1$	2	ξ

Μπορούμε να βρούμε περισσότερα παραδείγματα παρατηρώντας απλώς ότι το σύνολο των πολυωνύμων μετάθεσης είναι κλειστό ως προς τη σύνθεση, δηλαδή αν $f(x)$ και $g(x)$ είναι πολυώνυμα μετάθεσης του $\mathbb{F}_q[x]$, τότε και το $\big(f \circ g\big)(x)$ είναι πάλι πολυώνυμο μετάθεσης του $\mathbb{F}_q$.

Θεώρημα 2.2.6. *Έστω $r \in \mathbb{N}$ με ΜΚΔ$(r, q-1) = 1$ και s ένας θετικός διαιρέτης του $q-1$. Έστω ακόμα $g \in \mathbb{F}_q[x]$ τέτοιο ώστε το $g(x^s)$ να μην έχει μη μηδενική ρίζα στο $\mathbb{F}_q$. Τότε, το*

$$f(x) = x^r(g(x^s))^{(q-1)/s},$$

είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$.

Απόδειξη. Η συνθήκη (i) του κριτηρίου Hermite ικανοποιήται καθώς $f(0) = 0$ και δεν υπάρχει άλλη ρίζα στο $\mathbb{F}_q$. Για να αποδείξουμε την (ii) χρειάζεται να διακρίνουμε δύο περιπτώσεις. Διαλέγουμε $t \in \mathbb{Z}$ με $1 \leq t \leq q-2$ και πρώτα υποθέτουμε ότι το t δεν διαιρείται από το s. Παρατηρούμε στην περίπτωση αυτη ότι το $f(x)^t$ είναι άθροισμα όρων των οποίων οι εκθέτες είναι της μορφής $rt+ms$, όπου $m \in \mathbb{Z},\ m \geq 0$. Αφού ΜΚΔ$(r, s) = 1$, οι εκθέτες δεν διαιρούνται από το s και έτσι ούτε απο το $q-1$. Συνεπώς, το $f(x) \mod (x^q - x)$ έχει βαθμό $\leq q-2$. Διαφορετικά, αν το t διαιρείται από το s, δηλαδή $t = ks$ για κάποιο $k \in \mathbb{N}$, τότε

$$f(x)^t = x^{rt}(g(x^s))^{(q-1)k}.$$

Θεωρούμε $h(x) = x^{rt}$ και έχουμε $(f(c))^t = h(c)$ για $c \in \mathbb{F}_q^*$ αφού $(g(c^s))^{(q-1)k} = 1$. Καθώς $g(c^s) \neq 0$, επίσης παίρνουμε $(f(0))^t = h(0)$. Τότε, από το λήμμα 1.1.2, $(f(x))^t \equiv x^{rt} \mod (x^q - x)$ και αφού το $q-1$ δεν διαιρεί το rt, το $f(x)^t \mod (x^q - x)$ έχει βαθμό $\leq q-2$. □

Παράδειγμα 2.2.7. *Έχουμε το $\mathbb{F}_{11}$ και $11 - 1 = 2 \cdot 5$. Άρα μπορούμε να επιλέξουμε $s = 5$ και $\frac{q-1}{s} := l = 2$ και δοκιμάζουμε το $g(x) = 1 + x + x^2$. Θεωρούμε, τώρα, το πολυώνυμο $G(x) := g(x^5) = 1 + x^5 + x^{10} \mod (x^{11} - x)$. Παρατήρουμε ότι οι τιμές του G είναι:*

$$G(0) = 1,\ G(1) = 3,\ G(2) = 1,\ G(3) = 3,\ G(4) = 3,\ G(5) = 3,$$
$$G(6) = 1, G(7) = 1,\ G(8) = 1,\ G(9) = 3,\ G(10) = 1.$$

Δηλαδή, το G δεν έχει μη μηδενική ρίζα στο $\mathbb{F}_{11}$. Επίσης ΜΚΔ$(r, 10) = 1$, άρα μπορούμε να επιλέξουμε $r = 3$, και έτσι το

$$P(x) = x^3(1 + x^5 + x^{10})^2 \mod (x^{11} - x) = 5x^3 + 4x^8 \mod (x^{11} - x)$$

είναι πολυώνυμο μετάθεσης του $\mathbb{F}_{11}$. Οι τιμές του είναι:

c	0	1	2	3	4	5	6	7	8	9	10
$P(c)$	0	9	8	1	4	3	7	2	6	5	10

Ορισμός 2.2.8. *Έστω* $\eta : \mathbb{F}_q^* \to \{-1, 1\}$ *με τύπο*

$$\eta(c) = \begin{cases} 1, & \text{αν } c = b^2 \text{ για κάποιο } b \in \mathbb{F}_q^* \\ -1, & \text{αλλιώς} \end{cases}$$

υιοθετώντας την σύμβαση $\eta(c) = 0$ *όταν* $c = 0$. *Αυτή η συνάρτηση καλείται* ***τετραγωνικός χαρακτήρας***.

Θεώρημα 2.2.9. *Για* q *περιττό, το πολυώνυμο* $x^{(q+1)/2} + ax \in \mathbb{F}_q[x]$ *είναι πολυώνυμο μετάθεσης του* $\mathbb{F}_q$ *αν και μόνο αν* $\eta(a^2 - 1) = 1$.

Απόδειξη. Θεωρούμε το πολυώνυμο $f(x) = x^{(q+1)/2} + ax$ και θα δείξουμε ότι το $f(x)$ είναι ένα-προς-ένα αν και μόνο αν $\eta(a^2 - 1) = 1$. Η ακόλουθη απόδειξη θα γίνει με αντιθετοαντίστροφη. Αρχικά αποδεικνύεται το ευθή: Έστω ότι η f δεν ήταν ένα-προς-ένα. Τότε διακρίνουμε τις εξής περιπτώσεις:

1. Έστω $f(c) = f(0)$ με $c \in \mathbb{F}_q^*$. Τότε

   $$c^{(q+1)/2} + ac = 0 \Rightarrow c^{(q-1)/2} + a = 0 \Rightarrow a = -c^{(q-1)/2} \Rightarrow a^2 = (c^{(q-1)/2})^2 = 1.$$

   Δηλαδή $a^2 - 1 = 0$ και άρα $\eta(a^2 - 1) = 0$.

2. Αν $f(c) = f(b)$ με $b, c \in \mathbb{F}_q^*$ και $b \neq c$. Τότε,

   $$\begin{aligned} &b^{(q+1)/2} + ab = c^{(q+1)/2} + ac \iff \\ &b(b^{(q-1)/2} + a) = c(c^{(q-1)/2} + a) \iff \\ &bc^{-1} = (c^{(q-1)/2} + a)(b^{(q-1)/2} + a)^{-1}. \end{aligned}$$

   Έπειτα διακρίνουμε τις εξής υποπεριπτώσεις:

   - Αν $\eta(b) = \eta(c)$, τότε $b^{(q-1)/2} = c^{(q-1)/2}$,άρα από τη παραπάνω σχέση $b = c$, το οποίο είναι άτοπο.
   - Αν $\eta(b) \neq \eta(c)$, τότε χωρίς βλάβη της γενικότητας παίρνουμε $\eta(b) = -1$ και $\eta(c) = 1$. Τότε, $b^{(q-1)/2} = -1$ και $c^{(q-1)/2} = 1$.
     Επίσης, $bc^{-1} = \frac{a+1}{a-1}$. Έτσι, προκύπτει ότι $\eta(b)\eta(c) = -1$. Άρα, $-1 = \eta(bc^{-1}) = \eta((a+1)(a-1)^{-1}) = \eta((a+1)(a-1)) = \eta(a^2-1)$.

Αντίστροφα, υποθέτουμε ότι $\eta(a^2-1) \neq 1$ δηλαδή είτε $\eta(a^2-1) = 0 \Rightarrow a^2 = 1$ είτε $\eta(a^2 - 1) = -1$.

- Στην πρώτη περίπτωση, έχουμε $a = 1$ ή $a = -1$. Το πολυώνυμο θα ήταν το $f(x) = x^{(q+1)/2} + x$, το οποίο έχει ρίζα το 0. Από την άλλη, όταν το $a = \pm 1$, θα υπάρχει $c \in \mathbb{F}_q^*$ τέτοιο ώστε $c^{(q-1)/2} = -a$. Τότε, $f(c) = c^{(q-2)/2}c + ac = -ac + ac = 0 = f(0)$, το οποίο είναι άτοπο.

- Στην άλλη περίπτωση, αφού θεωρήσουμε $b = (a+1)(a-1)^{-1}$ παίρνουμε

$$\begin{aligned}&\eta(a^2-1) = -1 \Longrightarrow \eta((a+1)(a-1)) = -1 \Longrightarrow\\ &\eta((a+1)(a-1)^{-1}) = -1 \Longrightarrow\\ &\eta(b) = -1 \ \text{ με } \ b(a-1) = a+1.\end{aligned}$$

  Επίσης,

$$\begin{aligned}&\eta(b) = -1 \Longrightarrow b^{(q-1)/2} = -1,\\ &f(b) = b^{(q-1)/2}b + ab = b(a-1) = a+1.\end{aligned}$$

Όμως, $f(1) = 1 + a = f(b)$ με $b \neq 1$. Συμπεραίνουμε ότι και στις δύο περιπτώσεις η f δεν είναι ένα-προς-ένα.

□

Ένα χρήσιμο πόρισμα για να επιλέξουμε κατάλληλο a όπως αυτό αναφέρεται στο θεώρημα 2.2.9 είναι το παρακάτω

Πόρισμα 2.2.10. *$\eta(a^2-1) = 1$ αν και μόνο αν $a = (c^2+1)(c^2-1)$ για κάποιο $c \in \mathbb{F}_q^*$ και $c \neq 1$.*

Απόδειξη. Έστω $\eta(a^2-1) = 1$. Τότε $a^2 - 1 = b^2$, για κάποιο $b \in \mathbb{F}_q^*$. Επιλέγουμε $c = (a+1)b^{-1}$ και έχουμε $c \neq 0$ και $c^2 \neq 1$. Επιπλέον,

$$\begin{aligned}(c^2+1)(c^2-1) &= [\big((a+1)b\big)^2 + 1][\big((a+1)b\big)^2 - 1]\\ &= [(a+1)^2b^{-2} + 1][(a+1)^2b^{-2} - 1]\\ &= [(a+1)^2 + b^2][(a+1)^2 - b^2]\\ &= [2a^2 + 2a][2a+2] = a.\end{aligned}$$

Αντίστροφα, αν $a = (c^2+1)(c^2-1)$ για $c \in \mathbb{F}_q^*$ και $c^2 \neq 1$, τότε $a^2 - 1 = 4c^2(c^2-1)^{-2}$, άρα $\eta(a^2-1) = 1$. □

Παράδειγμα 2.2.11. *Έστω το πολυώνυμο x^2+x+2 που είναι αναγώγο πάνω από το $\mathbb{F}_3$ και ξ μία ρίζα του, δηλαδή $\xi^2+\xi+2 = 0$ ή $\xi^2 = 2\xi+1$. Έτσι, έχουμε*

$$\mathbb{F}_9 = \{0, 1, 2, \xi, \xi+1, \xi+2, 2\xi, 2\xi+1, 2\xi+2\}.$$

Οπότε,

$$(\xi^2+1)(\xi^2-1)^{-1} = (2\xi+2)(2\xi)^{-1} = (2\xi+2)(2\xi+2) = \xi+2.$$

Έτσι, $\eta(\xi+2) = 1$ και από το παραπάνω θεώρημα έχουμε ότι το $P(x) = x^5 + (\xi+2)x \in \mathbb{F}_9[x]$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_9$. Ουσιαστικά, η μετάθεση αυτή, είναι η εξής:

c	0	1	2	ξ	$\xi+1$	$\xi+2$	2ξ	$2\xi+1$	$2\xi+2$
$P(c)$	0	ξ	2ξ	1	$\xi+1$	$2\xi+1$	2	$2\xi+2$	$\xi+2$

Κεφάλαιο 3

ΠΟΛΥΩΝΥΜΑ ΤΗΣ ΜΟΡΦΗΣ $\mathbf{x^r f\left(x^{(q-1)/l}\right)}$

Γενικότερα, αποτελεί πρόκληση να διακρίνεις το πότε κάποιο πολυώνυμο είναι πολυώνυμο μετάθεσης. Στην πραγματικότητα λίγες κατηγορίες τέτοιου είδους πολυωνύμων είναι γνωστές. Μερικά παραδείγματα πολυωνύμων μετάθεσης μπορούν να κατασκευαστούν σαν υποκατηγορία των πολυωνύμων της μορφής $x^r f(x^{(q-1)/l})$, όπου $r, l \geq 1$ και $l|(q-1)$.

3.1 Εισαγωγη

Τα τελευταία χρόνια υπάρχει ιδιαίτερο ενδιαφέρον στη μελέτη πολυωνύμων μετάθεσης λόγω των εφαρμογών τους στην κρυπτογραφία και στην κωδικοποίηση. Μια γενικότερα χρήσιμη παρατήρηση είναι ότι οποιοδήποτε πολυώνυμο $h(x)$ του $\mathbb{F}_q[x]$ μπορεί να γραφεί στη μορφή $a(x^r f(x^{(q-1)/l}) + b$ για κάποιο $r \geq 0$ και $l|(q-1)$. Μπορούμε χωρις βλάβη της γενικότητας να γράψουμε

$$h(x) = a(x^n + a_{n-i_1}x^{n-i_1} + ... + a_{n-i_k}x^{n-i_k}) + b$$

όπου $a, a_{n-i_1} \neq 0$, $j = 1, ..., k$. Υποθέτουμε ότι $j \geq 1$ και $n - i_k = r$. Τότε το $h(x) = a(x^r f(x^{(q-1)/l})) + b$, όπου $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} ... + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$,

$$l = \frac{q-1}{(n-r, n-r-i_1, ..., n-r-i_{k-1}, q-1)},$$

και $(e_0, e_1, ..., e_{k-1}, l) = 1$. Εδώ, όπως και στις επόμενες σελίδες, με (a, b) συμβολίζουμε το μέγιστο κοινό διαιρέτη των a, b.

Λόγω του ενδιαφέροντος των πολυωνύμων αυτής της μορφής, έχει δοθεί πληθώρα κριτηρίων για το κάτω από ποιες προυποθέσεις κάποιο πολυώνυμο είναι πολυώνυμο μετάθεσης. Ο στόχος αυτού του κεφαλαίου είναι να παρουσιάσουμε κάποια από αυτά.

3.2 Γενικά Κριτήρια

Σε αυτό το κεφάλαιο θεωρούμε g ένα πρωταρχικό στοιχείο του $\mathbb{F}_q$, $\omega = g^{\frac{q-1}{l}}$ μια πρωταρχική l-οστή ρίζα και $s := \frac{q-1}{l}$. Επίσης, με $\mathrm{Ind_g}(a)$ θα συμβολίζουμε την κλάση $b \mod (q-1)$ τέτοιο ώστε το $a = g^b$.

Το βασικό θεώρημα αυτού του κεφαλαίου που βάση αυτού θα προκύψουν διάφορα κριτήρια, είναι το εξής:

Θεώρημα 3.2.1. *(Wan-Lidl) Έστω l και r θετικοί ακέραιοι οι οποίοι ικανοποιούν $l|(q-1)$. Έστω $f(x) \in \mathbb{F}_q[x]$. Τότε το πολυώνυμο $P(x) = x^r f(x^{\frac{(q-1)}{l}})$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μόνο αν οι ακόλουθες συνθήκες ισχύουν:*

(ι) $(r, (q-1)/l) = 1$,

(ιι) $f(\omega^i) \neq 0$, *για όλα τα* $0 \leq i < l$,

(ιιι) Για όλα τα $0 \leq i < j < l$,

$$\mathrm{Ind_g}\Big(\frac{f(\omega^i)}{f(\omega^j)}\Big) \not\equiv r(j-i) \mod l.$$

Απόδειξη. Για την πρώτη κατεύθυνση, υποθέτουμε ότι το $P(x)$ είναι πολυώνυμο μετάθεσης. Παρατηρούμε ότι $P(0) = 0$ και αφού το $P(x)$ είναι ένα-προς-ένα, έχουμε ότι τα $P(g^k) \neq 0$, όπου g ένα πρωταρχικό στοιχείο του $\mathbb{F}_q$ και για $1 \leq k \leq q-2$. Άρα, $g^{kr} f((g^s)^k) \neq 0$, δηλαδή $f(\omega^i) \neq 0$ με $0 \leq i \leq l$. Επομένως, επαληθεύσαμε την δεύτερη συνθήκη.

Τώρα, έστω $(r, \frac{q-1}{l}) = e > 1$ και η μια πρωταρχική e-οστή ρίζα της μονάδας. Τότε

$$\begin{aligned} P(\eta) &= \eta^r f(\eta^{\frac{q-1}{l}}) = f(1), \\ P(1) &= f(1) \end{aligned}$$

Άρα, $P(\eta) = P(1)$ το οποίο αντιφάσκει με το ότι το $P(x)$ είναι ένα-προς-ένα. Επομένως, η πρώτη συνθήκη ισχύει.

Για το (iii), έστω $0 \leq i < j < l$. Παίρνουμε $P(g^i) = g^{ir} f(\omega^i)$ και $P(g^j) = g^{jr} f(\omega^j)$ Έστω ότι ίσχυε $\mathrm{Ind_g}\Big(\frac{f(\omega^i)}{f(\omega^j)}\Big) \equiv r(j-i) \mod l$. Τότε για κάποιο $w \in \mathbb{Z}$,

$$\begin{aligned} \mathrm{Ind_g}\Big(\frac{f(\omega^i)}{f(\omega^j)}\Big) \equiv r(j-i) + wl &\Longrightarrow \frac{f(\omega^i)}{f(\omega^j)} = g^{r(j-i)+wl} \\ &\Longrightarrow g^{ri} f(\omega^i) = g^{rj} f(\omega^j) g^{wl} \\ &\Longrightarrow \frac{g^{ri} f(\omega^i)}{g^{rj} f(\omega^j)} = g^{wl} \\ &\Longrightarrow \frac{P(g^i)}{P(g^j)} = g^{wl} \end{aligned}$$

και $(r,s)=1$ άρα υπάρχουν x,y τέτοια ώστε $rx+sy=1 \Rightarrow lrx+lsy=l \Rightarrow lrx+(q-1)y=l$. Αντικαθιστώντας στην παραπάνω σχέση έχουμε

$$\frac{P(g^i)}{P(g^j)}=g^{w(lrx+(q-1)y)} \Longrightarrow \frac{P(g^i)}{P(g^j)}=g^{wlrx}$$
$$P(g^i)=g^{wlrx}P(g^j)=g^{wlrx}g^{rj}f(\omega^j)=g^{r(wlx+j)}f(\omega^{j+wlx})=P(g^{j+wlx}).$$

Όμως $i \neq j \mod l$ άρα $i \neq j+wlx$. Αφού καταλήξαμε σε άτοπο συμπεραίνουμε ότι η (iii) ισχύει.

Για την άλλη κατεύθυνση, δεχόμαστε ότι και οι τρεις συνθήκες ισχύουν. Έχουμε $P(0)=0$ και από το (ii) παίρνουμε $P(g^k)\neq 0$. Έστω $0 \leq m < k \leq q-2$ και

$$P(g^m)=P(g^k) \Longrightarrow g^{mr}f(\omega^m)=g^{kr}f(\omega^k)$$

Εκτελούμε ακέραια διαίρεση των εκθετών με το l και έχουμε $m=li'+i$ και $k=lj'+j$.

$$\begin{aligned}
g^{(li'+i)r}f(\omega^{li'+i})=g^{(lj'+j)r}f(\omega^{lj'+j}) &\Longrightarrow g^{rli'+ri}f(\omega^i)=g^{rlj'+rj}f(\omega^j)\\
&\Longrightarrow \frac{f(\omega^i)}{f(\omega^j)}=g^{lj'r-li'r+jr-ir}\\
&\Longrightarrow \mathrm{Ind_g}\Big(\frac{f(\omega^i)}{f(\omega^j)}\Big)=l(j'r-i'r)+(jr-ir) \mod (q-1)\\
&\Longrightarrow \mathrm{Ind_g}\Big(\frac{f(\omega^i)}{f(\omega^j)}\Big)\equiv r(j-i) \mod l
\end{aligned}$$

Άρα από την (iii) συμπεραίνω ότι $i=j$. Έτσι, $m=li'+i$ και $k=lj'+i$, οπότε

$$\begin{aligned}
P(g^m)=g^{lri'}g^{ri}f(\omega^i)=g^{lrj'}g^{ri}f(\omega^i) &\Longrightarrow lri' \equiv lrj' \mod (q-1)\\
&\Longrightarrow ri' \equiv rj' \mod s\\
&\Longrightarrow i'=j' \mod s
\end{aligned}$$

αφού $(r,s)=1$, οπότε $m=k$ και άρα το $P(x)$ είναι ένα-προς-ένα. □

Παράδειγμα 3.2.2. *Έστω $s=4$ και $l=3$ και $q=13$. Υπολογίζουμε στο $\mathbb{F}_{13}$,*

$2^1=2$	$2^2=4$	$2^3=8$	$2^4=3,$
$2^5=6$	$2^6=12$	$2^7=11$	$2^8=9,$
$2^9=5$	$2^{10}=10$	$2^{11}=7$	$2^{12}=1$

Εδώ το $g = 2$ *και* $\omega = 3$, $< \omega >= \{3, 9, 1\}$. *Αναζητούμε* $f(x)$ *με* $f(\omega^i) \neq 0$ *για* $i = 0, 1, 2$. *Δοκιμάζουμε το* $f(x) = 1 + x + x^2 + x^3 + x^4 \in \mathbb{F}_{13}[x]$.

Υπολογίζουμε,

$$f(3^0) = f(1) = 5,$$
$$f(3^1) = f(3) = 4,$$
$$f(3^2) = f(9) = 10.$$

Επίσης,

$$\mathrm{Ind}_2 \frac{f(3^0)}{f(3^1)} = \mathrm{Ind}_2 \frac{5}{4} = \mathrm{Ind}_2 11 = 7 \mod 3 \equiv 1 \mod 3 \not\equiv r(1-0),$$
$$\mathrm{Ind}_2 \frac{f(3^0)}{f(3^2)} = \mathrm{Ind}_2 \frac{5}{10} = \mathrm{Ind}_2 7 = 11 \mod 3 \equiv 2 \mod 3 \not\equiv r(2-0),$$
$$\mathrm{Ind}_2 \frac{f(3^1)}{f(3^2)} = \mathrm{Ind}_2 \frac{4}{10} = \mathrm{Ind}_g 3 = 4 \mod 3 \not\equiv r(2-1).$$

Έχουμε δηλαδή $r \not\equiv 1 \mod 3$ *και* $(r, 4) = 1$. *Επομένως, μπορούμε να επιλέξουμε* $r = 5$. *Υπολογίζουμε το* $f(x^4) = 1 + x^4 + x^8 + x^{12} + x^{16}$

Άρα, $P(x) = x^5(1 + x^4 + x^8 + x^{12} + x^{16}) \mod (x^{13} - x) = x^5 + x^9 + x^{13} + x^{17} + x^{21} \mod (x^{13} - x)$. *Το* $P(x) = x + 2x^5 + 2x^9$ *είναι πολυώνυμο μετάθεσης.*

Πράγματι,

c	0	1	2	3	4	5	6	7	8	9	10	11	12
$P(c)$	0	5	11	10	9	12	7	6	1	4	3	2	8

Λήμμα 3.2.3. *Έστω* $l|(q-1)$ *και* μ_l *το σύνολο όλων των* l*-οστών ριζών της μονάδας του* $\mathbb{F}_q$. *Έστω* $\xi_0, \xi_1, ..., \xi_{l-1}$ *να είναι κάποιες* l*-οστές ρίζες της μονάδας. Τότε*

$$\{\xi_0, \xi_1, ..., \xi_{l-1}\} = \mu_l \iff \sum_{t=0}^{l-1} \xi_t^c = 0, \quad \textit{για} \ \ c = 1, ..., l-1$$

Απόδειξη. Πρώτα, παρατηρούμε ότι για οποιαδήποτε l-οστή ρίζα της μονάδας ξ, έχουμε

$$1 + \xi + ... + \xi^{l-1} = \begin{cases} \text{αν } \xi \neq 1, & \frac{\xi^l - 1}{\xi - 1} = 0, \\ \text{αν } \xi = 1, & 1 + \ldots + 1 = l. \end{cases}$$

Τώρα, για $t = 0, ..., l-1$, ορίζουμε τα βοηθητικά πολυώνυμα

$$h_t(x) = \sum_{j=0}^{l-1} \xi_t^{l-j} x^j.$$

Επίσης, παρατηρούμε ότι

$$h_t(\xi_t) = \sum_{j=0}^{l-1} \xi_t^{l-j} \xi_t^j = \sum_{j=0}^{l-1} \xi_t^l = \sum_{j=0}^{l-1} 1 = l.$$

Επιπλέον, για $\xi_t \neq \xi_j$,

$$h_t(\xi_j) = \sum_{j=0}^{l-1} \xi_t^{l-j} \xi_j^j = \sum_{j=0}^{l-1} \xi_t^l \big(\frac{\xi_j}{\xi_t}\big)^j = 0.$$

Άρα,

$$h_t(\xi_j) = \begin{cases} 0 & \text{αν } \xi_t \neq \xi_j \\ l & \text{αν } \xi_t = \xi_j \end{cases}$$

Τώρα, έστω $\mathcal{J} = \{0 \leq t < l \ : \xi_t = \xi_j\}$ και

$$h(x) = \sum_{t=0}^{l-1} h_t(x) = l + \sum_{j=1}^{l-1} \Big(\sum_{t=0}^{l-1} \xi_t^{l-j} \Big) x^j,$$
$$m(x) = h(x) - l.$$

Έχουμε $h(\xi_j) = \sum_{j=0}^{l-1} h_t(\xi_j) = l|\mathcal{J}|$.

Αν $\{\xi_0, \xi_1, ..., \xi_{l-1}\} = \mu_l$ τότε $h(\xi_j) = l$, οπότε το $m(x)$ έχει l ρίζες και είναι βαθμού $\leq l-1$ άρα $\sum_{t=0}^{l-1} \xi_t^c = 0$.

Από την άλλη, αν $\sum_{t=0}^{l-1} \xi_t^c = 0$ προκύπτει άμεσα ότι $h(x) = 0$ και $h(\xi_j) = l$ που σημαίνει ότι $|\mathcal{J}| = \{0 \leq t < l \ : \xi_t = \xi_j\} = 1$.

□

Θεώρημα 3.2.4. *Έστω $q-1 = ls$ για κάποιους θετικούς ακεραίους l και s. Έστω ω μια πρωταρχική l-οστή ρίζα της μονάδας του $\mathbb{F}_q$ και $f(x)$ ένα πολυώνυμο του $\mathbb{F}_q[x]$. Τότε το $P(x) = x^r f(x^s)$ είναι πολυώνυμο μεταθεσης του $\mathbb{F}_q$ αν και μόνο αν*

(i) $(r, s) = 1$,

(ii) $f(\omega^t) \neq 0$, *για κάθε* $t = 0, ..., l-1$,

(iii) $\sum_{t=0}^{l-1} \omega^{crt} f(\omega^t)^{cs} = 0$ *για κάθε* $c = 1, ..., l-1$.

Απόδειξη. Έστω ότι το $P(x)$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$. Τότε $P(x) = 0$ μόνο για $x = 0$. Το (ii) προκύπτει άμεσα καθώς το $P(x)$ είναι ένα-προς-ένα. Για να δείξουμε ότι $(r, s) = 1$, υποθέτουμε ότι $(r, s) = e > 1$ και η είναι μια e-οστή ρίζα της μονάδας. Υπολογίζουμε

$$P(\eta) = \eta^r f(\eta^s) = f(1) = P(1),$$

το οποίο έρχεται σε αντίφαση με την ένα-προς-ένα ιδιότητα του $P(x)$. Έτσι αποδείχθηκε η (i).

Για να αποδείξουμε την (iii),αρκεί να δείξουμε ότι $\{\omega^{ir} f(\omega^i)^s : i = 0, ..., l-1\} = \mu_l$ και να εφαρμόσουμε το παραπάνω λήμμα. Έστω $0 \leq i < j \leq l-1$ και $\omega^{ir} f(\omega^i)^s = \omega^{jr} f(\omega^j)^s$.

Όμως,

$$P(g^i)^s = \omega^{ir} f(\omega^i)^s = \omega^{jr} f(\omega^j)^s = P(g^j)^s \Longrightarrow \Big(\frac{P(g^i)}{P(g^j)}\Big)^s = 1.$$

Άρα, υπάρχει $0 \leq v \leq s-1$ τέτοιο ώστε

$$\frac{P(g^i)}{P(g^j)} = g^{lv} \Longrightarrow P(g^i) = g^{lv} P(g^j).$$

Επιπλέον, $(r, s) = 1$ και άρα υπάρχει $t \in \mathbb{Z}$ τέτοιο ώστε $tr = v \mod s$. Συνεπώς, $tlr = lv \mod q-1$. Μάλιστα, χωρίς βλάβη της γενικότητας, το t μπορεί να επιλεχθεί ως $1 \leq t < s$ και

$$P(g^{tl+j}) = g^{(tl+j)r} f(\omega^{tl+j}) = g^{tlr} g^{jr} f(\omega^j) = g^{lv} P(g^j) = P(g^i).$$

Έπειδη το $P(x)$ είναι ένα-προς-ένα,

$$tl + j \equiv i \mod (q-1) \Rightarrow i - j \equiv tl \mod (q-1) \Rightarrow i - j \equiv 0 \mod l.$$

Το οποίο είναι άτοπο.

Για την αντιστροφη κατεύθυνση, έχουμε από το (ii) ότι $P(0) = 0$ και τα $P(g^k) \neq 0$. Από την (iii) έχουμε $\{\omega^{ir} f(\omega^i)^s : i = 0, ..., l-1\} = \mu_l$. Έστω

$P(g^m) = P(g^k)$. Τώρα, εκτελούμε την ακέραια διαίρεση των εκθετών με το l και έχουμε $m = li' + i$ και $k = lj' + j$. Αντικαθιστούμε και έχουμε

$$\begin{aligned} g^{(lj'+j)r} f(\omega^j) = g^{(li'+i)r} f(\omega^i) &\Longrightarrow g^{rlj'} g^{rj} f(\omega^j) = g^{rli'} g^{ri} f(\omega^i) \\ &\Longrightarrow g^{jrs} f(\omega^j)^s = g^{irs} f(\omega^i)^s \\ &\Longrightarrow \omega^{jr} f(\omega^j)^s = \omega^{jr} f(\omega^j)^s \\ &\Longrightarrow i = j \end{aligned}$$

Έχοντας ότι $i = j$ προκύπτει

$$\begin{aligned} P(g^m) = g^{rm} f(\omega^i) = g^{rk} f(\omega^i) = P(g^k) &\Longrightarrow g^{rli'+i} = g^{rlj'+i} \\ &\Longrightarrow rli' = rlj' \mod (q-1) \\ &\Longrightarrow ri' = rj' \mod s \end{aligned}$$

αφού $(r, s) = 1$ και άρα $i' = j'$ και άρα το $P(x)$ είναι ένα-προς-ένα.

□

Παράδειγμα 3.2.5. *Έστω ότι έχουμε το $\mathbb{F}_{11}$. Τότε, $11 - 1 = 2 \cdot 5$. Άρα, επιλέγουμε $l = 2$ και $s = 5$. Επιπλέον, έχουμε $< 10 >= \{10, 1\}$, δηλαδή $\omega = 10$. Δοκιμάζουμε το $f(x) = 1 + x + x^2$. Παρατηρήστε ότι αναγκαστηκά το $c = 1$ για την τρίτη συνθήκη. Το r είναι περιττός αφού από την συνθήκη (iii) έχουμε*

$$\sum_{t=0}^{1} 10^r f(10^t)^5 = 0$$
$$1^r + (-1)^r = 0.$$

Από την πρώτη έχουμε ότι $(r, s) = 1$. Επομένως, μπορούμε να επιλέξουμε $r = 3$. Στην περίπτωση αυτή, το $P(x)$ δίνεται από

$$\begin{aligned} P(x) &= x^3(1 + x^5 + x^{10}) \mod (x^{11} - x) \\ &= x^3 + x^8 + x^{13} \mod (x^{11} - x) \\ &= 2x^3 + x^8 \mod (x^{11} - x). \end{aligned}$$

Το $P(x)$ είναι πολυώνυμο μετάθεσης και οι τιμές του είναι

c	0	1	2	3	4	5	6	7	8	9	10
$P(c)$	0	3	8	4	5	1	7	2	6	9	10

Πόρισμα 3.2.6. *Έστω $q - 1 = ls$, $(r, s) = 1$, ω μια l-οστή ρίζα της μονάδας του $\mathbb{F}_q$ και $f(x)$ ένα πολυώνυμο του $\mathbb{F}_q[x]$ τέτοιο ώστε κανένα από τα ω^t με $t = 0, ..., l - 1$ να μην μηδενίζει το $f(x)$. Τότε, τα ακόλουθα είναι ισοδύναμα*

(ι) $\sum_{t=0}^{l-1} \omega^{crt} f(\omega^t)^{cs} = 0$ *για κάθε* $c = 1, ..., l-1$.

(ιι) Για όλα τα $0 \leq i < j < l$, $Ind_g\big(\frac{f(\omega^i)}{f(\omega^j)}\big) \not\equiv r(j-i) \pmod{l}$.

Έχουμε δει ήδη στο θεώρημα 2.2.9 ότι το διώνυμο $x^{(q+1)/2} + ax$ είναι πολυώνυμο μετάθεσης αν και μόνο αν $\eta(a^2-1) = 1$, όπου η είναι ο τετραγωνικός χαρακτήρας όπως αυτός ορίστηκε στον δεύτερο κεφάλαιο.

Πόρισμα 3.2.7. *Για* q *περιττό, το πολυώνυμο* $P(x) = x^r f(x^{(q-1)/2})$ *είναι πολυώνυμο μετάθεσης αν και μόνο αν*

$$(r, (q-1)/2) = 1 \ \text{ και } \ \eta(f(-1)f(1)) = (-1)^{r+1}.$$

Απόδειξη. Για $l = 2$ και $c = 1$ από το θεώρημα 3.2.4, έχουμε

$$\begin{aligned}
\sum_{t=0}^{1} \omega^{rt} f(\omega^t)^{\frac{q-1}{2}} = 0 &\Longrightarrow (-1)^r f((-1)^0)^{\frac{q-1}{2}} + (-1)^r f(-1)^{\frac{q-1}{2}} = 0 \\
&\Longrightarrow f(1)^{\frac{q-1}{2}} + (-1)^r f(-1)^{\frac{q-1}{2}} = 0 \\
&\Longrightarrow f(-1)^{\frac{q-1}{2}} f(1)^{\frac{q-1}{2}} + (-1)^r f(-1)^{\frac{q-1}{2}} f(-1)^{\frac{q-1}{2}} = 0 \\
&\Longrightarrow \big(f(-1)f(1)\big)^{\frac{q-1}{2}} = (-1)^{r+1} \\
&\Longrightarrow \eta(f(-1)f(1)) = (-1)^{r+1}.
\end{aligned}$$

□

3.3 Πρώτη Εφαρμογή

Θεώρημα 3.3.1. *Έστω* $q - 1 = ls$. *Υποθέτουμε ότι* $f(\omega^t)^s = 1$ *για* $t = 0, ..., l-1$. *Τότε, το* $P(x) = x^r f(x^s)$ *είναι πολυώνυμο μετάθεσης του* $\mathbb{F}_q$ *αν και μόνο αν* $(r, q-1) = 1$.

Απόδειξη. Έστω ότι $(r, q-1) = e > 1$ και έστω ότι το $P(x)$ είναι πολυώνυμο μετάθεσης. Τότε από τη σχέση (i) του 3.2.4 έχουμε ότι $(r, s) = 1$, συνεπώς συμπεραίνουμε ότι $(r, l) = e$. Δηλαδή, υπάρχει μ με $r = \mu \cdot e$. Επιλέγοντας τώρα $c = \frac{l}{e}$, έχουμε

$$\sum_{t=0}^{l-1} \omega^{crt} = \sum_{t=0}^{l-1} \omega^{\frac{l}{e}\mu et} = \sum_{t=0}^{l-1} (\omega^l)^{\mu t} = \sum_{t=0}^{l-1} 1 = l$$

και έτσι συμπεραίνουμε ότι η (iii) του 3.2.4 δεν ισχύει, επομένως το $P(x)$ δεν είναι πολυώνυμο μετάθεσης και έτσι καταλήξαμε σε αντίφαση. Αντίστροφα,

έστω ότι $(r, g-1) = 1$. Τότε έχουμε ότι $(r, s) = 1$, επομένως η (i) του 3.2.4 ισχύει. Επιπλέον από το ότι $f(\omega^t)^s = 1$ έχουμε ότι και η (ii) ισχύει. Τέλος, έχουμε

$$\sum_{t=0}^{l-1} \omega^{crt} = 1 + \omega^{cr} + \omega^{2cr} + ... + \omega^{(l-1)cr} = \frac{1-\omega^{crl}}{1-\omega^{cr}} = 0.$$

Έτσι έχουμε ότι και η (iii) του 3.2.4 ισχύει, οπότε το $P(x)$ είναι πολυώνυμο μετάθεσης. □

Πόρισμα 3.3.2. *(Laigle-Chapuy) Έστω p ένας πρώτος, l ένας θετικός ακέραιος και v η τάξη του p στην $(\mathbb{Z}/l\mathbb{Z})^*$. Για κάθε ακέραιο n, παίρνουμε $q = p^m = p^{lvn}$ και $q - 1 = ls$. Υποθέτουμε ότι $f(x) \in \mathbb{F}_{p^{vn}}[x]$. Τότε, το πολυώνυμο $P(x) = x^r f(x^s)$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μόνο αν $(r, q-1) = 1$ και $f(\omega) \neq 0$ για όλα τα $0 \leq t \leq l-1$.*

Απόδειξη. Από το θεώρημα 3.3.1, αρκεί να δείξουμε ότι $f(\omega^t)^s = 1$ για $0 \leq t \leq l-1$. Υπολογίζουμε

$$s = \frac{q-1}{l} = \frac{p^{vn}-1}{l} = \frac{p^{vn}-1}{l}\left((p^{vn})^{l-1} + (p^{vn})^{l-2} + ... + 1\right)$$

Άρα έχουμε

$$f(\omega^t)^s = (f(\omega^t)^\mu)^{p^{vn}-1} = 1.$$

$$\begin{aligned} f(\omega^t)^{\frac{q-1}{l}} &= f(\omega^t)^{\frac{p^{lvn}-1}{l}} \\ &= f(\omega^t)^{\frac{p^{vn}-1}{l}\left((p^{vn})^{l-1}+(p^{vn})^{l-2}+...+1\right)} \\ &= \left(f(\omega^t)^{(p^{vn})^{l-1}} f(\omega)^{(p^{vn})^{l-2}} ... f(\omega)^1\right)^{\frac{p^{vn-1}}{l}} \\ &= \left(\prod_{i=0}^{l-1} f(\omega^t)^{p^{v(ni)}}\right)^{\frac{p^{vn-1}}{l}} = \left(f(\omega^t)^l\right)^{\frac{p^{vn}-1}{l}} = f(\omega^t)^{p^{vn}-1} = 1. \end{aligned}$$

□

3.4 Δεύτερη Εφαρμογή

Θεώρημα 3.4.1. *Έστω $q - 1 = ls$ και ζ μια jl-οστή ρίζα της μονάδας. Υποθέτουμε ακόμα ότι $f(\zeta^{jt}) = \zeta^{ut}$ για όλα $t = 0, ..., l-1$ και σταθερό u και $j|us$. Τότε, το $P(x) = x^r f(x^s)$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μόνο αν ισχύουν τα ακόλουθα*

(ι) $(r, s) = 1$,

(ιι) $(r + \frac{us}{j}, l) = 1$.

Απόδειξη. Το πρώτο είναι τετριμένο. Για την δεύτερη, θα χρησιμόποιήσουμε το θεώρημα 3.2.4 για να δείξουμε ότι είναι ισοδύναμο με το $\sum_{t=0}^{l-1} \omega^{crt} f(\omega^t)^{cs} = 0$ για $c = 1, ..., l-1$ όπου ω μια l-οστή πρωταρχική ρίζα της μονάδας. Έχουμε,

$$\begin{aligned}\sum_{t=0}^{l-1} \omega^{crt} f(\omega^t)^{cs} &= \sum_{t=0}^{l-1} \zeta^{jcrt} f(\zeta^{jt})^{cs} = \sum_{t=0}^{l-1} \zeta^{jcrt} \zeta^{utcs} \\ &= \sum_{t=0}^{l-1} \zeta^{ct(jr+us)} = \sum_{t=0}^{l-1} (\zeta^j)^{ct(r+\frac{us}{j})} \\ &= \sum_{t=0}^{l-1} (\omega)^{ct(r+\frac{us}{j})}\end{aligned}$$

Το παραπάνω άθροισμα κάνει μηδέν αν και μόνο αν $l \nmid c(r + \frac{us}{j})$ για όλα τα $c = 1, ..., l-1$ το οποίο είναι ισοδύναμο με το ότι $(r + \frac{us}{j}, l) = 1$. □

Λήμμα 3.4.2. *Έστω p ένας περιττός πρώτος, $q - 1 = ls$ και $f(x) = 1 + x + ... + x^k$. Τότε, $f(\omega^t) \neq 0$ για κάθε $0 \leq t \leq l-1$ αν και μόνο αν $(lp, k+1) = 1$.*

Απόδειξη. Αρχικά δεχόμαστε ότι $f(\omega^t) \neq 0$. Έχουμε

$$f(1) = k + 1 \neq 0 \Longrightarrow (k+1, p) = 1$$

Επίσης,
Αρχικά δεχόμαστε ότι $f(\omega^t) \neq 0$. Έχουμε

$$\begin{aligned}f(\omega^t) = 1 + \omega^t + ... + \omega^{kt} = \frac{\omega^{(k+1)t} - 1}{\omega^t - 1} \neq 0 &\Longrightarrow \omega^{(k+1)t} - 1 \neq 0 \\ &\Longrightarrow \omega^{(k+1)t} \neq 1 \\ &\Longrightarrow l \nmid (k+1)t.\end{aligned}$$

Έστω $(l, k+1) = e > 1$ και $k + 1 = e \cdot \mu$ για $\mu \in \mathbb{Z}$. Τότε για $t = \frac{l}{e}$ θα είχαμε $l \nmid \mu e \frac{l}{e} \Rightarrow l \nmid \mu \cdot l$, το οποίο είναι άτοπο. Επομένως, $(l, k+1) = 1$. Άρα έχουμε ότι $(lp, k+1) = 1$.

Αντίστροφα, δεχόμαστε ότι $(lp, k+1) = 1$. Δηλαδή $(p, k+1) = 1$ και $(l, k+1) = 1$. Από την πρώτη συμπεραίνουμε ότι $f(1) = k+1 \neq 0$. Επιπλέον από την δεύτερη έχουμε ότι $l \nmid (k+1)t$ για $1 \leq t \leq l-1$. Δηλαδή

$$\omega^{(k+1)t} - 1 \neq 0 \Rightarrow \frac{\omega^{(k+1)t} - 1}{\omega^t - 1} \neq 0 \Rightarrow 1 + \omega^t + ... + \omega^{kt} \neq 0 \Rightarrow f(\omega^t) \neq 0.$$

□

Λήμμα 3.4.3. *Έστω p ένας περιττός πρώτος, $q - 1 = ls$ και a κάποιο μη μηδενικό στοιχείο του $\mathbb{F}_p$. Τότε*

(ι) Αν $p \equiv -1 \mod l$ και $l > 1$ περιττός, τότε $a^s = 1$ στο $\mathbb{F}_p$,

(ιι) Αν $p \equiv -1 \mod l$ και $l = 2l_1$ με $l_1 > 1$ περιττό, τότε έχουμε $a^s = 1$ στο $\mathbb{F}_p$.

Απόδειξη. Για την πρώτη συνθήκη αρκεί να δείξουμε ότι $s = (p-1) \cdot \mu$ με $\mu \in \mathbb{N}$, αφού $a^{p-1} = 1$ για κάθε $a \in \mathbb{F}_p$. Έχουμε

$$p \equiv -1 \mod l \Longrightarrow l | p+1 \quad \text{και}$$
$$l | p^m - 1 = (p-1)(p^{m-1} + ... + 1).$$

Όμως $s \cdot l = (p-1)(p^{m-1} + ... + 1)$, άρα αρκεί να δείξουμε ότι $(p-1, l) = 1$. Έστω ότι $d = (p-1, l)$. Ισχύουν επιπλέον οι συνθήκες

$$d | p - 1,$$
$$d | l \Longrightarrow d | p + 1.$$

Επομένως, $d|2$ και αφού το d διαιρεί τον περιττό l, έχουμε $d = 1$. Άρα $s|p-1$ και $a^s = 1$.

Για την δεύτερη συνθήκη αρκεί να δείξουμε ότι $(l_1, p-1) = 1$. Έστω $(p-1, l) = d$, και ισχύουν τα εξής

$$p \equiv -1 \mod l \Longrightarrow l | p+1 \quad \text{και}$$
$$l | p^m - 1 = (p-1)(p^{m-1} + ... + 1).$$

Άρα $d|2$ και αφού το d διαιρεί το $l = 2 \cdot l_1$ προκύπτει ότι $d = 2$. Επιπλέον,

$$2 \cdot l_1 \cdot s = (p-1)(p^{m-1} + ... + 1).$$

Επίσης,

$$p \equiv -1 \mod l \Longrightarrow p^m \equiv (-1)^m \mod l \Longrightarrow q \equiv (-1)^m \mod l$$

Έστω ότι το m είναι περιττός. Τότε $q \equiv -1 \mod l$. Όμως,

$$l|q+1,$$
$$l|q-1.$$

Επομένως, $l|2 \Longrightarrow 2 \cdot l_1|2$ και $l_1 > 1$, το οποίο είναι άτοπο. Άρα το m είναι άρτιος. Άρα το $2|p^{m-1} + ... + p + 1$. Επομένως,

$$2 \cdot l_1 \cdot s = (p-1)(p^{m-1} + ... + 1) \Longrightarrow l_1 \cdot s = (p-1)\frac{(p^{m-1} + ... + 1)}{2}$$

Έχουμε $(2l_1, p-1) = 2 \Rightarrow (l_1, \frac{p-1}{2}) = 1$ και $(l_1, 2) = 1$. Άρα $(l_1, p-1) = 1$. □

Θεώρημα 3.4.4. *Έστω p περιττός πρώτος και $q - 1 = ls$. Υποθέτουμε ότι είτε $l > 1$ περιττός είτε $l = 2l_1$ με $l_1 > 1$ περιττό. Αν $p \equiv -1 \mod l$, τότε το πολυώνυμο $P(x) = x^r(1 + x^s + ... + x^{ks})$ είναι πολυώνυμο μετάθεσης του $\mathbb{F}_q$ αν και μόνο αν ισχύουν τα ακόλουθα*

(ι) $(r, s) = 1$,

(ιι) $(r + \frac{ks}{2}, l) = 1$,

(ιιι) $(lp, k+1) = 1$.

Απόδειξη. Επιλέγουμε $u = k$ και $j = 2$, ζ μια πρωταρχική $2l$-ρίζα του 1 του $\mathbb{F}_q$ και θεωρούμε την παράσταση

$$\begin{aligned} A &= \zeta^{-ut} f(\zeta^{jt}) = \zeta^{-kt} f(\zeta^{2t}) \\ &= \zeta^{-kt}(1 + \zeta^{2t} + \zeta^{4t} + ... + \zeta^{kt}) \\ &= \zeta^{-kt}\frac{(\zeta^{2t})^{k+1} - 1}{\zeta^{2t} - 1} \\ &= \frac{\zeta^{2kt+2t-kt} - \zeta^{-kt}}{\zeta^{2t} - 1} \\ &= \frac{\zeta^{(k+1)t} - \zeta^{-(k+1)t}}{\zeta^{t} - \zeta^{-t}}. \end{aligned}$$

Τώρα, αφού $2l|p+1$ και $p \equiv -1 \mod l$ προκύπτει ότι $2l|p+1$ και $\zeta^{pt} =$

$\zeta^{(p+1)t}\zeta^{-t} = \zeta^{-t}$. Έτσι,

$$\begin{aligned}
A &= \frac{\zeta^{(k+1)t} - \zeta^{-(k+1)t}}{\zeta^t - \zeta^{-t}} \\
&= \frac{\zeta^t - \zeta^{-t}}{\zeta^t - \zeta^{-t}}\Big((\zeta^t)^k + (\zeta^t)^{k-1}(\zeta^{-t}) + ... + (\zeta^t)(\zeta^{-t})^{k-1} + (\zeta^{-t})^k\Big) \\
&= \Big((\zeta^t)^k + (\zeta^t)^{k-1}(\zeta^{-t}) + ... + (\zeta^t)(\zeta^{-t})^{k-1} + (\zeta^{-t})^k\Big). \\
A^p &= \Big((\zeta^t)^k + (\zeta^t)^{k-1}(\zeta^{-t}) + ... + (\zeta^t)(\zeta^{-t})^{k-1} + (\zeta^t)^k\Big)^p \\
&= (\zeta^{pt})^k + (\zeta^{pt})^{k-1}(\zeta^{-pt}) + ... + (\zeta^{pt})(\zeta^{-pt})^{k-1} + (\zeta^{-pt})^k \\
&= (\zeta^{-t})^k + (\zeta^{-t})^{k-1}(\zeta^t) + ... + (\zeta^{-t})(\zeta^t)^{k-1} + (\zeta^t)^k.
\end{aligned}$$

Έτσι, $A^p = A$ και $A \in \mathbb{F}_p$. Από το παραπάνω λήμμα παίρνουμε άμεσα ότι $A^s = 1$. Δηλαδή $\zeta^{-ut} f(\zeta^{jt})^s = 1$. Τώρα, τα (i), (ii) προκύπτουν άμεσα από το θεώρημα 3.4.1. □

Παράδειγμα 3.4.5. *Θεωρούμε το ανάγωγο πολυώνυμο $x^2 - 2$ πάνω από του $\mathbb{F}_5$. Έστω θ μία ρίζα του, έτσι έχουμε*

$$\begin{aligned}
\mathbb{F}_{25} = \{&0, 1, 2, 3, 4, \theta, \theta+1, \theta+2, \theta+3, \theta+4, 2\theta, 2\theta+1, 2\theta+2, 2\theta+3, 2\theta+4, \\
&3\theta, 3\theta+1, 3\theta+2, 3\theta+3, 3\theta+4, 4\theta, 4\theta+1, 4\theta+2, 4\theta+2, 4\theta+3, \theta+4\}
\end{aligned}$$

Εδώ έχουμε $25 - 1 = 6 \cdot 4$ και $5 = -1 \mod 6$ με $6 = 2 \cdot 3$, έτσι άμεσα επιλέγουμε $l = 6$ και $s = 4$. Τώρα $(r, 4) = 1$, άρα επιλέγουμε $r = 3$, τέλος $(3 + 2k, 6) = 1$ και $(30, k + 1) = 1$, άρα επιλέγουμε $k = 10$.

Έτσι το πολυώνυμο

$$P(x) = x^3(1 + x^4 + x^8 + x^{12} + x^{16} + x^{20} + x^{24} + x^{28} + x^{32} + x^{36} + x^{40}) \mod (x^{25} - x) =$$
$$P(x) = 2x^3 + 2x^7 + 2x^{11} + 2x^{15} + 2x^{19} + x^{23} \mod (x^{25} - x)$$

είναι πολυώνυμο μετάθεσης του $\mathbb{F}_{25}$.

Πράγματι,

c	0	1	2	3	4	θ	$\theta+1$	$\theta+2$	$\theta+3$	$\theta+4$
$P(c)$	0	1	3	2	4	2θ	$4\theta+1$	$3\theta+4$	$3\theta+1$	$4\theta+4$
c	2θ	$2\theta+1$	$2\theta+2$	$2\theta+3$	$2\theta+4$	3θ	$3\theta+1$	$3\theta+2$	$3\theta+3$	$3\theta+4$
$P(c)$	θ	$4\theta+3$	$2\theta+3$	$2\theta+2$	$4\theta+2$	4θ	$\theta+3$	$3\theta+3$	$3\theta+2$	$\theta+2$
c	4θ	$4\theta+1$	$4\theta+2$	$4\theta+3$	$4\theta+4$					
$P(c)$	3θ	$\theta+1$	$2\theta+4$	$2\theta+1$	$\theta+4$					

Κεφάλαιο 4

ΑΡΙΘΜΙΣΗ ΠΟΛΥΩΝΥΜΩΝ ΜΕΤΑΘΕΣΗΣ ΒΑΘΜΟΥ $q-2$ ΠΑΝΩ ΑΠΟ ΤΟ $\mathbb{F}_q$

Έστω $\mathbb{F}_q$ ένα πεπερασμένο σώμα με $q = p^m > 2$ στοιχεία, για m φυσικό αριθμό και μια μετάθεση $\sigma \in S(\mathbb{F}_q)$. Το πολυώνυμο μετάθεσης f_σ που αντιστοιχεί στην σ είναι:

$$f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)(1-(x-c)^{q-1})$$

η f_σ έχει την ιδιότητα $f_\sigma(a) = \sigma(a)$ για κάθε $a \in \mathbb{F}_q$.
Από το θεώρημα 1.1.4 παρατηρούμε ότι για κάθε σ

$$deg(f_\sigma) \leq q-2.$$

Ένα μεγάλο ζήτημα που προκύπτει γύρω από τα πολυώνυμα μετάθεσης είναι το κατα πόσο μπορούμε να καθορίσουμε τον αριθμό N_d των πολυωνύμων μετάθεσης με σταθερό βαθμό d. Στην συνέχεια αποδεικνύεται ένα θεώρημα το οποίο επιβεβαιώνει την κοινή άποψη ότι σχεδόν όλα τα πολυώνυμα μετάθεσης έχουν βαθμό $q-2$.

Θεώρημα 4.0.6. *Έστω*

$$N = \#\{\sigma \in S(\mathbb{F}_q) |\ deg(f_\sigma) < q-2\}$$

Τότε,

$$|N-(q-1)!| \leq q^{q/2}\sqrt{\frac{2e}{\pi}}.$$

Οι πρώτες τιμές του N φαίνονται στον παρακάτω πίνακα:

q	2	3	4	5	7	8	9	11
N	0	0	12	20	630	5.368	42.120	3.634.950
$(q-1)!$	1	2	6	24	720	5.040	40.320	3.628.800

Απόδειξη. Στην παρακάτω απόδειξη θα χρησιμοποιήσουμε εκθετικά αθροίσματα.

Αρχικά αναπτύσουμε το

$$f_\sigma(x) = \sum_{c\in\mathbb{F}_q} \sigma(c)(1-(x-c)^{q-1}) = \sum_{c\in\mathbb{F}_q} \sigma(c) - \sum_{c\in\mathbb{F}_q} \sigma(c)(x-c)^{q-1} =$$
$$= \sum_{c\in\mathbb{F}_q} \sigma(c) - \sum_{c\in\mathbb{F}_q} \sigma(c)(x^{q-1} - cx^{q-2} + ... + c^{q-2})$$

και παρατηρούμε ότι το παραπάνω πολυώνυμο έχει βαθμό μικρότερο από $q-2$ αν και μόνο αν ο συντελεστής του x^{q-2} είναι 0, δηλαδή

$$\sum_{c\in\mathbb{F}_q} c\sigma(c) = 0.$$

Τώρα, για συγκεκριμένα S, T υποσύνολα του $\mathbb{F}_q$ εισάγουμε τα βοηθητικά σύνολα συναρτήσεων:

$$N_S = \Big\{ f |\ f : \mathbb{F}_q \to S \ \text{ και } \ \sum_{c\in\mathbb{F}_q} cf(c) = 0 \Big\}$$

$$M_T = \Big\{ f |\ f : \mathbb{F}_q \to T \ \text{ επί και } \sum_{c\in\mathbb{F}_q} cf(c) = 0 \Big\}$$

Θεωρούμε $n(S) = |N_S|$ και $m(T) = |M_T|$.

Παρατηρούμε ότι $N_S = \bigcup_{T\subseteq S} M_T$, καθώς $f \in N_S$ τότε η f θα ανήκει σε κάποιο N_T δηλαδή θα είναι επί συνάρτηση σε κάποιο $T \subseteq \mathbb{F}_q$. Από την άλλη αν διαλέξουμε κάποιο στοιχείο f της $\bigcup_{T\subseteq S} M_T$, τότε αυτό ανήκει στο N_S αφού είναι συνάρτηση από το $\mathbb{F}_q$ στο S.

Ορισμός 4.0.7. *Έστω N ένα πεπερασμένο σύνολο και $S \subset T \subset N$, τότε ορίζουμε*

$$\mu(S,T) := (-1)^{|T|-|S|}$$

Λήμμα 4.0.8. *(Inclusion-Exclusion)'Εστω N ένα πεπερασμένο σύνολο και f μία συνάρτηση ορισμένη στα υποσύνολα του N. Αν*

$$g(S) := \sum_{R \subset S} f(R)$$

Τότε,

$$f(T) = \sum_{S \subset T} \mu(S,T) g(S).$$

Απόδειξη.

$$\sum_{S \subset T} \mu(S,T) g(S) = \sum_{S \subset T} \mu(S,T) \sum_{R \subset S} f(R) = \sum_{R \subset T} f(R) \sum_{R \subset S \subset T} \mu(S,T),$$

τότε το αποτέλεσμα ακολουθεί από την ισότητα:

$$\sum_{R \subset S \subset T} \mu(S,T) = \sum_{j=0}^{|T|-|R|} \binom{|T|-|R|}{j} (-1)^j = (1-1)^{|T|-|R|} = \begin{cases} 0 & \text{αν } R \neq T \\ 1 & \text{αν } R = T \end{cases}$$

□

Χρησιμοποιώντας το παραπάνω λήμμα προκύπτει:

$$n(S) = \sum_{T \subset S} m(T) \Rightarrow m(R) = \sum_{R \subset S} \mu(S,R) n(S)$$

Εδώ,

$$m(\mathbb{F}_q) = N = \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} n(S). \tag{4.1}$$

Τώρα, θεωρούμε $e_p(u) = e^{2\pi i u/p}$ και θέλουμε ουσιαστικά να βρούμε το πλήθος των f για τις οποίες ισχύει ότι

$$\sum_{c \in \mathbb{F}_q} c f(c) = 0$$

και από το εξής βοηθητικό λήμμα:

Λήμμα 4.0.9.

$$\frac{1}{q} \sum_{a \in \mathbb{F}_q} e_p(Tr(ax)) = \begin{cases} 1 & \text{αν } x = 0 \\ 0 & \text{αν } x \neq 0 \end{cases}$$

Απόδειξη. Έστω $s = \sum_{a\in\mathbb{F}_q} e_p(Tr(ax)) = \sum_{a\in\mathbb{F}_q} e_p(Tr(a))$ αφού η $h : \mathbb{F}_q \to \mathbb{F}_q$ με τύπο $h(a) = ax$, με $x \in \mathbb{F}_q^*$ είναι ένα προς ένα και επί. Τώρα, $\exists b \in \mathbb{F}_q$ τέτοιο ώστε $Tr(b) \neq 0$. Έτσι, έχουμε

$$e^{\frac{2\pi i}{p}Tr(b)} \sum_{a\in\mathbb{F}_q} e^{\frac{2\pi i}{p}(Tr(a)+Tr(b))} = \sum_{a\in\mathbb{F}_q} e^{\frac{2\pi i}{p}Tr(a+b)} = \sum_{a\in\mathbb{F}_q} e^{\frac{2\pi i}{p}Tr(a)}.$$

Άρα,

$$e^{\frac{2\pi i}{p}Tr(b)}s = s \iff (e^{\frac{2\pi i}{p}Tr(b)} - 1)s = 0 \iff s = 0.$$

□

παίρνουμε ότι

$$\begin{aligned} n(S) &= \sum_{f:\mathbb{F}_q\to S} \frac{1}{q} \sum_{a\in\mathbb{F}_q} e_p\big(Tr(a \sum_{c\in\mathbb{F}_q} cf(c))\big) \\ &= \frac{1}{q} \sum_{f:\mathbb{F}_q\to S} \sum_{a\in\mathbb{F}_q} e_p\big(\sum_{c\in\mathbb{F}_q} Tr(acf(c))\big) \end{aligned}$$

Παρατηρώντας ότι

$$\begin{aligned} e_p\Big(\sum_{c\in\mathbb{F}_q} Tr(acf(c))\Big) &= e^{\frac{2\pi i}{p}\sum\limits_{c\in\mathbb{F}_q} Tr(acf(c))} \\ &= e^{\frac{2\pi i}{p}(Tr(ac_1f(c_1)+\ldots+Tr(ac_qF(c_q)))} \\ &= e^{\frac{2\pi i}{p}Tr(ac_1f(c_1))} \cdots e^{\frac{2\pi i}{p}Tr(ac_qf(c_q))} \\ &= e_p(Tr(ac_1f(c_1))) \cdots e_p(Tr(ac_qf(c_q))) \\ &= \prod_{c\in\mathbb{F}_q} e_p(Tr(acf(c))), \end{aligned}$$

συμπεραίνουμε λοιπόν ότι η αλλαγή του αθροίσματος με το γινόμενο είναι επιτρεπτή. Επιπλέον, δεδομένου του ότι $t_1, t_2, ..., t_s$ είναι τα στοιχεία του S.

$$\sum_{f:\mathbb{F}_q\to S}\prod_{c\in\mathbb{F}_q} e_p\big(Tr(acf(c))\big) = \sum_{(t_1,t_2,\dots,t_q)\in S^q}\prod_{j=1}^{q} e_p\big(Tr(ac_jt_j)\big)$$
$$= \sum_{t_1\in S}\sum_{t_2\in S}\dots\sum_{t_q\in S} e_p\big(Tr(ac_1t_1)\big)e_p\big(Tr(ac_2t_2)\big)\dots e_p\big(Tr(ac_qt_q)\big)$$
$$= \prod_{j=1}^{q}\sum_{t_j\in S} e_p\big(Tr(ac_jt_j)\big)$$
$$= \sum_{t_1\in S} e_p\big(Tr(ac_1t_1)\sum_{t_2\in S} e_p\big(Tr(ac_2t_2)\big)\dots\sum_{t_q\in S} e_p\big(Tr(ac_qt_q)\big)$$

Κάνοντας αντικαταστάσεις σύμφωνα με τα παραπάνω, έχουμε

$$n(S) = \frac{1}{q}\sum_{a\in\mathbb{F}_q}\Big(\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(Tr(act))\Big).$$

Υπολογίζουμε το εξωτερικό άθροισμα για $a = 0$ και προκύπτει

$$\frac{1}{q}\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(Tr(0)) = \frac{1}{q}\prod_{c\in\mathbb{F}_q}|S| = \frac{1}{q}|S|^q.$$

Τελικά, παρατηρώντας ότι το εσωτερικό άθροισμα δεν επιρεάζεται από το a, έχουμε

$$n(S) = \frac{|S|^q}{q} + \frac{1}{q}\sum_{a\in\mathbb{F}_{q^*}}\Big(\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(Tr(bt))\Big) = \frac{|S|^q}{q} + \frac{q-1}{q}\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(Tr(bt)). \tag{4.2}$$

Τώρα, τοποθετώντας την (4.2) στην (4.1), παίρνουμε

$$N = \sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\Big(\frac{|S|^q}{q} + \frac{q-1}{q}\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(Tr(bt))\Big) \iff$$

$$N - \sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\frac{|S|^q}{q} = \frac{q-1}{q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(Tr(bt))$$

Τώρα, όπως και προηγουμένως θεωρούμε σύνολα

- $F_S = \Big\{f : \mathbb{F}_q \to S\Big\}$,

- $G_T = \Big\{ f : \mathbb{F}_q \to T \mid \ f \text{ επί} \Big\}$.

Εδώ, $F_s = \bigcup_{T \subseteq S} G_T$ και έστω $f(S) = |F_S|$ και $g(S) = |G_T|$. Τότε από το λήμμα 4.0.6 προκύπτει

$$f(S) = \sum_{T \subseteq S} g(T)$$
$$g(T) = \sum_{S \subseteq T} \mu(S,T) f(S)$$

Όμως, $f(S) = |S|^q$ και $g(\mathbb{F}_q) = q!$, άρα

$$\sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} |S|^q = q! \iff \sum_{S \subseteq \mathbb{F}_q} \frac{(-1)^{q-|S|}}{q} |S|^q = (q-1)!.$$

Για $b = 0$ στην (4.2), προκύπτει

$$\sum_{t \in S} e_p(Tr(0)) = |S|.$$

Τελικά, έχουμε

$$N - (q-1)! = \frac{q-1}{q} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} |S| \prod_{b \in \mathbb{F}_q^*} \sum_{t \in S} e_p(Tr(bt)).$$

Χρησιμοποιώντας το γεγονός ότι το $b \in \mathbb{F}_{q^*}$, προκύπτει άμεσα ότι

$$\sum_{t \in \mathbb{F}_q} e_p(Tr(bt)) = 0 \iff \sum_{t \in S} e_p(Tr(bt)) = -\sum_{t \notin S} e_p(Tr(bt)).$$

Τώρα, τοποθετώντας τους όρους του S και τους όρους του $\mathbb{F}_q \setminus S$ έχουμε

$$N - (q-1)! = \frac{q-1}{q} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} |S| \prod_{b \in \mathbb{F}_q^*} \sum_{t \in S} e_p(Tr(bt)).$$

Αλλιώς,

$$N - (q-1)! = \frac{q-1}{q} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|+1} (-|S|) \prod_{b \in \mathbb{F}_q^*} \sum_{t \in S} e_p(Tr(bt)). \qquad (4.3)$$

Για το $\mathbb{F}_q \setminus S$, έχουμε

$$N-(q-1)!=\frac{q-1}{q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{|S|}(q-|S|)\prod_{b\in\mathbb{F}_q^*}\sum_{t\notin S}e_p(Tr(bt)) \iff$$

$$N-(q-1)!=\frac{q-1}{q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{|S|+q-1}(q-|S|)\prod_{b\in\mathbb{F}_q^*}\sum_{t\in S}e_p(Tr(bt)). \quad (4.4)$$

Τώρα, προσθέτοντας τις (4.3) και (4.4), προκύπτει

$$2(N-(q-1)!)=\frac{q-1}{q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{|S|+q-1}(q-2|S|)\prod_{b\in\mathbb{F}_q^*}\sum_{t\in S}e_p(Tr(bt)).$$

Η τριγωνική ανισότητα οδηγεί στην

$$|N-(q-1)!|\leq\frac{q-1}{2q}\sum_{S\subseteq\mathbb{F}_q}\big|q-2|S|\big|\prod_{b\in\mathbb{F}_q^*}\sum_{t\in S}e_p(Tr(bt)). \quad (4.5)$$

Στην συνέχεια, παρατηρούμε ότι

$$\begin{aligned}
\sum_{b\in\mathbb{F}_q}\Big|\sum_{t\in S}e_p(Tr(bt))\Big|^2 &= \sum_{b\in\mathbb{F}_q}\Big[\Big(\sum_{t\in S}e^{\frac{2\pi iTr(bt)}{p}}\Big)\Big(\overline{\sum_{t\in S}e^{\frac{2\pi iTr(bt)}{p}}}\Big)\Big]\\
&= \sum_{b\in\mathbb{F}_q}\Big[\Big(\sum_{t\in S}e^{\frac{2\pi iTr(bt)}{p}}\Big)\Big(\sum_{t\in S}\overline{e^{\frac{2\pi iTr(bt)}{p}}}\Big)\Big]\\
&= \sum_{b\in\mathbb{F}_q}\Big[\Big(\sum_{t\in S}e^{\frac{2\pi iTr(bt)}{p}}\Big)\Big(\sum_{t\in S}\frac{1}{e^{\frac{2\pi iTr(bt)}{p}}}\Big)\Big]\\
&= \sum_{b\in\mathbb{F}_q}\Big[\Big(e^{\frac{2\pi iTr(bt_1)}{p}}+e^{\frac{2\pi iTr(bt_2)}{p}}+...+e^{\frac{2\pi iTr(bt_n)}{p}}\Big)\times\\
&\qquad\Big(\frac{1}{e^{\frac{2\pi iTr(bt_1)}{p}}}+\frac{1}{e^{\frac{2\pi iTr(bt_2)}{p}}}+...+\frac{1}{e^{\frac{2\pi iTr(bt_n)}{p}}}\Big)\Big]\\
&= \sum_{b\in\mathbb{F}_q}\Big(\sum_{t\in S}1+\sum_{\substack{1\le i,j\le n\\ i\neq j}}e^{\frac{2\pi i(Tr(bt_i)-Tr(bt_j))}{p}}\Big)\\
&= \sum_{b\in\mathbb{F}_q}\Big(|S|+\sum_{\substack{1\le i,j\le n\\ i\neq j}}e^{\frac{2\pi i(Tr(b(t_i-t_j))}{p}}\Big)\\
&= q|S|+\sum_{b\in\mathbb{F}_q}\sum_{\substack{1\le i,j\le n\\ i\neq j}}e^{\frac{2\pi i(Tr(b(t_i-t_j))}{p}}\\
&= q|S|+\sum_{\substack{1\le i,j\le n\\ i\neq j}}\sum_{b\in\mathbb{F}_q}e^{\frac{2\pi i(Tr(b(t_i-t_j))}{p}}
\end{aligned}$$

Όμως, το δεύτερο άθροισμα ισούται με μηδέν από το λήμμα 4.0.7. Ακόμα, για $b=0$, έχουμε

$$|\sum_{t\in S}e_p(Tr(0))|^2=|S|^2.$$

Τελικά, προκύπτει

$$\sum_{b\in\mathbb{F}_q}\Big|\sum_{t\in S}e_p(Tr(bt))\Big|^2=q|S|$$

Έτσι έχουμε

$$\sum_{b\in\mathbb{F}_q^*}\Big|\sum_{t\in S}e_p(Tr(bt))\Big|^2=(q-|S|)|S|$$

Χρησιμοποιώντας την ανισότητα Cauchy,

$$(\prod_{i=1}^{k}|a_i|^2)^{\frac{1}{k}} \leq \frac{1}{k}\sum_{i=1}^{k}|a_i|^2,$$

έχουμε

$$\begin{aligned}\prod_{b\in\mathbb{F}_q^*}\Big|\sum_{t\in S}e_p(Tr(bt))\Big| &= \prod_{b\in\mathbb{F}_q^*}\Big(\Big|\sum_{t\in S}e_p(Tr(bt))\Big|^2\Big)^{\frac{q-1}{2}}\\ &\leq \Big(\frac{1}{q-1}\sum_{b\in\mathbb{F}_q^*}\Big|\sum_{t\in S}e_p(Tr(bt))\Big|^2\Big)^{q-1}\\ &= \Big(\frac{(q-|S|)|S|}{q-1}\Big)^{\frac{q-1}{2}}.\end{aligned}$$

Έτσι, από τα παραπάνω, η (4.5) διαμορφώνεται ως εξής

$$|N-(q-1)!| \leq \frac{q-1}{2q(q-1)^{\frac{q-1}{2}}}\sum_{S\subseteq\mathbb{F}_q}|q-2|S||((q-|S|)|S|)^{\frac{(q-1)}{2}}.$$

Τώρα, οι νέες ποσότητες που εμφανίστηκαν εκτιμούνται ως εξής:

$$\begin{aligned}&(q-|S|)|S| \leq (q-\frac{q}{2})(\frac{q}{2}) = \frac{q^2}{4} = (\frac{q}{2})^2,\\ &((q-|S|)|S|)^{\frac{q-1}{2}} \leq \big((\frac{q}{2})^2\big)^{\frac{q-1}{2}} = (\frac{q}{2})^{q-1}.\end{aligned} \tag{4.6}$$

Χωρίζοντας τα σύνολα ανάλογα με τον πληθαριθμό τους, παίρνουμε

$$\sum_{S\subseteq\mathbb{F}_q}|q-2|S|| = 2\sum_{\substack{S\subseteq\mathbb{F}_q\\ |S|\leq\frac{q}{2}}}(q-2|S|)$$

Τώρα, αναλύωντας το παραπάνω άθροισμα και χρησιμοποιώντας τις παραπάνω εκτιμήσεις, παίρνουμε

$$\sum_{\substack{S\subseteq\mathbb{F}_q\\ |S|\leq\frac{q}{2}}}(q-2|S|) = q+\binom{q}{1}(q-2\cdot 1)+\binom{q}{2}(q-2\cdot 2)+\cdots+\binom{q}{[\frac{q}{2}]}(q-2\cdot\left[\frac{q}{2}\right])$$

$$= q+\binom{q}{1}(q-1)-\binom{q}{1}+\binom{q}{2}(q-2)-2\binom{q}{2}\cdots+\binom{q}{\left[\frac{q}{2}\right]}(q-\binom{q}{\left[\frac{q}{2}\right]})-\left[\frac{q}{2}\right]\binom{q}{\left[\frac{q}{2}\right]}$$

$$= \sum_{i=0}^{[q/2]}\binom{q}{i}(q-i)-\sum_{i=1}^{[q/2]}\binom{q}{i}(i)$$

$$= \sum_{i=0}^{[q/2]}\frac{q(q-1)!(q-i)}{i!(q-i)!}-\sum_{i=1}^{[q/2]}\frac{q(q-1)!i!}{i!(q-i)!}$$

$$= q\sum_{i=0}^{[q/2]}\binom{q-1}{i}-q\sum_{i=1}^{[q/2]}\binom{q-1}{i-1}.$$

Τώρα, κάνοντας την αλλαγή μεταβλητής $i=j-1$ στο παραπάνω άθροισμα, προκύπτει

$$\sum_{j=1}^{[q/2]}\binom{q-1}{j-1}=\sum_{i=0}^{[q/2]-1}\binom{q-1}{i}.$$

Άρα,

$$\sum_{j=0}^{[q/2]}\binom{q-1}{j}-\sum_{j=1}^{[q/2]}\binom{q-1}{j-i}=\sum_{j=0}^{[q/2]}\binom{q-1}{j}-\sum_{j=1}^{[q/2]-1}\binom{q-1}{j}=\binom{q-1}{[q/2]}.$$

Τελικά,

$$2\sum_{\substack{S\subseteq\mathbb{F}_q\\ |S|\leq\frac{q}{2}}}(q-2|S|)=2q\binom{q-1}{[q/2]}\implies\sum_{S\subseteq\mathbb{F}_q}(q-2|S|)=2q\binom{q-1}{[q/2]}. \quad (4.7)$$

Ο στόχος μας τώρα είναι να εκτιμήσουμε την ποσότητα $\binom{q-1}{[q/2]}$.
Από τον τύπο του Stirling, για κατάλληλη ακολουθία $\{\lambda_n\}$, έχουμε

$$\binom{2n}{n}=\frac{(2n)!}{n!n!}\frac{\sqrt{2\pi 2n}(\frac{2n}{e})^{2n}e^{\lambda_{2n}}}{\sqrt{2\pi n}(\frac{n}{3})^n e^{\lambda_n}\sqrt{2\pi n}(\frac{n}{3})^n e^{\lambda_n}}=\sqrt{\frac{1}{\pi n}}2^{2n}e^{\lambda_{2n}-2\lambda_n}.$$

Όμως, για την ακολουθία $\{\lambda_n\}$, έχουμε

$$\lambda_{2n} - 2\lambda_n < \frac{1}{24n} - \frac{n}{12n+1} < 0 \Rightarrow e^{\lambda_{2n}-2\lambda_n} \leq 1.$$

Επομένως, αποδείξαμε την εκτίμηση

$$\binom{2n}{n} \leq \sqrt{\frac{1}{\pi n}} 2^{2n},$$

για κάθε $n \in \mathbb{N}$. Τώρα, το ερώτημα που τίθεται είναι αν ο τύπος του Stirling εφαρμόζεται στην δική μας περίπτωση για την εκτίμηση της ποσότητας $\binom{q-1}{[q/2]}$. Αν το q είναι περίττος, θα μπορούσε να εφαρμοστεί η παραπάνω εκτίμηση. Από την άλλη πλευρά, αν είχαμε το $\mathbb{F}_{2^m}$, δηλαδή το σώμα $\mathbb{F}_q$ ήταν χαρακτηριστικής 2, πάλι θα μπορούσε να εφαρμοστεί η παραπάνω εκτίμηση αφού

$$\binom{2^m-1}{[\frac{2^m-1}{2}]} = \frac{(2^m-1)!}{(2^{m-1}!)(2^{m-1}-1)} = \frac{2^{m-1}}{2^m}\binom{2^m}{2^{m-1}} = \frac{1}{2}\binom{2N}{N}.$$

Επομένως, ο τύπος του Stirling εφαρμόζεται και παίρνουμε

$$\binom{q-1}{[q/2]} \leq \sqrt{\frac{1}{\pi[\frac{q}{2}]}} 2^{q-1}. \tag{4.8}$$

Από τις (4.5),(4.6),(4.7) και (4.8), προκύπτει

$$\begin{aligned} |N-(q-1)!| &\leq \frac{q-1}{2q(q-1)^{\frac{q-1}{2}}} 2q \frac{1}{\sqrt{\pi[\frac{q}{2}]}} 2^{q-1} (\frac{q}{2})^{q-1} \\ &= \frac{q-1}{\sqrt{\pi[\frac{q}{2}]}} (\frac{q}{q-1})^{\frac{q-1}{2}} q^{\frac{q-1}{2}} \\ &= \frac{q-1}{\sqrt{\pi[\frac{q}{2}]q}} (\frac{q}{q-1})^{\frac{q-1}{2}} q^{\frac{q}{2}}. \end{aligned}$$

Τώρα, συνεχίζουμε τις εκτιμήσεις. Χρησιμοποιούμε την ταυτότητα

$$\frac{q-1}{\sqrt{q[\frac{q}{2}]}} < \sqrt{2}.$$

Αυτή αποδεικνύεται ως εξής:

- Αν ο q είναι άρτιος, $q^2 - 2q + 1 < q^2 \Rightarrow 2q > 1$.

- Αν ο q είναι περιττός, $q^2 - 2q + 1 < q^2 - q \Rightarrow q > 1$, η οποία ισχύει για κάθε $q > 2$.

Ακόμα,

$$\Big(\frac{q}{q-1}\Big)^{\frac{q-1}{2}} = \Big(\frac{q+1-1}{q-1}\Big)^{\frac{q-1}{2}} = \Big((1+\frac{1}{q-1})^{q-1}\Big)^{\frac{1}{2}} < \sqrt{e}.$$

Τέλος, αντικαθιστώντας τις εκτιμήσεις αυτές, παίρνουμε το τέλικο συμπέρασμα:

$$|N - (q-1)!| \leq \sqrt{2e/\pi} q^{q/2}.$$

□

Βιβλιογραφία

[1] Rudolf Lidl and Harald Niederreiter Rudolf Lidl and Harald Niederreiter, *Finite Fields*

[2] Amir Akbary and Qiang Wang, *On polynomials of the form* $x^r f(x^{(q-1)/l})$

[3] Daqing Wan, Rudolf Lidl *Permutation Polynomials of the Form* $x^r f(x^{(q-1)/d})$ *And Their Group Structure*

[4] Sergei Konyagin, Francesco Pappalardi *Enumerating Permutation Polynomials over Finite Fields by Degree*