Εφαρμογές του μετασχηματισμού **Fourier** στην Κωδικοποίηση

Μεταπτυχιακή εργασία
Στέλλα Φουρφουλάκη

Επιβλέπων Καθηγητής
Θεόδουλος Γαρεφαλάκης

Τμήμα Μαθηματικών και Εφαρμοσμένων Μαθηματικών
Πανεπιστήμιο Κρήτης

Η παρούσα μεταπτυχιακή εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος «Μαθηματικά και Εφαρμογές τους» στην κατεύθυνση Μαθηματικά της Πληροφορικής του Τμήματος Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης.

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον κ. Θεόδουλο Γαρεφαλάκη για τη βοήθεια και την ουσιαστική καθοδήγηση τόσο κατά τη συγγραφή της εν λόγω μεταπτυχιακής εργασίας όσο και καθ'όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

Επίσης ευχαριστώ τον κ. Θεμιστοκλή Μήτση και τον κ. Αλέξανδρο Κουβιδάκη για τη συμμετοχή τους στην επιτροπή αξιολόγησης και για τη συμβολή τους.

Περίληψη

Ο μετασχηματισμός Fourier είναι ένα χρηστικό μαθηματικό εργαλείο για τη μελέτη πολυάριθμων και σημαντικών εφαρμογών σε διαφόρους κλάδους των Θετικών Επιστημών. Στην εργασία αυτή θα δούμε κάποιες ενδιαφέρουσες εφαρμογές του μετασχηματισμού Fourier στη Θεωρία Κωδίκων. Ειδικότερα, θα ασχοληθούμε με την εφαρμογή του μετασχηματισμού Fourier στην απόδειξη των λεγόμενων Εξισώσεων MacWilliams, οι οποίες αποτελούν το σημαντικότερο εργαλείο που διαθέτουμε για τον υπολογισμό κατανομών βαρών γραμμικών κωδίκων.

Αρχικά αναφερόμαστε σε κάποιες βασικές έννοιες της Θεωρίας Γραμμικών Κωδίκων και εισάγουμε την έννοια του χαρακτήρα μιας πεπερασμένης Αβελιανής ομάδας με κάποιες βασικές ιδιότητες. Ακόμη, ορίζουμε το μετασχηματισμό Fourier πάνω σε μια πεπερασμένη Αβελιανή ομάδα και ειδικότερα στην προσθετική Αβελιανή ομάδα $\mathbb{F}_q^n$.

Στη συνέχεια, παρουσιάζουμε τέσσερις μορφές των εξισώσεων MacWilliams καθώς και την απόδειξή τους. Τέλος, αναφερόμαστε στο Φράγμα γραμμικού προγραμματισμού και βλέπουμε πώς από αυτό προκύπτουν άλλα γνωστά φράγματα της Θεωρίας Κωδίκων.

Περιεχόμενα

Κεφάλαιο 1

Γραμμικοί κώδικες

1.1 Ορισμός και Βασικές Ιδιότητες

Έστω p ένας πρώτος, $e \in \mathbb{N}$, $q = p^e$ και συμβολίζουμε με $\mathbb{F}_q$ το πεπερασμένο σώμα με q στοιχεία. Έστω $\mathbb{F}_q^n$ ο διανυσματικός χώρος όλων των διανυσμάτων μήκους n πάνω από το $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(v_1, \ldots, v_n) : v_i \in \mathbb{F}_q\}.$$

Θεωρούμε τα διανύσματα $v = (v_1, \ldots, v_n)$ και $u = (u_1, \ldots, u_n)$ του $\mathbb{F}_q^n$. Το σύνηθες εσωτερικό γινόμενο στο $\mathbb{F}_q^n$ ορίζεται με

$$\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i,$$

και ικανοποιεί τις ακόλουθες ιδιότητες: για κάθε $u, v, w \in \mathbb{F}_q^n$ και $\lambda \in \mathbb{F}_q$,
(i) $\langle u, v \rangle = \langle v, u \rangle$
(ii) $\langle \lambda u + w, v \rangle = \lambda \langle u, v \rangle + \langle w, v \rangle$
(iii) Αν $\langle u, v \rangle = 0$ για κάθε $v \in \mathbb{F}_q^n$, τότε $u = 0$.

Ορισμός 1.1.1. *Ένας γραμμικός κώδικας C μήκους n πάνω από το $\mathbb{F}_q$ είναι ένας υπόχωρος του $\mathbb{F}_q^n$.*

Ορισμός 1.1.2. *Έστω C ένας γραμμικός κώδικας στο $\mathbb{F}_q^n$.*
(i) *Ο δυϊκός κώδικας του C είναι το ορθογώνιο συμπλήρωμα $C^\perp$ του υποχώρου C του $\mathbb{F}_q^n$, που ορίζεται ως*

$$C^\perp = \{v \in \mathbb{F}_q^n : \langle v, c \rangle = 0, \forall c \in C\}.$$

(ii) *Η διάσταση του γραμμικού κώδικα C είναι η διάσταση του C ως διανυσματικού χώρου πάνω από το $\mathbb{F}_q$.*

Θεώρημα 1.1.3. *Έστω C ένας γραμμικός κώδικας μήκους n πάνω από το $\mathbb{F}_q$. Τότε,*

(i) $|C| = q^{\dim(C)}$, *δηλαδή* $\dim(C) = \log_q|C|$.
(ii) $C^\perp$ *είναι ένας γραμμικός κώδικας και* $\dim(C) + \dim(C^\perp) = n$.
(iii) $(C^\perp)^\perp = C$.

Παρατήρηση 1.1.4. *Ένας γραμμικός κώδικας C μήκους n και διάστασης k πάνω από το $\mathbb{F}_q$ ονομάζεται $[n,k]-$κώδικας πάνω από το $\mathbb{F}_q$.*

Ορισμός 1.1.5. *Έστω C ένας γραμμικός κώδικας.*
(i) *C είναι αυτοορθογώνιος αν $C \subseteq C^\perp$.*
(ii) *C είναι αυτοδυϊκός αν $C = C^\perp$.*

1.2 Βάρη και αποστάσεις

Ορισμός 1.2.1. *Έστω $x, y \in \mathbb{F}_q^n$. Η απόσταση (Hamming) από το x στο y, που συμβολίζεται με $d(x,y)$, ορίζεται ως ο αριθμός των συντεταγμένων στις οποίες διαφέρουν τα x και y. Αν $x = x_1 \cdots x_n$ και $y = y_1 \cdots y_n$, τότε*

$$d(x,y) = d(x_1,y_1) + \cdots + d(x_n,y_n), \tag{1.1}$$

όπου θεωρούμε τα x_i και y_i λέξεις μήκους 1, και

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

Πρόταση 1.2.2. *Έστω $x, y, z \in \mathbb{F}_q^n$. Τότε έχουμε*
(i) $0 \leq d(x,y) \leq n$,
(ii) $d(x,y) = 0$ *αν και μόνο αν* $x = y$,
(iii) $d(x,y) = d(y,x)$,
(iv) *(Τριγωνική ανισότητα.)* $d(x,z) \leq d(x,y) + d(y,z)$.

Εκτός από το μήκος και τη διάσταση ενός κώδικα, ένα άλλο σημαντικό και χρήσιμο χαρακτηριστικό είναι η απόσταση του κώδικα.

Ορισμός 1.2.3. *Για ένα κώδικα C που περιέχει τουλάχιστον δυο λέξεις, η (ελάχιστη) απόσταση του C, που συμβολίζεται με $d(C)$, είναι*

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

Παρατήρηση 1.2.4. *Αν η απόσταση d ενός $[n,k]-$κώδικα πάνω από το $\mathbb{F}_q$ είναι γνωστή, τότε αναφέρεται ως $[n,k,d]-$κώδικας.*

Ορισμός 1.2.5. *Έστω $x \in \mathbb{F}_q^n$. Το βάρος (Hamming) του x, που συμβολίζεται με $\mathrm{wt}(x)$, ορίζεται ως ο αριθμός των μη μηδενικών συντεταγμένων του x, δηλαδή*

$$\mathrm{wt}(x) = d(x,0),$$

όπου 0 είναι η μηδενική λέξη.

Παρατήρηση 1.2.6. *Για κάθε στοιχείο $a \in \mathbb{F}_q$, μπορούμε να ορίσουμε το βάρος Hamming ως εξής:*

$$\mathrm{wt}(a) = d(a,0) = \begin{cases} 1 & \text{αν } a \neq 0 \\ 0 & \text{αν } a = 0. \end{cases}$$

Τότε, γράφοντας το $x \in \mathbb{F}_q^n$ ως $x = (x_1, x_2, \ldots, x_n)$, το βάρος (Hamming) του x μπορεί να οριστεί ισοδύναμα ως

$$\mathrm{wt}(x) = \mathrm{wt}(x_1) + \mathrm{wt}(x_2) + \cdots + \mathrm{wt}(x_n). \tag{1.2}$$

Λήμμα 1.2.7. *Αν $x, y \in \mathbb{F}_q^n$, τότε $d(x,y) = \mathrm{wt}(x-y)$.*

Απόδειξη. Για $x_1, y_1 \in \mathbb{F}_q$, $d(x_1, y_1) = 0$ αν και μόνο αν $x_1 = y_1$, που ισχύει αν και μόνο αν $x_1 - y_1 = 0$ ή, ισοδύναμα, $\mathrm{wt}(x_1 - y_1) = 0$. Από (1.1) και (1.2) έχουμε το ζητούμενο. □

Ορισμός 1.2.8. *Έστω C ένας γραμμικός κώδικας πάνω από το $\mathbb{F}_q$. Το ελάχιστο βάρος (Hamming) του C, που συμβολίζεται με $\mathrm{wt}(C)$, είναι το μικρότερο από τα βάρη των μη μηδενικών λέξεων του C.*

Θεώρημα 1.2.9. *Έστω C ένας γραμμικός κώδικας πάνω από το $\mathbb{F}_q$. Τότε $d(C) = \mathrm{wt}(C)$.*

Απόδειξη. Υπενθυμίζουμε ότι για οποιεσδήποτε λέξεις x, y έχουμε $d(x,y) = \mathrm{wt}(x-y)$. Εξόρισμού,υπάρχουν $x', y' \in C$ τέτοια ώστε $d(x', y') = d(C)$, οπότε

$$d(C) = d(x', y') = \mathrm{wt}(x' - y') \geq \mathrm{wt}(C),$$

αφού $x' - y' \in C$.
Αντίστροφα, υπάρχει κάποιο $z \in C \setminus \{0\}$ τέτοιο ώστε $\mathrm{wt}(C) = \mathrm{wt}(z)$, οπότε

$$\mathrm{wt}(C) = \mathrm{wt}(z) = d(z,0) \geq d(C).$$

□

Έστω $A_i(C)$ ο αριθμός των λέξεων βάρους i σε έναν κώδικα C μήκους n. Η λίστα $A_i(C)$ για $0 \leq i \leq n$ ονομάζεται κατανομή βαρών του C και προσδιορίζει τον αριθμό των λέξεων κάθε πιθανού βάρους $0, 1, \ldots, n$. Εάν ο κώδικας είναι γνωστός, συμβολίζουμε την κατανομή βαρών του με $A_i = A_i(C)$ για $0 \leq i \leq n$ και την κατανομή βαρών του $C^\perp$ με $A_i^\perp = A_i(C^\perp)$ για $0 \leq i \leq n$. Επειδή σε έναν κώδικα για πολλές τιμές του i ισχύει $A_i(C) = 0$, οι τιμές αυτές συνήθως παραλείπονται από τη λίστα.

Θεώρημα 1.2.10. *Έστω C ένας $[n,k,d]$-κώδικας πάνω από το $\mathbb{F}_q$. Τότε*

(i) $\sum_{i=0}^{n} A_i = q^k$.
(ii) $A_0(C) = 1$ *και* $A_i(C) = 0$ *για* $1 \leq i < d$.

Έστω C ένας $[n,k,d]$ κώδικας πάνω από το $\mathbb{F}_q$ με κατανομή βαρών A_i για $0 \leq i \leq n$. Θεωρούμε το πολυώνυμο μιας μεταβλητής που παράγεται από την κατανομή βαρών του κώδικα. Το πολυώνυμο αυτό ονομάζεται απαριθμητής βαρών του κώδικα C και ορίζεται ως

$$W_C(x) = \sum_{i=0}^{n} A_i x^i.$$

Παρατηρούμε ότι $W_C(0) = A_0(C) = 1$ και $W_C(1) = \sum_{i=0}^{n} A_i = q^k$.
Ο απαριθμητής βαρών δεν καθορίζει τον κώδικα, δηλαδή είναι δυνατό να έχουμε διαφορετικούς κώδικες με ίδιο απαριθμητή βαρών, όπως θα δούμε στην επόμενη ενότητα (Παράδειγμα 1.3.4).

1.3 Πίνακας βάσης και πίνακας ελέγχου

Αφού ένας γραμμικός κώδικας είναι ένας διανυσματικός χώρος, όλα τα στοιχεία του μπορούν να γραφτούν ως προς μια βάση. Γνωρίζοντας μια βάση του κώδικα μπορούμε να περιγράψουμε όλες τις λέξεις του αναλυτικά. Στη θεωρία κωδίκων, μια βάση για ένα γραμμικό κώδικα παριστάνεται συχνά στη μορφή ενός πίνακα, που ονομάζεται πίνακας βάσης, ενώ ένας πίνακας που αναπαριστά μια βάση για τον δυϊκό κώδικα ονομάζεται πίνακας ελέγχου. Αυτοί οι πίνακες παίζουν σημαντικό ρόλο στη θεωρία κωδίκων.

Ορισμός 1.3.1. (i) *Ένας πίνακας βάσης για ένα γραμμικό κώδικα C είναι ένας πίνακας G που οι γραμμές του αποτελούν μια βάση για τον C.*
(ii) *Ένας πίνακας ελέγχου H για ένα γραμμικό κώδικα C είναι ένας πίνακας βάσης για το $C^{\perp}$.*

Παρατήρηση 1.3.2. (i) *Αν C είναι ένας $[n,k]-$κώδικας, τότε ένας πίνακας βάσης για τον C πρέπει να είναι ένας $k \times n$ πίνακας και ένας πίνακας ελέγχου για τον C πρέπει να είναι ένας $(n-k) \times n$ πίνακας.*
(ii) *Καθώς ένας διανυσματικός χώρος συνήθως έχει παραπάνω από μια βάση, οι πίνακες βάσεις για ένα γραμμικό κώδικα είναι συνήθως παραπάνω από ένας.Επιπλέον, ακόμη και αν η βάση είναι καθορισμένη, μια μετάθεση των γραμμών του πίνακα βάσης οδηγεί επίσης σε ένα διαφορετικό πίνακα βάσης.*

Πρόταση 1.3.3. *Έστω C ένας γραμμικός κώδικας με πίνακα ελέγχου H. Τα ακόλουθα είναι ισοδύναμα:*
(i) *Ο C έχει απόσταση d.*
(ii) *Κάθε $d-1$ στήλες του H είναι γραμμικά ανεξάρτητες και ο H έχει d στήλες που είναι γραμμικά εξαρτημένες.*

Παράδειγμα 1.3.4. *Έστω C_1 και C_2 οι $[6,3]$ δυαδικοί κώδικές με πίνακες βάσης G_1 και G_2, αντίστοιχα, όπου*

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{ και } G_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Οπότε $C_1 =< 110000, 001100, 000011 >= \{000000, 110000, 001100, 000011, 111100, 110011, 001111, 111111\}$ *και* $C_2 =< 110000, 011000, 111111 >= \{000000, 110000, 011000, 111111, 101000, 001111, 100111, 010111\}$.
Διαπιστώνουμε ότι οι δυο κώδικες έχουν ελάχιστη απόσταση 2 *και την ίδια κατανομή βαρών* $A_0 = 1$, $A_2 = 3$, $A_4 = 3$ *και* $A_6 = 1$ *, ενώ δεν είναι ίσοι.*
Επομένως $W_{C_1}(x) = W_{C_2}(x) = x^6 + 3x^4 + 3x^2 + 1$.

1.4 Κώδικες Hamming

Έστω $q \geq 2$ μια δύναμη πρώτου. Σημειώνουμε ότι οποιοδήποτε μη μηδενικό $v \in \mathbb{F}_q^r$ παράγει έναν υπόχωρο $< v >$ διάστασης 1. Επιπλέον, για $v, w \in \mathbb{F}_q^r \backslash \{0\}$, $< v >=< w >$ αν και μόνο αν υπάρχει $\lambda \in \mathbb{F}_q \backslash \{0\}$ τέτοιο ώστε $v = \lambda w$. Επομένως, υπάρχουν ακριβώς $(q^r - 1)/(q - 1)$ υπόχωροι διάστασης 1 στο $\mathbb{F}_q^r$.

Ορισμός 1.4.1. *Έστω* $r \geq 2$. *Ένας γραμμικός κώδικας πάνω από το* $\mathbb{F}_q$, *με πίνακα ελέγχου* H *τέτοιο ώστε οι στήλες του αποτελούνται από ακριβώς ένα μη μηδενικό διάνυσμα από κάθε υπόχωρο διάστασης* 1 *του* $\mathbb{F}_q^r$, *ονομάζεται κώδικας Hamming και συμβολίζεται με* $Ham(r, q)$.

Πρόταση 1.4.2. *Ο* $Ham(r, q)$ *είναι ένας* $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3]-$*κώδικας.*

Απόδειξη. Αφού ο πίνακας ελέγχου H του $\mathrm{Ham}(r, q)$ είναι ένας $r \times (q^r - 1)/(q - 1)$ πίνακας, η διάσταση του $\mathrm{Ham}(r, q)$ είναι $(q^r - 1)/(q - 1) - r$ και έχει μήκος $(q^r - 1)/(q - 1)$.

Αφού οι στήλες του H ανά δυο ανήκουν σε διαφορετικούς υπόχωρους διάστασης 1 του $\mathbb{F}_q^r$, οποιεσδήποτε δυο στήλες του H είναι γραμμικά ανεξάρτητες. Από την άλλη, ο H περιέχει τις στήλες $(\lambda_1 00 \ldots 0)^T$, $(0\lambda_2 0 \ldots 0)^T$ και $(\mu_1 \mu_2 0 \ldots 0)^T$, όπου $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{F}_q^*$, οι οποίες είναι ένα γραμμικά εξαρτημένο σύνολο. Οπότε, η απόσταση του $\mathrm{Ham}(r, q)$ είναι ίση με 3. □

Ορισμός 1.4.3. *Ο δυϊκός ενός κώδικα Hamming* $Ham(r, q)$ *ονομάζεται κώδικας simplex και συμβολίζεται με* $S(r, q)$.

Πρόταση 1.4.4. *Ο* $S(r, q)$ *είναι ένας* $[(q^r - 1)/(q - 1), r, q^{r-1}]-$*κώδικας.*

Απόδειξη. Αφού ο πίνακας βάσης του $\mathrm{S}(r, q)$ είναι ένας $r \times (q^r - 1)/(q - 1)$ πίνακας (ο πίνακας ελέγχου H του $\mathrm{Ham}(r, q)$), η διάσταση του $\mathrm{S}(r, q)$ είναι r και έχει μήκος $(q^r - 1)/(q - 1)$.

Παρατηρούμε ότι $\mathrm{S}(r, q) = \{vH : v \in \mathbb{F}_q^r\}$, οπότε για να υπολογίσουμε το βάρος του vH πρέπει να βρούμε πόσα από τα $< v, h_i >= 0$, όπου h_i η i-στήλη του H. Έστω λοιπόν ένα μη μηδενικό διάνυσμα $v \in \mathbb{F}_q^r$ και $\{v\}^\perp$ το σύνολο των διανυσμάτων του $\mathbb{F}_q^r$ που είναι κάθετα στο v. Είναι εύκολο να επαληθεύσουμε ότι $\{v\}^\perp$ είναι ένας υπόχωρος του $\mathbb{F}_q^r$ και ότι $< v >^\perp = \{v\}^\perp$. Τότε έχουμε

$$\dim(< v >) + \dim(< v >^\perp) = r,$$

επομένως $\dim(< v >^{\perp}) = r - \dim(< v >) = r - 1$. Θέτουμε $S = \{v\}^{\perp}$. Αφού $\dim(S) = r - 1$, το S έχει q^{r-1} στοιχεία. Οπότε υπάρχουν $q^{r-1} - 1$ μη μηδενικά διανύσματα του $\mathbb{F}_q^r$ που είναι κάθετα στο v. Χωρίζουμε αυτά τα διανύσματα σε κλάσεις. Στο σύνολο $S \setminus \{0\}$ θεωρούμε τη σχέση ισοδυναμίας

$$u \sim w \Leftrightarrow u = \lambda w, \lambda \in \mathbb{F}_q^*.$$

Η κλάση ισοδυναμίας του $u \in S\setminus\{0\}$ είναι $[u] = \{\lambda u : \lambda \in \mathbb{F}_q^*\}$. Οπότε $|[u]| = q-1$ και

$$S \setminus \{0\} = \bigcup [u]$$

ή

$$q^{r-1} - 1 = A(q-1),$$

άρα $A = (q^{r-1} - 1)/(q-1)$. Από την κατασκευή του πίνακα ελέγχου H του $\mathrm{Ham}(r, q)$, έπεται ότι υπάρχουν ακριβώς $(q^{r-1}-1)/(q-1)$ στήλες του H κάθετες στο v. Επομένως το πλήθος των μη μηδενικών συντεταγμένων του vH είναι $(q^r-1)/(q-1) - (q^{r-1}-1)/(q-1) = q^{r-1}$. Οπότε, η απόσταση του $\mathrm{S}(r, q)$ είναι ίση με q^{r-1}. □

1.5 Φράγματα

Ορισμός 1.5.1. *Για δοσμένο q και θετικούς ακέραιους n και d, έστω $B_q(n, d)$ συμβολίζει το μεγαλύτερο δυνατό μέγεθος q^k για το οποίο υπάρχει ένας $[n, k, d]-$κώδικας πάνω από το $\mathbb{F}_q$. Συνεπώς,*

$B_q(n, d) = max\{q^k : \exists [n, k, d]-$ *κώδικας πάνω από το* $\mathbb{F}_q\}$.

Ακολουθεί ένα άνω φράγμα για το $B_q(n, d)$ που οφείλεται στο Singleton.

Θεώρημα 1.5.2. *(Φράγμα του Singleton.) Για οποιαδήποτε δύναμη πρώτου q και θετικούς ακέραιους n και d τέτοιους ώστε $1 \leq d \leq n$, έχουμε*

$$B_q(n, d) \leq q^{n-d+1}.$$

Το επόμενο άνω φράγμα για το $B_q(n, d)$ είναι το φράγμα του Plotkin, το οποίο ισχύει για κώδικες με μεγάλο d σε σχέση με το n.

Θεώρημα 1.5.3. *(Φράγμα του Plotkin.) Έστω δύναμη πρώτου q και υποθέτουμε ότι οι θετικοί ακέραιοι n, d ικανοποιούν $rn < d$, όπου $r = 1 - q^{-1}$. Τότε,*

$$B_q(n, d) \leq \left\lfloor \frac{d}{d - rn} \right\rfloor.$$

Η απόδειξη των φραγμάτων του Singleton και του Plotkin θα προκύψει ως ειδική περίπτωση του φράγματος γραμμικού προγραμματισμού (Παράδειγμα 4.3.4).

Κεφάλαιο 2

Χαρακτήρες πεπερασμένων ομάδων

2.1 Αποτελέσματα από Θεωρία Ομάδων

Παρουσιάζουμε μερικά αποτελέσματα από τη θεωρία ομάδων που θα χρησιμοποιήσουμε, στη συνέχεια, στη θεωρία των χαρακτήρων πεπερασμένων Αβελιανών ομάδων.

Έστω $\mathbb{Z}$ η ομάδα των ακεραίων με πράξη την πρόσθεση και, για ένα θετικό ακέραιο n, έστω $\mathbb{Z}_n$ η ομάδα των ακεραίων modulo n με πράξη την πρόσθεση modulo n. Χρησιμοποιούμε την προσθετική γραφή για τις πράξεις σε αυτές τις δυο ομάδες. Τα ταυτοτικά στοιχεία των $\mathbb{Z}$ και $\mathbb{Z}_n$ συμβολίζονται και τα δυο με 0 και το αντίστροφο του $k \in \mathbb{Z}$ ή $k \in \mathbb{Z}_n$ με $-k$.

Γενικά, χρησιμοποιούμε την πολλαπλασιαστική γραφή για την πράξη μιας ομάδας: δηλαδή αν G είναι μια ομάδα και a και b είναι στοιχεία της G, τότε ab συμβολίζει το γινόμενο των a και b, που ορίζεται σύμφωνα με την πράξη στην G. Το ταυτοτικό στοιχείο της G συμβολίζεται με 1 και το αντίστροφο του $g \in G$ συμβολίζεται με g^{-1}.

Σε οποιαδήποτε ομάδα G, η εξίσωση $xg = xg'$ είναι ισοδύναμη με την $g = g'$ (νόμος διαγραφής). Αυτή η απλή ιδιότητα οδηγεί στο ακόλουθο θεώρημα.

Θεώρημα 2.1.1. *Υποθέτουμε ότι G είναι μια πεπερασμένη ομάδα και x είναι ένα στοιχείο της G. Η συνάρτηση $f_x : G \to G$ που ορίζεται με $f_x(g) = xg$ είναι μια μετάθεση της G.*

Έστω G_1 και G_2 ομάδες. Μια απεικόνιση $h : G_1 \to G_2$ ονομάζεται ομομορφισμός αν $h(ab) = h(a)h(b)$ για κάθε $a, b \in G_1$. Εδώ, το ab είναι γινόμενο στοιχείων στην G_1, ενώ το $h(a)h(b)$ είναι γινόμενο στοιχείων στην G_2. Ένας ομομορφισμός ονομάζεται ισομορφισμός αν είναι 1-1 και επί απεικόνιση. Χρησιμοποιούμε την έκφραση $G_1 \cong G_2$ για να δείξουμε ότι δυο ομάδες G_1 και G_2 είναι ισόμορφες. Υπάρχουν, μέχρι ισομορφισμού, μόνο μια άπειρη κυκλική ομάδα και μια πεπερασμένη κυκλική τάξης n, οι $\mathbb{Z}$ και $\mathbb{Z}_n$, αντίστοιχα.

Θεώρημα 2.1.2. *Υποθέτουμε ότι η G είναι μια κυκλική ομάδα. Τότε*
(i) *$G \cong \mathbb{Z}$ αν η G είναι άπειρη,*
(ii) *$G \cong \mathbb{Z}_n$ αν η G είναι πεπερασμένη και $n = |G|$.*

Αν $G_1, \ldots, G_m$ είναι ομάδες και

$$G = G_1 \times \cdots \times G_m = \{(g_1, \ldots, g_m) : g_j \in G_j\},$$

τότε η G είναι μια ομάδα ως προς την πράξη που ορίζεται με

$$(g_1, \ldots, g_m)(g_1', \ldots, g_m') = (g_1 g_1', \ldots, g_m g_m'),$$

όπου $g_j g_j'$ είναι το γινόμενο που ορίζεται στην G_j για $j = 1, \ldots, m$. Το ταυτοτικό στοιχείο για αυτήν την πράξη είναι το $(1, \ldots, 1)$, που συμβολίζεται απλά με 1. Το αντίστροφο του $(g_1, \ldots, g_m)$, που συμβολιζεται με $(g_1, \ldots, g_m)^{-1}$, δίνεται από $(g_1^{-1}, \ldots, g_m^{-1})$. Η ομάδα G ως προς την πράξη που ορίσαμε παραπάνω ονομάζεται ευθύ εξωτερικό γινόμενο των $G_1, \ldots, G_m$. Αν $G_j = A$ για κάθε j, τότε γράφουμε $G = A^m$. Αν οι εμπλεκόμενες ομάδες γράφονται προσθετικά, όπως για παράδειγμα οι $\mathbb{Z}$ και $\mathbb{Z}_n$, τότε η γραφή της πράξης, του ουδέτερου στοιχείου και των αντιστρόφων τροποποιούνται κατά τον προφανή τρόπο.

Θεώρημα 2.1.3. (Το Θεμελιώδες Θεώρημα των πεπερασμένων Αβελιανών ομάδων). *Αν η G είναι μια μη τετριμμένη πεπερασμένη Αβελιανή ομάδα (έχει περισσότερα από ένα στοιχεία), τότε υπάρχουν μοναδικοί θετικοί ακέραιοι s και $n_1, \ldots, n_s$, όπου κάθε $n_j \geq 2$, τέτοιοι ώστε $n_j | n_{j+1}$ για $j = 1, \ldots, s-1$ και*

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}.$$

2.2 Ορισμός και Βασικές Ιδιότητες Χαρακτήρων

Ορισμός 2.2.1. *Ένας χαρακτήρας μιας ομάδας G είναι ένας ομομορφισμός χ από τη G στην ομάδα $\mathbb{C}^*$. Δηλαδή, ένας χαρακτήρας της G είναι μια απεικόνιση $\chi : G \to \mathbb{C}^*$ τέτοια ώστε $\chi(ab) = \chi(a)\chi(b)$ για κάθε $a, b \in G$. Ένας χαρακτήρας χ ονομάζεται τετριμμένος αν $\chi(g) = 1$ για κάθε $g \in G$.*

Από τον προηγούμενο ορισμό έπεται ότι: (1) κάθε ομάδα έχει ένα χαρακτήρα, τον τετριμμένο χαρακτήρα, ο οποίος συμβολίζεται με χ_T. (2) Κάθε χαρακτήρας απεικονίζει το ταυτοτικό στοιχείο της G στο 1.

Έστω χ και χ' χαρακτήρες της G. Το γινόμενο (κατά σημείο) των χ και χ' είναι η συνάρτηση $\chi\chi' : G \to \mathbb{C}^*$ που ορίζεται με $\chi\chi'(g) = \chi(g)\chi'(g)$.

Θεώρημα 2.2.2. *Το σύνολο των χαρακτήρων μιας ομάδας G είναι μια Αβελιανή ομάδα ως προς το γινόμενο κατά σημείο.*

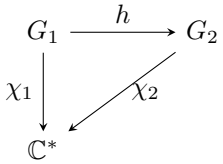
Η ομάδα των χαρακτήρων της G συμβολίζεται με $\hat{G}$ και ονομάζεται ομάδα χαρακτήρων ή δυϊκή ομάδα της G.

Υποθέτουμε ότι $h : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων και χ είναι ένας χαρακτήρας της G_2. Το *pullback* του χ από h, που συμβολίζεται $h^\star\chi$, ορίζεται ως

$h^\star\chi = \chi \circ h$, η σύνθεση των χ και h. Επειδή η σύνθεση δυο ομομορφισμών είναι ομομορφισμός, έπεται ότι το pullback ενός χαρακτήρα της G_2 είναι χαρακτήρας της G_1.

Θεώρημα 2.2.3. *Ισόμορφες ομάδες έχουν ισόμορφες ομάδες χαρακτήρων. Δηλαδή, αν G_1 και G_2 είναι ομάδες και $G_1 \cong G_2$, τότε $\hat{G_1} \cong \hat{G_2}$.*

Απόδειξη. Υποθέτουμε ότι $h : G_1 \to G_2$ είναι ένας ισομορφισμός ομάδων και χ_2 είναι ένας χαρακτήρας της G_2. Θεωρούμε το διάγραμμα



Παρατηρούμε ότι το pullback $\chi_2 \circ h$ της χ_2 είναι χαρακτήρας της G_1. Αντίστροφα, κάθε χαρακτήρας της G_1 είναι ένα pullback κάποιου χαρακτήρα χ_2 της G_2 (θέτουμε $\chi_2 = \chi_1 \circ h^{-1}$). Έτσι η συνάρτηση $h^\star : \hat{G_2} \to \hat{G_1}$ είναι επί. Τώρα θα δείξουμε ότι $h^\star$ είναι ένας ισομορφισμός:

1. Ομομορφισμός: Αν $\chi_2, \chi_2' \in \hat{G_2}$, τότε, από τον ορισμό κατά σημείο,
$$h^\star(\chi_2\chi_2') = (h^\star\chi_2)(h^\star\chi_2').$$
Πράγματι, για κάθε $g \in G_1$ ισχύει
$$h^\star(\chi_2\chi_2')(g) = (\chi_2\chi_2') \circ h(g) = \chi_2\chi_2'(h(g)) = \chi_2(h(g))\chi_2'(h(g))$$
$$= h^\star\chi_2(g)h^\star\chi_2'(g) = (h^\star\chi_2)(h^\star\chi_2')(g).$$
2. $ker(h^\star) = \{\chi_{T_2}\}$: Για $j = 1, 2$, έστω χ_{T_j} ο τετριμένος χαρακτήρας της G_j. Αν $h^\star\chi_2 = \chi_{T_1}$, τότε $\chi_2 \circ h(g_1) = 1$ για κάθε $g_1 \in G_1$. Επειδή η h είναι 1-1 και επί, προκύπτει ότι $\chi_2 = \chi_{T_2}$. □

Υποθέτουμε τώρα ότι G_1 και G_2 είναι ομάδες και χ_1 και χ_2 είναι χαρακτήρες των G_1 και G_2, αντίστοιχα. Το τανυστικό γινόμενο των χ_1 και χ_2 είναι η συνάρτηση $\chi_1 \otimes \chi_2$: $G_1 \times G_2 \to \mathbb{C}^*$ που ορίζεται με

$$\chi_1 \otimes \chi_2(g_1, g_2) = \chi_1(g_1)\chi_2(g_2). \tag{2.1}$$

Υπάρχουν δυο άμεσες συνέπειες του παραπάνω ορισμού:

(i) Το τανυστικό γινόμενο δεν είναι αντιμεταθετικό. Γενικά, $\chi_1 \otimes \chi_2$ και $\chi_2 \otimes \chi_1$ έχουν διαφορετικά πεδία ορισμού.
(ii) Από τον ορισμό της πράξης της ομάδας $G_1 \times G_2$, τον ορισμό του $\chi_1 \otimes \chi_2$

και την αντιμεταθετικότητα του γινομένου των μιγαδικών αριθμών έπεται ότι το τανυστικό γινόμενο $\chi_1 \otimes \chi_2$ είναι χαρακτήρας της $G_1 \times G_2$.
Κάθε χαρακτήρας της $G_1 \times G_2$ είναι της μορφής $\chi_1 \otimes \chi_2$, όπως αποδεικνύεται στο επόμενο θεώρημα.

Θεώρημα 2.2.4. *Έστω G_1 και G_2 ομάδες. Τότε χ είναι χαρακτήρας της $G_1 \times G_2$ αν και μόνο αν $\chi = \chi_1 \otimes \chi_2$, για κάποιο $\chi_1 \in \hat{G_1}$ και $\chi_2 \in \hat{G_2}$.*

Απόδειξη. Έστω $\chi = \chi_1 \otimes \chi_2$, για κάποιο $\chi_1 \in \hat{G_1}$ και $\chi_2 \in \hat{G_2}$ και (g_1, g_2), $(g_1', g_2') \in G_1 \times G_2$. Τότε

$$\chi_1 \otimes \chi_2(g_1 g_1', g_2 g_2') = \chi_1(g_1 g_1')\chi_2(g_2 g_2') = \chi_1(g_1)\chi_2(g_2)\chi_1(g_1')\chi_2(g_2')$$
$$= \chi_1 \otimes \chi_2(g_1, g_2)\chi_1 \otimes \chi_2(g_1', g_2').$$

Άρα χ είναι ένας χαρακτήρας της $G_1 \times G_2$. Απομένει να δείξουμε ότι αν χ είναι ένας χαρακτήρας της $G_1 \times G_2$, τότε υπάρχουν χαρακτήρες χ_1 της G_1 και χ_2 της G_2 τέτοιοι ώστε $\chi = \chi_1 \otimes \chi_2$. Επειδή η εμφύτευση $\imath_1 : G_1 \hookrightarrow G_1 \times G_2$ που δίνεται από $\imath_1(g_1) = (g_1, 1)$ είναι ομομορφισμός, το pullback του χ από $\imath_1$ είναι ένας χαρακτήρας της G_1. Ομοίως, το pullback του χ από $\imath_2$ είναι ένας χαρακτήρας της G_2. Είναι άμεσο να ελέγξουμε ότι αν $\chi_1 = \imath_1^\star \chi$ και $\chi_2 = \imath_2^\star \chi$, τότε $\chi = \chi_1 \otimes \chi_2$. □

Πόρισμα 2.2.5. *Αν G_1 και G_2 είναι ομάδες, τότε*

$$\widehat{G_1 \times G_2} = \hat{G_1} \otimes \hat{G_2},$$

όπου $\hat{G_1} \otimes \hat{G_2} = \{\chi_1 \otimes \chi_2 \mid \chi_1 \in \hat{G_1}$ και $\chi_2 \in \hat{G_2}\}$.

Πρόταση 2.2.6. *Αν G_1 και G_2 είναι ομάδες, τότε*

$$\hat{G_1} \times \hat{G_2} \cong \hat{G_1} \otimes \hat{G_2}.$$

Στη συνέχεια ορίζουμε το συζυγή ενός χαρακτήρα, ο οποίος είναι επίσης χαρακτήρας και μάλιστα, για πεπερασμένες ομάδες, ο συζυγής ενός χαρακτήρα είναι ακριβώς ο αντίστροφός του, όπως θα δούμε παρακάτω. Για οποιοδήποτε χαρακτήρα χ της G, ο συζυγής του χ, συμβολίζεται με $\bar{\chi}$ και ορίζεται ως $\bar{\chi}(g) = \chi(g)$ για κάθε $g \in G$.

Υποθέτουμε ότι χ είναι ένας χαρακτήρας της G και g είναι ένα στοιχείο της G πεπερασμένης τάξης k. Επειδή $\chi(g)^k = \chi(g^k) = \chi(1) = 1$, έπεται ότι οι χαρακτήρες στέλνουν στοιχεία πεπερασμένης τάξης σε ρίζες της μονάδας. Συγκεκριμένα, αν G είναι μια πεπερασμένη ομάδα και n είναι ο μικρότερος θετικός ακέραιος τέτοιος ώστε $g^n = 1$ για κάθε $g \in G$, τότε τα στοχεία της G απεικονίζονται σε n-οστές ρίζες της μονάδας μέσω των χαρακτήρων. Σε αυτήν την περίπτωση, το $\mathbb{C}^*$ στον ορισμό των χαρακτήρων μπορεί να αντικατασταθεί από το σύνολο $U_n = \{\xi_n^k \mid \xi_n = e^{2\pi i/n}, 0 \leq k < n\}$ που αποτελείται από όλες τις n-οστές ρίζες της μονάδας και είναι κυκλική υποομάδα του $\mathbb{C}^*$ με γεννήτορα το ξ_n. Επομένως, αν $\chi \in \hat{G}$, τότε $|\chi(g)| = 1$ για κάθε $g \in G$. Έτσι,

$$\bar{\chi}(g) = \overline{\chi(g)} = \frac{1}{\chi(g)} = \chi(g^{-1}) = \chi^{-1}(g),$$

που δίνει

$$\bar{\chi} = \chi^{-1}. \tag{2.2}$$

Τονίζουμε ότι η εξίσωση (2.2) είναι συνέπεια της ύπαρξης ενός θετικού ακέραιου n τέτοιου ώστε $g^n = 1$ για κάθε $g \in G$. Ο μικρότερος από αυτούς ονομάζεται εκθέτης της G και συμβολίζεται με $exp(G)$. Αν η G είναι πεπερασμένη ομάδα, τότε υπάρχει πάντα ο εκθέτης και μάλιστα είναι διαιρέτης της τάξης της G. Έστω $exp(G) = k$ και $G = \{g_1, \ldots, g_n\}$, οπότε $|G| = n$. Πράγματι, αφού G πεπερασμένη, ισχύει $ord(g_i)|n$ και $g_i^n = 1$, για $i = 1, \ldots, n$. Οπότε θα είναι $k \leq n$ και n κοινό πολλαπλάσιο των $ord(g_1), \ldots, ord(g_n)$. Από υπόθεση $g_i^k = 1$, οπότε $ord(g_i)|k$. Άρα και το k είναι κοινό πολλαπλάσιο των $ord(g_1), \ldots, ord(g_n)$ και είναι ο μικρότερος θετικός ακέραιος τ.ω. $g^k = 1$. Επομένως $k = lcm(ord(g_1), \ldots, ord(g_n))$. Οπότε $k|n$.

Το Θεώρημα 2.1.3, το Θεωρήμα 2.2.3 και το Πόρισμα 2.2.5 περιορίζουν τη μελέτη των χαρακτήρων πεπερασμένων Αβελιανών ομάδων στη μελέτη των χαρακτήρων κυκλικών ομάδων πεπερασμένης τάξης. Έτσι, θα επικεντρωθούμε σε χαρακτήρες ομάδων του τελευταίου τύπου.

Οι χαρακτήρες της U_n είναι εύκολο να βρεθούν. Υποθέτουμε ότι το g είναι ένας γεννήτορας της U_n και $h : U_n \to U_n$ είναι ένας ομομορφισμός. Αν το $h(g)$ είναι γνωστό, τότε, επειδή $h(g)^k = h(g^k)$, το $h(g^k)$ είναι καθορισμένο, επομένως και το $h(u)$ είναι καθορισμένο για κάθε $u \in U_n$. Έτσι, μια επιλογή για το $h(g)$ καθορίζει την h μοναδικά. Επειδή η ομάδα U_n έχει n στοιχεία, υπάρχουν n επιλογές για το $h(g)$. Επομένως, η ομάδα χαρακτήρων $\hat{U}_n$ έχει n στοιχεία, δηλαδή $|\hat{U}_n| = n$. Επίσης, επειδή η ταυτοτική συνάρτηση της U_n είναι στοιχείο της $\hat{U}_n$ τάξης n, η $\hat{U}_n$ είναι κυκλική. Έτσι, οι ομάδες U_n και $\hat{U}_n$ είναι κυκλικές τάξης n. Τότε, από το Θεώρημα 2.1.2 έχουμε $U_n \cong \mathbb{Z}_n$ και $\hat{U}_n \cong \mathbb{Z}_n$. Αφού $U_n \cong \mathbb{Z}_n$, από το Θεώρημα 2.2.3, έχουμε $\hat{U}_n \cong \hat{\mathbb{Z}}_n$. Επομένως, συνοψίζουμε το ακόλουθο αποτέλεσμα.

Θεώρημα 2.2.7. *Αν n είναι ένας θετικός ακέραιος, τότε $\mathbb{Z}_n \cong \hat{\mathbb{Z}}_n$.*

Πόρισμα 2.2.8. *Αν G είναι μια πεπερασμένη Αβελιανή ομάδα, τότε $G \cong \hat{G}$.*

Απόδειξη. Από το Θεμελιώδες Θεώρημα των πεπερασμένων Αβελιανών ομάδων, έχουμε $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ για μοναδικούς ακέραιους s και $n_1, \ldots, n_s$, όπου $n_j \geq 2$ με $n_j | n_{j+1}$ για $j = 1, \ldots, s-1$. Έπειτα, από το Θεώρημα 2.2.3, έχουμε $\hat{G} \cong \widehat{\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}}$ και από το Πόρισμα 2.2.5 παίρνουμε $\widehat{\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}} = \hat{\mathbb{Z}}_{n_1} \otimes \cdots \otimes \hat{\mathbb{Z}}_{n_s}$. Τέλος από την Πρόταση 2.2.6 και το Θεώρημα 2.2.7 έχουμε το ζητούμενο. □

Παράδειγμα 2.2.9. *Χρησιμοποιώντας προσθετική γραφή για τη διμελή πράξη στο $\mathbb{Z}_n$, ένας χαρακτήρας της $\mathbb{Z}_n$ είναι μια απεικόνιση $\chi : \mathbb{Z}_n \to U_n$ τέτοια ώστε*

$$\chi(a+b) = \chi(a)\chi(b)$$

για κάθε $a, b \in \mathbb{Z}_n$. Επειδή η πρόσθεση modulo n είναι μια διμελής πράξη στο $\mathbb{Z}_n$, το άθροισμα $a+b$ στην προηγούμενη εξίσωση σημαίνει $(a+b)(mod\ n)$. Για κάθε $a \in \mathbb{Z}_n$, έστω $\chi_a : \mathbb{Z}_n \to U_n$ η συνάρτηση που ορίζεται με

$$\chi_a(b) = \xi_n^{ab}.$$

Η συνάρτηση είναι καλά ορισμένη, αφού αν $b = c \pmod n$ *τότε* $b = c + kn$, *για κάποιο* $k \in \mathbb{Z}$, *οπότε έχουμε*

$$\chi_a(b) = \xi_n^{ab} = \xi_1^k \xi_n^{ac} = \xi_n^{ac} = \chi_a(c).$$

Για $b_1, b_2 \in \mathbb{Z}_n$ *έχουμε*

$$\chi_a(b_1 + b_2) = \xi_n^{a(b_1+b_2)} = \xi_n^{ab_1}\xi_n^{ab_2} = \chi_a(b_1)\chi_a(b_2).$$

Επομένως χ_a *είναι ένας χαρακτήρας της* $\mathbb{Z}_n$.

Επιπλέον, $\chi_a = \chi_b$ *αν και μόνο αν* $a = b$. *Επειδή είναι φανερό ότι αν* $a = b$ *τότε* $\chi_a = \chi_b$, *μένει να δείξουμε ότι αν* $\chi_a = \chi_b$, *τότε* $a = b$. *Η ισότητα* $\chi_a = \chi_b$ *συνεπάγεται ότι* $\chi_a(1) = \chi_b(1)$ *ή* $\xi_n^a = \xi_n^b$, *οπότε* $a = b \pmod n$. *Επειδή* $0 \le a, b < n$ *έχουμε* $a = b$.

Έχουμε βρει n *χαρακτήρες της* $\mathbb{Z}_n$, *και συγκεκριμένα τους* χ_0,..., χ_{n-1}. *Αυτοί είναι όλοι οι χαρακτήρες της* $\mathbb{Z}_n$, *αφού* $|\hat{\mathbb{Z}}_n| = n$. *Σημειώνουμε ότι οι χαρακτήρες της* $\mathbb{Z}_n$ *είναι συμμετρικοί με την έννοια ότι* $\chi_a(b) = \chi_b(a)$.

Πρόταση 2.2.10. *Έστω* G *μια πεπερασμένη Αβελιανή ομάδα. Αν* $g \in G\backslash\{1\}$ *τότε υπάρχει χαρακτήρας* χ *της* G *τέτοιος ώστε* $\chi(g) \neq 1$.

Απόδειξη. Έστω $G' = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$. Εφαρμόζουμε επαγωγή στο s. Αν $s = 1$, τότε έχουμε $G' = \mathbb{Z}_{n_1}$. Υποθέτουμε ότι για $b \in \mathbb{Z}_{n_1}, b \neq 0$ έχουμε $\chi_a(b) = 1$ για κάθε $a \in \mathbb{Z}_{n_1}$. Τότε $ab \equiv 0 \pmod{n_1}$ ή $n_1 | ab$ με $0 \le a, b < n_1$. Για $a = 1$ έχουμε $n_1 | b$ με $b < n_1$. Άτοπο. Επομένως, για $b \in \mathbb{Z}_{n_1}, b \neq 0$ υπάρχει $a \in \mathbb{Z}_{n_1}$ τέτοιο ώστε $\chi_a(b) \neq 1$. Έστω ότι για την ομάδα $G' = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$, αν $g \in G'\backslash\{1\}$ τότε υπάρχει χαρακτήρας χ' της G' τέτοιος ώστε $\chi'(g) \neq 1$. Θα αποδείξουμε ότι το ίδιο ισχύει και για την ομάδα $G'' = G' \times \mathbb{Z}_{n_{s+1}} = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}_{n_{s+1}}$. Έστω $\chi_{T_{s+1}}$ ο τετριμμένος χαρακτήρας της $\mathbb{Z}_{n_{s+1}}$ και $a \in \mathbb{Z}_{n_{s+1}}$. Τότε ο $\chi'' = \chi' \otimes \chi_{T_{s+1}}$ είναι χαρακτήρας της G'' τέτοιος ώστε για $y = (g, a)$, $g \in G'\backslash\{1\}$,

$$\chi''(y) = \chi' \otimes \chi_{T_{s+1}}(g, a) = \chi'(g)\chi_{T_{s+1}}(a) = \chi'(g) \neq 1$$

από την επαγωγική υπόθεση. Από το Θεμελιώδες Θεώρημα των πεπερασμένων Αβελιανών ομάδων, έχουμε $G \cong G'$, επομένως ισχύει το ζητούμενο. □

Έστω G μια πεπερασμένη Αβελιανή ομάδα. Η *διπλή δυϊκή* της G ορίζεται να είναι η δυϊκή της δυϊκής της G και συμβολίζεται με $\hat{\hat{G}}$. Από το Πόρισμα 2.2.8 έχουμε $G \cong \hat{\hat{G}}$. Ο ισομορφισμός αυτός εξαρτάται από τον ισομορφισμό που δίνεται από το Θεμελιώδες Θεώρημα των πεπερασμένων Αβελιανών ομάδων. Εναλλακτικά, μπορούμε να ορίσουμε έναν ισομορφισμό από τη G στη $\hat{\hat{G}}$ ανεξάρτητο του Θεωρήματος αυτού: έστω $\kappa : G \to \hat{\hat{G}}$ η απεικόνιση που ορίζεται με $g \mapsto \kappa_g$, όπου κ_g είναι ένας χαρακτήρας της $\hat{G}$ που δίνεται από $\kappa_g(\chi) = \chi(g)$ για κάθε $\chi \in \hat{G}$. Παρατηρούμε ότι η απεικόνιση κ είναι κάλά ορισμένη. Πράγματι, για $\chi_1, \chi_2 \in \hat{G}$ έχουμε

$$\kappa_g(\chi_1\chi_2) = \chi_1\chi_2(g) = \chi_1(g)\chi_2(g) = \kappa_g(\chi_1)\kappa_g(\chi_2).$$

Επομένως κ_g είναι ένας χαρακτήρας της $\hat{G}$. Επιπλέον, για $g_1, g_2 \in G$ έχουμε $\kappa(g_1g_2) = \kappa_{g_1g_2}$ με $\kappa_{g_1g_2}(\chi) = \chi(g_1g_2) = \chi(g_1)\chi(g_2) = \kappa_{g_1}(\chi)\kappa_{g_2}(\chi) = \kappa_{g_1}\kappa_{g_2}(\chi)$ για κάθε $\chi \in \hat{G}$. Οπότε

$$\kappa_{g_1g_2} = \kappa_{g_1}\kappa_{g_2} = \kappa(g_1)\kappa(g_2).$$

Επομένως κ είναι ένας ομομορφισμός ομάδων. Τώρα θα δείξουμε ότι η κ είναι ένας ισομορφισμός:
$ker(\kappa) = \{1\}$: Έστω κ_T ο τετριμμένος χαρακτήρας της $\hat{G}$. Αν $\kappa(g) = \kappa_g = \kappa_T$, τότε $\kappa_g(\chi) = \chi(g) = 1$ για κάθε $\chi \in \hat{G}$. Από την Πρόταση 2.2.10 έπεται ότι $g = 1$. Επίσης, επειδή $|G| = |\hat{G}| = |\hat{\hat{G}}|$, έχουμε το ζητούμενο.

2.3 Σχέσεις ορθογωνιότητας για Χαρακτήρες

Η έννοια της ορθογωνιότητας των χαρακτήρων πεπερασμένων Αβελιανών ομάδων είναι απαραίτητη στον ορισμό του μετασχηματισμού Fourier.

Έστω G μια πεπερασμένη Αβελιανή ομάδα και H μια υποομάδα της G. Έστω ακόμη $\hat{G}_H$ το σύνολο των χαρακτήρων της G οι οποίοι είναι ταυτοτικά 1 στην H.

Θεώρημα 2.3.1. *Αν H μια υποομάδα της G και $\chi \in \hat{G}$, τότε*

$$\sum_{h\in H} \chi(h) = \begin{cases} |H| & \text{αν } \chi \in \hat{G}_H, \\ 0 & \text{διαφορετικά.} \end{cases}$$

Απόδειξη. Έστω A το άθροισμα στη διατύπωση του θεωρήματος. Αν $\chi \in \hat{G}_H$, τότε $\chi(h) = 1$ για κάθε $h \in H$, οπότε $A = |H|$. Από την άλλη, αν $\chi \notin \hat{G}_H$, τότε υπάρχει $h_0 \in H$ τέτοιο ώστε $\chi(h_0) \neq 1$. Από το Θεώρημα 2.1.1 έχουμε

$$A = \sum_{h\in H} \chi(h_0h) = \chi(h_0) \sum_{h\in H} \chi(h) = \chi(h_0)A,$$

οπότε $A = 0$. □

Πόρισμα 2.3.2. *Αν χ είναι χαρακτήρας της G, τότε*

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \text{αν } \chi = \chi_T, \\ 0 & \text{αν } \chi \neq \chi_T. \end{cases}$$

Απόδειξη. Θέτουμε $H = G$ στο Θεώρημα 2.3.1. □

Πόρισμα 2.3.3. *(Σχέσεις ορθογωνιότητας).*
(i) *Αν χ και ψ είναι χαρακτήρες της G, τότε*

$$\sum_{g\in G} \chi(g)\bar{\psi}(g) = \begin{cases} |G| & \text{αν } \chi = \psi, \\ 0 & \text{αν } \chi \neq \psi. \end{cases}$$

(ii) *Αν χ είναι χαρακτήρας της G, τότε*

$$\sum_{\chi\in\hat{G}} \bar{\chi}(a)\chi(b) = \begin{cases} |G| & \text{αν } a = b, \\ 0 & \text{αν } a \neq b. \end{cases}$$

Απόδειξη. (i) Από την εξίσωση (2.2) έχουμε $\bar{\psi} = \psi^{-1}$, οπότε

$$\sum_{g\in G} \chi(g)\bar{\psi}(g) = \sum_{g\in G} \chi(g)\psi^{-1}(g) = \sum_{g\in G} \chi\psi^{-1}(g) = \begin{cases} |G| & \text{αν } \chi = \psi, \\ 0 & \text{αν } \chi \neq \psi, \end{cases}$$

σύμφωνα με το προηγούμενο Πόρισμα.
(ii)

$$\sum_{\chi\in\hat{G}} \bar{\chi}(a)\chi(b) = \sum_{\chi\in\hat{G}} \chi(b)\chi^{-1}(a) = \sum_{\chi\in\hat{G}} \chi(b)\chi(a^{-1}) = \sum_{\chi\in\hat{G}} \chi(ba^{-1})$$

$$= \sum_{\chi\in\hat{G}} \kappa_{ba^{-1}}(\chi) = \begin{cases} |G| & \text{αν } a = b, \\ 0 & \text{αν } a \neq b, \end{cases}$$

σύμφωνα με το προηγούμενο Πόρισμα. □

Πόρισμα 2.3.4. *Αν χ είναι χαρακτήρας της G, τότε*

$$\sum_{\chi\in\hat{G}} \chi(b) = \begin{cases} |G| & \text{αν } b = 1, \\ 0 & \text{αν } b \neq 1. \end{cases}$$

Απόδειξη. Θέτουμε $a = 1$ στο (ii) του προηγούμενου πορίσματος. □

Κεφάλαιο 3

Ο Μετασχηματισμός Fourier

3.1 Ορισμός και Μερικές Ιδιότητες

Έστω G μια πεπερασμένη Αβελιανή ομάδα και V_G ο χώρος των μιγαδικών συναρτήσεων που ορίζονται στη G. Στο V_G ορίζουμε το εσωτερικό γινόμενο

$$\langle f, g\rangle = \sum_{a\in G} f(a)\bar{g}(a).$$

Ορισμός 3.1.1. *Ο μετασχηματισμός Fourier μιας απεικόνισης $f : G \to \mathbb{C}$ είναι μια απεικόνιση $\hat{f} : \hat{G} \to \mathbb{C}$ με*

$$\hat{f}(\chi) = \frac{1}{\sqrt{|G|}}\langle f, \chi\rangle = \frac{1}{\sqrt{|G|}} \sum_{a\in G} f(a)\bar{\chi}(a).$$

Πρόταση 3.1.2. *Έστω $f, g : G \to \mathbb{C}$ και $\lambda \in \mathbb{C}$. Τότε ισχύουν οι ακόλουθες ιδιότητες:*
(i) $\widehat{f+g} = \hat{f} + \hat{g}$
(ii) $\widehat{\lambda f} = \lambda\hat{f}$.

Απόδειξη. Για κάθε $\chi \in \hat{G}$ έχουμε
(i)

$$\widehat{f+g}(\chi) = \frac{1}{\sqrt{|G|}}\langle f+g, \chi\rangle = \frac{1}{\sqrt{|G|}}\langle f, \chi\rangle + \frac{1}{\sqrt{|G|}}\langle g, \chi\rangle = \hat{f}(\chi) + \hat{g}(\chi)$$

και (ii)

$$\widehat{\lambda f}(\chi) = \frac{1}{\sqrt{|G|}}\langle \lambda f, \chi\rangle = \lambda\frac{1}{\sqrt{|G|}}\langle f, \chi\rangle = \lambda\hat{f}(\chi).$$

□

Παράδειγμα 3.1.3. *Έστω $f : G \to \mathbb{C}$ σταθερή με $f(a) = c$. Τότε*

$$\hat{f}(\chi) = \begin{cases} c\sqrt{|G|} & \text{αν } \chi = \chi_T, \\ 0 & \text{αν } \chi \neq \chi_T. \end{cases}$$

Πράγματι,

$$\hat{f}(\chi) = \frac{1}{\sqrt{|G|}} \sum_{a \in G} f(a)\bar{\chi}(a) = c\frac{1}{\sqrt{|G|}} \sum_{a \in G} \bar{\chi}(a) = \begin{cases} c\sqrt{|G|} & \text{αν } \bar{\chi} = \chi_T, \\ 0 & \text{αν } \bar{\chi} \neq \chi_T, \end{cases}$$

σύμφωνα με το Πόρισμα 2.3.2.

Θεώρημα 3.1.4. *Έστω $f : G \to \mathbb{C}$ και $a \in G$. Τότε*

$$\hat{\hat{f}}(\kappa_a) = f(a^{-1}).$$

Απόδειξη.

$$\hat{\hat{f}}(\kappa_a) = \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\bar{\kappa_a}(\chi) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \sum_{b \in G} f(b)\bar{\chi}(b)\bar{\chi}(a)$$

$$= \frac{1}{|G|} \sum_{\chi \in \hat{G}} \sum_{b \in G} f(b^{-1})\chi(b)\bar{\chi}(a) = \frac{1}{|G|} \sum_{b \in G} f(b^{-1}) \sum_{\chi \in \hat{G}} \kappa_b(\chi)\bar{\kappa}_a(\chi) = f(a^{-1}).$$

□

Θεώρημα 3.1.5. (Τύπος αντιστροφής.) *Έστω $f : G \to \mathbb{C}$ και $b \in G$. Τότε*

$$f(b) = \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(b).$$

Απόδειξη.

$$\sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(b) = \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \sum_{a \in G} f(a)\bar{\chi}(a)\chi(b)$$

$$= \frac{1}{\sqrt{|G|}} \sum_{a \in G} f(a) \sum_{\chi \in \hat{G}} \chi(b)\bar{\chi}(a)$$

$$= \frac{1}{\sqrt{|G|}} \sum_{a \in G} f(a) \sum_{\chi \in \hat{G}} \chi(ba^{-1})$$

$$= \sqrt{|G|} f(b),$$

σύμφωνα με το Πόρισμα 2.3.4. Επομένως έχουμε

$$f(b) = \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(b).$$

□

3.2 Συνέλιξη

Έστω $f, g : G \to \mathbb{C}$. Ορίζουμε τη συνέλιξη των f, g με

$$f * g(a) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f(b)g(b^{-1}a).$$

Θεώρημα 3.2.1. *Για $f, g : G \to \mathbb{C}$ έχουμε $\widehat{f * g} = \hat{f}\hat{g}$, όπου δεξιά έχουμε το γινόμενο κατά σημείο.*

Απόδειξη. Έχουμε

$$\widehat{f * g}(\chi) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f * g(b)\bar{\chi}(b) = \frac{1}{|G|} \sum_{a \in G} \sum_{b \in G} f(a)g(a^{-1}b)\bar{\chi}(b).$$

Από το Θεώρημα 2.1.1, αντικαθιστώντας το b με ab, παίρνουμε

$$\widehat{f * g}(\chi) = \frac{1}{|G|} \sum_{a \in G} f(a)\bar{\chi}(a) \sum_{b \in G} g(b)\bar{\chi}(b) = \hat{f}(\chi)\hat{g}(\chi).$$

□

Πρόταση 3.2.2. *Έστω $f, g, h : G \to \mathbb{C}$. Τότε ισχύουν οι ακόλουθες ιδιότητες:*
(i) $(f * g) * h = f * (g * h)$
(ii) $f * (g + h) = f * g + f * h$
(iii) $f * g = g * f$.

Απόδειξη. Για κάθε $a \in G$ ισχύει (i)

$$(f * g) * h(a) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f * g(b)h(b^{-1}a)$$

$$= \frac{1}{|G|} \sum_{b \in G} \sum_{c \in G} f(c)g(c^{-1}b)h(b^{-1}a)$$

$$= \frac{1}{|G|} \sum_{c \in G} f(c) \sum_{b \in G} g(b)h(c^{-1}b^{-1}a),$$

όπου η τελευταία ισότητα έπεται από το Θεώρημα 2.1.1. Ακόμη

$$f * (g * h)(a) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f(b) g * h(b^{-1}a)$$

$$= \frac{1}{|G|} \sum_{b \in G} f(b) \sum_{c \in G} g(c) h(c^{-1}b^{-1}a)$$

$$= (f * g) * h(a).$$

(ii)

$$f * (g + h)(a) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f(b)(g + h)(b^{-1}a)$$

$$= \frac{1}{\sqrt{|G|}} \sum_{b \in G} f(b)(g(b^{-1}a) + h(b^{-1}a))$$

$$= \frac{1}{\sqrt{|G|}} (\sum_{b \in G} f(b) g(b^{-1}a) + \sum_{b \in G} f(b) h(b^{-1}a))$$

$$= f * g(a) + f * h(a).$$

(iii)

$$f * g(a) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f(b) g(b^{-1}a) = \frac{1}{\sqrt{|G|}} \sum_{b \in G} f(b^{-1}) g(ba)$$

$$= \frac{1}{\sqrt{|G|}} \sum_{b \in G} g(b) f(b^{-1}a) = g * f(a),$$

όπου η προτελευταία ισότητα έπεται από το Θεώρημα 2.1.1. □

Κεφάλαιο 4

Ανάλυση Fourier στο $\mathbb{F}_q^n$

4.1 Εισαγωγή

Η απεικόνιση του ίχνους στο $\mathbb{F}_q$ ορίζεται με

$$\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p, \mathrm{Tr}(\theta) = \sum_{i=0}^{e-1} \theta^{p^i}.$$

Η απεικόνιση του ίχνους είναι $\mathbb{F}_p$-γραμμική και απεικονίζει το $\mathbb{F}_q$ στο $\mathbb{F}_p$. Ειδικότερα, για $\theta \in \mathbb{F}_p$, $\mathrm{Tr}(\theta) = e\theta$. Επιπλέον, υπάρχει $a \in \mathbb{F}_q$ τέτοιο ώστε $\mathrm{Tr}(a) \neq 0$ και $\mathrm{im}(\mathrm{Tr}) = \mathbb{F}_p$, δηλαδή η απεικόνιση είναι επί.

Θεωρούμε την απεικόνιση

$$e_p : \mathbb{F}_p \to \mathbb{C}^*, e_p(x) = \exp\left(\frac{2\pi i x}{p}\right).$$

Για κάθε $u \in \mathbb{F}_q^n$, ορίζουμε την απεικόνιση

$$\chi_u : \mathbb{F}_q^n \to \mathbb{C}^*, \chi_u(v) = e_p(\mathrm{Tr}(\langle u, v\rangle)).$$

Τότε για $v_1, v_2 \in \mathbb{F}_q^n$ έχουμε

$$\chi_u(v_1 + v_2) = e_p(\mathrm{Tr}(\langle u, v_1 + v_2\rangle)) = e_p(\mathrm{Tr}(\langle u, v_1\rangle + \langle u, v_2\rangle))$$

$$= e_p(\mathrm{Tr}(\langle u, v_1\rangle) + \mathrm{Tr}(\langle u, v_2\rangle)) = e_p(\mathrm{Tr}(\langle u, v_1\rangle))e_p(\mathrm{Tr}(\langle u, v_2\rangle)) = \chi_u(v_1)\chi_u(v_2).$$

Επομένως χ_u είναι ένας χαρακτήρας της ομάδας $\mathbb{F}_q^n$.

Επιπλέον, $\chi_u = \chi_w$ αν και μόνο αν $u = w$. Επειδή είναι φανερό ότι αν $u = w$ τότε $\chi_u = \chi_w$, μένει να δείξουμε ότι αν $\chi_u = \chi_w$, τότε $u = w$. Η ισότητα $\chi_u = \chi_w$ συνεπάγεται ότι $\chi_u(v) = \chi_w(v)$ ή $e_p(\mathrm{Tr}(\langle u, v\rangle)) = e_p(\mathrm{Tr}(\langle w, v\rangle)) \Rightarrow e_p(\mathrm{Tr}(\langle u, v\rangle) - \mathrm{Tr}(\langle w, v\rangle)) = 1 \Rightarrow \frac{2\pi}{p}(\mathrm{Tr}(\langle u, v\rangle) - \mathrm{Tr}(\langle w, v\rangle)) = 2k\pi \Rightarrow \mathrm{Tr}(\langle u - w, v\rangle) = 0$, για κάθε $v \in \mathbb{F}_q^n$.
Έστω ότι $u - w \neq 0$. Τότε, η απεικόνιση $L : \mathbb{F}_q^n \to \mathbb{F}_q$ που δίνεται από $v \mapsto$

$\langle u-w, v\rangle$ δεν είναι η μηδενική, οπότε επειδή $dim\mathrm{im}(L) \leq dim\mathbb{F}_q = 1$, θα είναι $\mathrm{im}(L) = \mathbb{F}_q$. Αυτό σημαίνει ότι η L είναι επί, άρα το μη μηδενικό πολυώνυμο $X + X^p + ... + X^{p^{e-1}} \in \mathbb{F}_p[X]$ έχει q ρίζες. Άτοπο. Άρα $u = w$.

Έχουμε βρει q^n χαρακτήρες της $\mathbb{F}_q^n$, και συγκεκριμένα τους χ_u, $u \in \mathbb{F}_q^n$. Αυτοί είναι όλοι οι χαρακτήρες της $\mathbb{F}_q^n$, αφού $|\widehat{\mathbb{F}_q^n}| = q^n$. Σημειώνουμε ότι οι χαρακτήρες της $\mathbb{F}_q^n$ είναι συμμετρικοί με την έννοια ότι $\chi_u(v) = \chi_v(u)$ και $\chi_{\lambda u}(v) = \chi_u(\lambda v)$ για $\lambda \in \mathbb{F}_q$.

Θεώρημα 4.1.1. *Υπάρχει ένας κανονικός ισομομορφισμός $\mathbb{F}_q^n \to \widehat{\mathbb{F}_q^n}$ που δίνεται από $u \mapsto \chi_u$, όπου χ_u είναι ένας χαρακτήρας της $\mathbb{F}_q^n$.*

Απόδειξη. Η απεικόνιση $u \mapsto \chi_u$ είναι ένας ομομορφισμός, αφού για $u_1, u_2 \in \mathbb{F}_q^n$ έχουμε

$$\chi_{u_1+u_2}(v) = e_p(\mathrm{Tr}(\langle u_1+u_2, v\rangle)) = e_p(\mathrm{Tr}(\langle u_1, v\rangle + \langle u_2, v\rangle))$$

$$= e_p(\mathrm{Tr}(\langle u_1, v\rangle) + \mathrm{Tr}(\langle u_2, v\rangle)) = e_p(\mathrm{Tr}(\langle u_1, v\rangle))e_p(\mathrm{Tr}(\langle u_2, v\rangle))$$

$$= \chi_{u_1}(v)\chi_{u_2}(v) = \chi_{u_1}\chi_{u_2}(v).$$

Παραπάνω δείξαμε ότι αν $\chi_u = \chi_w$, τότε $u = w$, άρα η απεικόνιση είναι 1-1. Επίσης, επειδή $|\mathbb{F}_q^n| = |\widehat{\mathbb{F}_q^n}|$, έχουμε το ζητούμενο. □

Για $f : \mathbb{F}_q^n \to \mathbb{C}$ ορίζουμε ως μετασχηματισμό Fourier της f την απεικόνιση $\hat{f} : \mathbb{F}_q^n \to \mathbb{C}$ με

$$\hat{f}(u) = \frac{1}{q^{n/2}} \sum_{v\in\mathbb{F}_q^n} f(v)\bar{\chi}_u(v) = \frac{1}{q^{n/2}} \sum_{v\in\mathbb{F}_q^n} f(v)\chi_{-u}(v).$$

Η ισότητα $\bar{\chi}_u = \chi_{-u}$ ισχύει καθώς $\chi_u\chi_{-u} = \chi_T$. Πράγματι, έχουμε

$$\chi_u(v)\chi_{-u}(v) = e_p(\mathrm{Tr}(\langle u, v\rangle))e_p(\mathrm{Tr}(\langle -u, v\rangle)) = \exp(\mathrm{Tr}(\langle u, v\rangle) + \mathrm{Tr}(\langle -u, v\rangle))$$

$$= \exp(\mathrm{Tr}(\langle u, v\rangle) - \mathrm{Tr}(\langle u, v\rangle)) = \exp(0) = 1,$$

για κάθε $v \in \mathbb{F}_q^n$.

Παράδειγμα 4.1.2. *Έστω $u_0 \in \mathbb{F}_q^n$ και $f : \mathbb{F}_q^n \to \mathbb{C}$ με*

$$f(u) = \begin{cases} 1 & \text{αν } u = u_0, \\ 0 & \text{αν } u \neq u_0. \end{cases}$$

Τότε

$$\hat{f}(u) = \frac{1}{q^{n/2}} \sum_{v\in\mathbb{F}_q^n} f(v)\bar{\chi}_u(v) = \frac{1}{q^{n/2}}\chi_{-u}(u_0) = \frac{1}{q^{n/2}} e_p(\mathrm{Tr}(\langle u, -u_0\rangle)).$$

Από το Θεώρημα 3.1.4 ισχύει ο τύπος

$$\hat{\hat{f}}(a) = f(-a),$$

για

$G = \mathbb{F}_q^n$. Πράγματι, έχουμε

$$\hat{\hat{f}}(a) = \frac{1}{q^{n/2}} \sum_{u \in \mathbb{F}_q^n} \hat{f}(u) \bar{\kappa_a}(\chi_u)$$

$$= \frac{1}{q^n} \sum_{u \in \mathbb{F}_q^n} \sum_{v \in \mathbb{F}_q^n} f(v) \chi_{-u}(v) \bar{\chi}_u(a)$$

$$= \frac{1}{q^n} \sum_{u \in \mathbb{F}_q^n} \sum_{v \in \mathbb{F}_q^n} f(-v) \chi_u(v) \bar{\chi}_u(a)$$

$$= \frac{1}{q^n} \sum_{v \in \mathbb{F}_q^n} f(-v) \sum_{u \in \mathbb{F}_q^n} \kappa_v(\chi_u) \bar{\kappa}_a(\chi_u)$$

$$= f(-a).$$

Από το Θεώρημα 3.1.5 ισχύει ο τύπος

$$f(w) = \frac{1}{q^{n/2}} \sum_{u \in \mathbb{F}_q^n} \hat{f}(u) \chi_u(w),$$

για $G = \mathbb{F}_q^n$. Πράγματι, έχουμε

$$\sum_{u \in \mathbb{F}_q^n} \hat{f}(u) \chi_u(w) = \frac{1}{q^{n/2}} \sum_{u,v \in \mathbb{F}_q^n} f(v) \bar{\chi}_u(v) \chi_u(w)$$

$$= \frac{1}{q^{n/2}} \sum_{v \in \mathbb{F}_q^n} f(v) \sum_{u \in \mathbb{F}_q^n} \chi_{-u}(v) \chi_u(w)$$

$$= \frac{1}{q^{n/2}} \sum_{v \in \mathbb{F}_q^n} f(v) \sum_{u \in \mathbb{F}_q^n} \chi_u(w - v)$$

$$= q^{n/2} f(w),$$

σύμφωνα με το Πόρισμα 2.3.4. Επομένως έχουμε

$$f(w) = \frac{1}{q^{n/2}} \sum_{u \in \mathbb{F}_q^n} \hat{f}(u) \chi_u(w).$$

Για ένα υποσύνολο $C \subseteq \mathbb{F}_q^n$, συμβολίζουμε με $\mathbf{1}_C$ τη χαρακτηριστική συνάρτηση του C.

Λήμμα 4.1.3. *Αν C είναι ένας γραμμικός υπόχωρος του $\mathbb{F}_q^n$, τότε $\hat{\mathbf{1}}_C = |C|/q^{n/2} \mathbf{1}_{C^\perp}$.*

Απόδειξη. Έστω $u \in \mathbb{F}_q^n$. Τότε $\hat{\mathbf{1}}_C(u) = \frac{1}{q^{n/2}} \sum_{c \in C} \chi_u(-c) = \frac{1}{q^{n/2}} \sum_{c \in C} \chi_u(c)$. Για κάθε $\theta \in \mathbb{F}_q$ ορίζουμε $C_\theta(u) = \{c \in C : \langle c, u \rangle = \theta\}$, έτσι ώστε

$$\hat{\mathbf{1}}_C(u) = \frac{1}{q^{n/2}} \sum_{\theta \in \mathbb{F}_q} \sum_{c \in C_\theta(u)} e_p(\mathrm{Tr}(\theta)) = \frac{1}{q^{n/2}} \sum_{\theta \in \mathbb{F}_q} |C_\theta(u)| e_p(\mathrm{Tr}(\theta)).$$

Αν $u \in C^\perp$ τότε $C_0(u) = C$ και $C_\theta(u) = \emptyset$ για $\theta \neq 0$ και έχουμε

$$\hat{\mathbf{1}}_C(u) = \frac{1}{q^{n/2}} \sum_{c \in C} e_p(\mathrm{Tr}(0)) = |C|/q^{n/2}.$$

Αν $u \notin C^\perp$, τότε υπάρχει κάποιο $c' \in C$ τέτοιο ώστε $\langle c', u \rangle = \theta' \neq 0$. Θέτοντας $c_\theta = \theta(\theta')^{-1} c'$, βλέπουμε ότι για κάθε $\theta \in \mathbb{F}_q$ υπάρχει κάποιο $c_\theta \in C$ τέτοιο ώστε $\langle c_\theta, u \rangle = \theta$. Ακόμη, η απεικόνιση $C_0(u) \to C_\theta(u)$, $c \mapsto c + c_\theta$ είναι αμφιμονοσήμαντη, οπότε $|C_0(u)| = |C_\theta(u)|$ για κάθε $\theta \in \mathbb{F}_q$. Έπεται ότι

$$\hat{\mathbf{1}}_C(u) = \frac{1}{q^{n/2}} |C_0(u)| \sum_{\theta \in \mathbb{F}_q} e_p(\mathrm{Tr}(\theta)) = 0,$$

αφού $e_p(\mathrm{Tr}(\cdot))$ είναι ένας χαρακτήρας της $\mathbb{F}_q$. □

4.2 Ο μετασχηματισμός της σφαίρας

Για $1 \leq i \leq n$, έστω $U_i = \{v \in \mathbb{F}_q^n : \|v\| = i\}$ η σφαίρα ακτίνας i. Ο μετασχηματισμός Fourier της χαρακτηριστικής συνάρτησης του U_i μπορεί να εκφραστεί με τα λεγόμενα πολυώνυμα Krawtchouk. Για δοσμένο q και n το $i-$οστό πολυώνυμο Krawtchouk ορίζεται ως

$$K_i(x) = \sum_{j=0}^{i} \binom{x}{j} \binom{n-x}{i-j} (-1)^j (q-1)^{i-j}, i = 0, 1, ..., n.$$

Ορίζουμε τα πραγματικά πολυώνυμα P_j, για $j \geq 0$, τα οποία θα χρησιμοποιήσουμε στον παραπάνω ορισμό. Θέτουμε $P_0 = 1$ και, για $j \geq 1$,

$$P_j(x) = \frac{1}{j!}x(x-1)...(x-j+1).$$

Προφανώς, για $i \geq j \geq 0$, $P_j(i) = \binom{i}{j}$. Για δοσμένο q και n έχουμε

$$K_i(x) = \sum_{j=0}^{i} P_j(x)P_{i-j}(n-x)(-1)^j(q-1)^{i-j}, i = 0, 1, ..., n.$$

Πρόταση 4.2.1. *(Ιδιότητες των πολυωνύμων Krawtchouk.)*

(i) *Αν z μια μεταβλητή, τότε* $\sum_{k=0}^{\infty} K_k(x)z^k = (1-z)^x(1+(q-1)z)^{n-x}$.
(ii) $K_i(x) = \sum_{j=0}^{i} \binom{n-i+j}{j}\binom{n-x}{i-j}(-1)^j q^{i-j}$.
(iii) *Το $K_i(x)$ είναι ένα πολυώνυμο βαθμού i, με συντελεστή μεγιστοβάθμιου όρου $(-q)^i/i!$ και σταθερό όρο $K_i(0) = \binom{n}{i}(q-1)^i$.*
(iv) *(Σχέσεις ορθογωνιότητας.)* $\sum_{i=0}^{n}\binom{n}{i}(q-1)^i K_k(i)K_l(i) = \delta_{kl}\binom{n}{k}(q-1)^k q^n$, *όπου δ_{kl} είναι η συνάρτηση δέλτα του Kronecker:*

$$\delta_{kl} = \begin{cases} 1 & \text{αν } k = l, \\ 0 & \text{διαφορετικά.} \end{cases}$$

(v) $(q-1)^i\binom{n}{i}K_k(i) = (q-1)^k\binom{n}{k}K_i(k)$.
(vi) $\sum_{i=0}^{j}\binom{n-i}{n-j}K_i(x) = q^j\binom{n-x}{j}$.
(vii) *Κάθε πολυώνυμο $f(x)$ βαθμού r μπορεί να εκφραστεί ως* $f(x) = \sum_{k=0}^{r} f_k K_k(x)$, *όπου* $f_k = q^{-n}\sum_{i=0}^{n} f(i)K_i(k)$.

Απόδειξη. (i) Από το διωνυμικό ανάπτυγμα έχουμε

$$(1-z)^x = \sum_{k=0}^{\infty}(-1)^k\binom{x}{k}z^k$$

και

$$(1+(q-1)z)^{n-x} = \sum_{k=0}^{\infty}\binom{n-x}{k}(q-1)^k z^k.$$

Θέτουμε $a_k = (-1)^k\binom{x}{k}$ και $b_k = \binom{n-x}{k}(q-1)^k$. Επομένως

$$(1-z)^x(1+(q-1)z)^{n-x} = \sum_{\nu=0}^{\infty} c_\nu z^\nu,$$

όπου

$$c_\nu = \sum_{k=0}^{\nu} a_k b_{\nu-k} = \sum_{k=0}^{\nu}(-1)^k\binom{x}{k}\binom{n-x}{\nu-k}(q-1)^{\nu-k} = K_\nu(x).$$

Για το (ii) χρησιμοποιούμε την ισότητα

$$(1+(q-1)z)^{n-x}(1-z)^x = (1-z)^n\left(1+\frac{qz}{1-z}\right)^{n-x}.$$

(iii) Αρχικά παρατηρούμε ότι

$P_j(x)P_{i-j}(n-x) = \frac{(-1)^{i-j}}{j!(i-j)!}x^i +$ όροι βαθμού μικρότερου από i,

που συνεπάγεται ότι

$K_i(x) = \sum_{j=0}^{i}\frac{(-1)^i}{j!(i-j)!}(q-1)^{i-j}x^i +$ όροι βαθμού μικρότερου από i.

Έχουμε

$$\sum_{j=0}^{i}\frac{(-1)^i}{j!(i-j)!}(q-1)^{i-j} = \frac{(-1)^i}{i!}\sum_{j=0}^{i}\binom{i}{j}(q-1)^{i-j} = \frac{(-q)^i}{i!}.$$

Επιπλέον έχουμε

$$K_i(0) = \sum_{j=0}^{i}P_j(0)P_{i-j}(n)(-1)^j(q-1)^{i-j} = P_i(n)(q-1)^i = \binom{n}{i}(q-1)^i.$$

(iv) Θεωρούμε το πραγματικό πολυώνυμο δυο μεταβλητών

$$P(x,y) = \sum_{k=0}^{n}\sum_{l=0}^{n}\left(\sum_{i=0}^{n}\binom{n}{i}(q-1)^iK_k(i)K_l(i)\right)x^ky^l. \tag{4.1}$$

Τότε

$$P(x,y) = \sum_{i=0}^{n}\binom{n}{i}(q-1)^i\sum_{k=0}^{n}K_k(i)x^k\sum_{l=0}^{n}K_l(i)y^l$$

$$= \sum_{i=0}^{n}\binom{n}{i}(q-1)^i(1-x)^i(1+(q-1)x)^{n-i}(1-y)^i(1+(q-1)y)^{n-i}$$

$$= \sum_{i=0}^{n}\binom{n}{i}((q-1)(1-x)(1-y))^i((1+(q-1)x)(1+(q-1)y))^{n-i}$$

$$= ((q-1)(1-x)(1-y)+(1+(q-1)x)(1+(q-1)y))^n.$$

Μετά από πράξεις, παίρνουμε

$$P(x,y) = q^n(1+(q-1)xy)^n = \sum_{i=0}^{n}q^n\binom{n}{i}(q-1)^ix^iy^i. \tag{4.2}$$

Επομένως, εξισώνοντας τους συντελεστές στις (4.1),(4.2) έχουμε

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_k(i) K_l(i) = 0$$

αν $k \neq l$, και

$$\sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_k(i) K_l(i) = \binom{n}{k} (q-1)^k q^n$$

αν $k = l$.
(v) Θεωρούμε το πραγματικό πολυώνυμο δυο μεταβλητών

$$Q(x,y) = \sum_{k=0}^{n} \sum_{i=0}^{n} \binom{n}{i} (q-1)^i K_k(i) x^k y^i. \tag{4.3}$$

Τότε

$$Q(x,y) = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i y^i \sum_{k=0}^{n} K_k(i) x^k = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i y^i (1-x)^i (1+(q-1)x)^{n-i},$$

σύμφωνα με το (i), οπότε

$$Q(x,y) = \sum_{i=0}^{n} \binom{n}{i} ((q-1)y(1-x))^i (1+(q-1)x)^{n-i} = ((q-1)y(1-x)+(1+(q-1)x))^n$$

$$= ((q-1)(1-y)x+(1+(q-1)y))^n = \sum_{k=0}^{n} \binom{n}{k} (q-1)^k (1-y)^k x^k (1+(q-1)y)^{n-k},$$

από το διωνυμικό ανάπτυγμα. Επομένως

$$Q(x,y) = \sum_{k=0}^{n} \binom{n}{k} (q-1)^k x^k \sum_{i=0}^{n} K_i(k) y^i = \sum_{k=0}^{n} \sum_{i=0}^{n} \binom{n}{k} (q-1)^k K_i(k) x^k y^i. \tag{4.4}$$

Συγκρίνουμε τους συντελεστές στις (4.3),(4.4) και έχουμε το ζητούμενο.
(vii) Για $n \in \mathbb{N}$, συμβολίζουμε με $\mathbb{R}_n[X]$ το σύνολο των πραγματικών πολυωνύμων βαθμού το πολύ n. Ο $\mathbb{R}_n[X]$ είναι ένας πραγματικός διανυσματικός χώρος διάστασης $n+1$. Για ένα σταθερό $q \geq 2$, ορίζουμε ένα εσωτερικό γινόμενο $\langle \cdot, \cdot \rangle$ στο $\mathbb{R}_n[X]$ ως εξής:

$$\langle A, B \rangle = \sum_{i=0}^{n} \binom{n}{i} (q-1)^i A(i) B(i).$$

Αν $0 \leq i \leq n$, τότε $K_i \in \mathbb{R}_n[X]$ και από το (iv) έχουμε ότι $\langle K_k, K_l \rangle = 0$ για $k \neq l$. Οπότε το σύνολο των πολυωνύμων $\{K_i : 0 \leq i \leq n\}$ είναι γραμμικά ανεξάρτητο, άρα αποτελεί βάση του $\mathbb{R}_n[X]$. Δηλαδή κάθε πολυώνυμο $f \in \mathbb{R}_n[X]$ βαθμού r γράφεται ως $f(x) = \sum_{k=0}^{r} f_k K_k(x)$.
Έχουμε

$\langle f, K_k\rangle = \sum_{i=0}^n \binom{n}{i}(q-1)^i K_k(i)f(i) = \binom{n}{k}(q-1)^k \sum_{i=0}^n K_i(k)f(i)$,
σύμφωνα με το (v),
και $\langle f, K_k\rangle = \langle \sum_{j=0}^r f_j K_j, K_k\rangle = \sum_{j=0}^r f_j\langle K_j, K_k\rangle = f_k\binom{n}{k}(q-1)^k q^n$, σύμφωνα με το (iv).
Επομένως $f_k = q^{-n}\sum_{i=0}^n f(i)K_i(k)$. □

Θεώρημα 4.2.2. *Έστω $0 \le i \le n$ και $u \in \mathbb{F}_q^n$. Τότε $\hat{\mathbf{1}}_{U_i}(u) = \frac{1}{q^{n/2}}K_i(\|u\|)$.*

Απόδειξη. Σταθεροποιούμε i και $u \in \mathbb{F}_q^n$. Συμβολίζουμε με $N = \{1, ..., n\}$ και έστω $supp(u) = T \subseteq N$. Τότε

$$\hat{\mathbf{1}}_{U_i}(u) = \frac{1}{q^{n/2}}\sum_{v\in\mathbb{F}_q^n}\mathbf{1}_{U_i}(v)\chi_{-u}(v)$$

$$= \frac{1}{q^{n/2}}\sum_{\|v\|=i}\chi_{-u}(v) = \frac{1}{q^{n/2}}\sum_{\|v\|=i}\chi_u(v)$$

$$= \frac{1}{q^{n/2}}\sum_{\|v\|=i} e_p(\mathrm{Tr}(v_1u_1 + ... + v_nu_n))$$

$$= \frac{1}{q^{n/2}}\sum_{\|v\|=i}\prod_{k=1}^n e_p(\mathrm{Tr}(v_ku_k))$$

$$= \frac{1}{q^{n/2}}\sum_{S\subseteq N, |S|=i}\ \sum_{supp(v)=S}\ \prod_{k\in S\cap T} e_p(\mathrm{Tr}(v_ku_k)).$$

Προχωράμε στον υπολογισμό του εσωτερικού αθροίσματος. Σταθεροποιούμε ένα υποσύνολο S του N και υποθέτουμε ότι $|S\cap T| = j$. Έστω $S\cap T = \{k_1, ..., k_j\}$ και $S = \{k_1, ..., k_j, ..., k_i\}$. Έχουμε

$$\sum_{supp(v)=S}\ \prod_{k\in S\cap T} e_p(\mathrm{Tr}(v_ku_k)) = \sum_{v_{k_1}\in\mathbb{F}_q^*}\cdots\sum_{v_{k_i}\in\mathbb{F}_q^*}\prod_{l=1}^j e_p(\mathrm{Tr}(v_{k_l}u_{k_l}))$$

$$= \prod_{l=1}^j\sum_{v_{k_l}\in\mathbb{F}_q^*} e_p(\mathrm{Tr}(v_{k_l}u_{k_l}))\prod_{l=j+1}^i\sum_{v_{k_l}\in\mathbb{F}_q^*}1$$

$$\prod_{l=1}^j(-1)\prod_{l=j+1}^i(q-1) = (-1)^j(q-1)^{i-j}.$$

Υπάρχουν $\binom{|T|}{j}\binom{n-|T|}{i-j}$ τρόποι να επιλέξουμε ένα υποσύνολο S του N τέτοιο ώστε $|S \cap T| = j$ και $|S| = i$. Έπεται ότι

$$\hat{\mathbf{1}}_{U_i}(u) = \frac{1}{q^{n/2}} \sum_{j=0}^{i} \binom{\|u\|}{j}\binom{n-\|u\|}{i-j}(-1)^j(q-1)^{i-j} = \frac{1}{q^{n/2}} K_i(\|u\|).$$

□

4.3 Εξισώσεις MacWilliams

Η κατανομή βαρών γενικά δεν προσδιορίζει μοναδικά έναν κώδικα, αλλά δίνει σημαντικές πληροφορίες πρακτικής και θεωρητικής σημασίας. Όμως, ο υπολογισμός της κατανομής βαρών ενός μεγάλου κώδικα, ακόμη και από τον υπολογιστή, μπορεί να είναι ένα δύσκολο πρόβλημα.

Ένας γραμμικός κώδικας C καθορίζεται μοναδικά από το δυϊκό του $C^\perp$. Το σημαντικότερο αποτέλεσμα για τις κατανομές βαρών είναι ένα σύνολο γραμμικών σχέσεων μεταξύ των κατανομών βαρών του C και του $C^\perp$. Από τις σχέσεις αυτές, αν γνωρίζουμε την κατανομή βαρών του C, μπορούμε να προσδιορίσουμε την κατανομή βαρών του $C^\perp$ χωρίς να γνωρίζουμε συγκεκριμένα τις λέξεις του $C^\perp$ ή οτιδήποτε άλλο για τη δομή του. Οι γραμμικές αυτές σχέσεις αποτελούν το σημαντικότερο εργαλείο για τη μελέτη και τον υπολογισμό των κατανομών βαρών. Αναπτύχθηκαν πρώτα από την MacWilliams και συνεπώς ονομάζονται εξισώσεις MacWilliams ή ταυτότητες MacWilliams.

Στο Θεώρημα που ακολουθεί αναφέρουμε τέσσερις ισοδύναμες μορφές των εξισώσεων MacWilliams, που συνδέουν την κατανομή βαρών ενός $[n, k]$ κώδικα C πάνω από το $\mathbb{F}_q$ με την κατανομή βαρών του δυϊκού του $C^\perp$. Η πρώτη μορφή εκφράζει την κατανομή βαρών του δυϊκού κώδικα σε σχέση με την κατανομή βαρών του αρχικού κώδικα, με χρήση των πολυωνύμων Krawtchouk και περιλαμβάνει $n+1$ εξισώσεις. Η δεύτερη μορφή είναι μια ταυτότητα που περιλαμβάνει τον απαριθμητή βαρών ενός κώδικα και του δυϊκού του. Η τρίτη και η τέταρτη μορφή περιέχουν μόνο κατανομές βαρών και διωνυμικούς συντελεστές. Και οι δυο αποτελούνται απο ένα σύνολο $n + 1$ εξισώσεων.

Θεώρημα 4.3.1.

$$A_j^\perp = \frac{1}{|C|} \sum_{i=0}^{n} A_i K_j(i), 0 \le j \le n, \tag{K}$$

$$W_{C^\perp}(x) = \frac{1}{|C|}(1 + (q-1)x)^n W_C\left(\frac{1-x}{1+(q-1)x}\right). \tag{M_1}$$

$$\sum_{j=0}^{n-v}\binom{n-j}{v} A_j = q^{k-v}\sum_{j=0}^{v}\binom{n-j}{n-v} A_j^\perp, 0 \le v \le n. \tag{M_2}$$

$$\sum_{j=v}^{n}\binom{j}{v}A_j = q^{k-v}\sum_{j=0}^{v}(-1)^j\binom{n-j}{n-v}(q-1)^{v-j}A_j^{\perp}, 0\le v\le n. \qquad (M_3)$$

Απόδειξη. (K) Παρατηρούμε ότι

$$A_j^{\perp} = |C^{\perp}\cap U_j| = \sum_{v\in\mathbb{F}_q^n}\mathbf{1}_{C^{\perp}}(v)\mathbf{1}_{U_j}(v) = \sum_{v\in\mathbb{F}_q^n}\mathbf{1}_{C^{\perp}}(v)\mathbf{1}_{U_j}(-v) = q^{n/2}\mathbf{1}_{C^{\perp}}*\mathbf{1}_{U_j}(0).$$

Ορίζουμε $f(w)=\mathbf{1}_{C^{\perp}}*\mathbf{1}_{U_j}(w)$. Τότε

$$\hat{f}(w) = \hat{\mathbf{1}}_{C^{\perp}}(w)\hat{\mathbf{1}}_{U_j}(w) = \frac{q^{n/2}}{|C|}\hat{\hat{\mathbf{1}}}_C(w)\hat{\mathbf{1}}_{U_j}(w) = \frac{1}{|C|}\mathbf{1}_C(-w)K_j(\|w\|),$$

οπότε

$$\hat{\hat{f}}(w) = \frac{1}{|C|q^{n/2}}\sum_{v\in\mathbb{F}_q^n}\mathbf{1}_C(v)K_j(\|v\|)\chi_{-w}(v).$$

Επειδή $\hat{\hat{f}}(w)=f(-w)$, για $w=0$ έχουμε

$$f(0)=\mathbf{1}_{C^{\perp}}*\mathbf{1}_{U_j}(0) = \frac{1}{|C|q^{n/2}}\sum_{v\in C}\mathbf{1}_C(v)K_j(\|v\|)$$

$$= \frac{1}{|C|q^{n/2}}\sum_{v\in C}K_j(\|v\|)$$

$$= \frac{1}{|C|q^{n/2}}\sum_{i=0}^{n}\sum_{v\in C,\|v\|=i}K_j(\|v\|)$$

$$= \frac{1}{|C|q^{n/2}}\sum_{i=0}^{n}A_iK_j(i), 0\le j\le n.$$

Οπότε τελικά

$$A_j^{\perp} = \frac{1}{|C|}\sum_{i=0}^{n}A_iK_j(i), 0\le j\le n.$$

(M_1) Έχουμε

$$W_{C^{\perp}}(x) = \sum_{i=0}^{n}A_i^{\perp}x^i = \frac{1}{|C|}\sum_{i=0}^{n}\left(\sum_{k=0}^{n}A_kK_i(k)\right)x^i = \frac{1}{|C|}\sum_{k=0}^{n}A_k\sum_{i=0}^{n}K_i(k)x^i.$$

Για το εσωτερικό άθροισμα έχουμε

$$\sum_{i=0}^{n} K_i(k)x^i = \sum_{i=0}^{n}\sum_{j=0}^{i}\binom{k}{j}\binom{n-k}{i-j}(-1)^j(q-1)^{i-j}x^i.$$

Θέτοντας $i' = i - j$, έχουμε

$$\sum_{i=0}^{n} K_i(k)x^i = \sum_{j=0}^{k}\binom{k}{j}(-1)^j x^j \sum_{i'=0}^{n-k}\binom{n-k}{i'}(q-1)^{i'}x^{i'} = (1-x)^k(1+(q-1)x)^{n-k}.$$

Επομένως

$$W_{C^\perp}(x) = \frac{1}{|C|}\sum_{k=0}^{n} A_k(1-x)^k(1+(q-1)x)^{n-k} = \frac{1}{|C|}(1+(q-1)x)^n \sum_{k=0}^{n} A_k\left(\frac{1-x}{1+(q-1)x}\right)^k$$

$$= \frac{1}{|C|}(1+(q-1)x)^n W_C\left(\frac{1-x}{1+(q-1)x}\right).$$

(M_2) Σύμφωνα με τις εξισώσεις (K), έχουμε

$$q^{k-v}\sum_{j=0}^{v}\binom{n-j}{n-v}A_j^\perp = \frac{1}{|C|}q^{k-v}\sum_{j=0}^{v}\binom{n-j}{n-v}\sum_{i=0}^{n}A_iK_j(i) = q^{-v}\sum_{i=0}^{n}A_i\sum_{j=0}^{v}\binom{n-j}{n-v}K_j(i).$$

Από την ιδιότητα (vi) της Πρότασης 4.2.1, για το εσωτερικό άθροισμα έχουμε

$$\sum_{j=0}^{v}\binom{n-j}{n-v}K_j(i) = q^v\binom{n-i}{v}.$$

Επομένως

$$q^{k-v}\sum_{j=0}^{v}\binom{n-j}{n-v}A_j^\perp = q^{-v}\sum_{i=0}^{n}A_iq^v\binom{n-i}{v} = \sum_{i=0}^{n}\binom{n-i}{v}A_i = \sum_{j=0}^{n}\binom{n-j}{v}A_j.$$

Για $v > n-j$ ή ισοδύναμα $j > n-v$ είναι $\binom{n-j}{v} = 0$, οπότε έχουμε το ζητούμενο. □

Εφαρμογή. Η κατανομή βαρών του $\mathrm{S}(r,q)$, από την Πρόταση 1.4.4, είναι $A_0 = 1$ και $A_{q^{r-1}} = q^r - 1$. Επομένως έχουμε $W_{S(r,q)}(x) = 1 + (q^r-1)x^{q^{r-1}}$ και εφαρμόζοντας τη μορφή (M_1) των εξισώσεων MacWilliams,

$$W_{S(r,q)^\perp}(x) = W_{Ham(r,q)}(x) = \frac{1}{|S(r,q)|}(1+(q-1)x)^{(q^r-1)/(q-1)}W_{S(r,q)}\left(\frac{1-x}{1+(q-1)x}\right)$$

$$= \frac{(1+(q-1)x)^{(q^r-1)/(q-1)}}{q^r}\left(1+(q^r-1)\left(\frac{1-x}{1+(q-1)x}\right)^{q^{r-1}}\right).$$

Παράδειγμα 4.3.2. *Έστω C ένας $[5,2]$ δυαδικός κώδικας που παράγεται από*

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

Οπότε $C =< 11000, 01111 >= \{00000, 11000, 01111, 10111\}$. Άρα, η κατανομή βαρών του C είναι $A_0 = 1$, $A_2 = 1$ και $A_4 = 2$.
Θα χρησιμοποιήσουμε τώρα το σύνολο εξισώσεων (K) του Θεωρήματος 4.3.1 για να βρούμε την κατανομή βαρών του $C^\perp$. Έχουμε

$A_0^\perp = \frac{1}{|C|}\sum_{i=0}^5 A_i K_0(i) = \frac{1}{|C|}\sum_{i=0}^5 A_i = 1,$

$A_1^\perp = \frac{1}{|C|}\sum_{i=0}^5 A_i K_1(i) = \frac{1}{|C|}\sum_{i=0}^5 A_i(5-2i) = 0,$

$A_2^\perp = \frac{1}{|C|}\sum_{i=0}^5 A_i K_2(i) = \frac{1}{|C|}\sum_{i=0}^5 A_i(\binom{5-i}{2} - i(5-i) + \binom{i}{2}) = 3,$

$A_3^\perp = \frac{1}{|C|}\sum_{i=0}^5 A_i K_3(i) = \frac{1}{|C|}\sum_{i=0}^5 A_i(\binom{5-i}{3} - i\binom{5-i}{2} + \binom{i}{2}(5-i) - \binom{i}{3}) = 3,$

$A_4^\perp = \frac{1}{|C|}\sum_{i=0}^5 A_i K_4(i) = \frac{1}{|C|}\sum_{i=0}^5 A_i(\binom{5-i}{4} - i\binom{5-i}{3} + \binom{i}{2}\binom{5-i}{2} - \binom{i}{3}(5-i) + \binom{i}{4}) = 0$

και $A_5^\perp = \frac{1}{|C|}\sum_{i=0}^5 A_i K_5(i) = \frac{1}{|C|}\sum_{i=0}^5 A_i(\binom{5-i}{5} - i\binom{5-i}{4} + \binom{i}{2}\binom{5-i}{3} - \binom{i}{3}\binom{5-i}{2} + \binom{i}{4}(5-i) - \binom{i}{5} = 1.$

Άρα, η κατανομή βαρών του $C^\perp$ είναι $A_0^\perp = 1$, $A_2^\perp = 3$, $A_3^\perp = 3$ και $A_5^\perp = 1$.
Για να επαληθεύσουμε το προηγούμενο αποτέλεσμα αρκεί να βρούμε τα διανύσματα του $C^\perp$. Έστω $y = (y_1, \ldots, y_5) \in \mathbb{F}_q^n$. Τότε $y \in C^\perp \Leftrightarrow Gy^T = 0$. Επομένως αρκεί $y_1 = y_2$ και $y_2 = y_3 + y_4 + y_5$. Οπότε έχουμε $y = (y_3 + y_4 + y_5, y_3 + y_4 + y_5, y_3, y_4, y_5) = y_3(1,1,1,0,0) + y_4(1,1,0,1,0) + y_5(1,1,0,0,1)$.
Άρα $C^\perp =< 111000, 11010, 11001 >= \{00000, 111000, 11010, 11001, 00110, 00101, 00011, 11111\}$. Πράγματι, λοιπόν, προκύπτει η παραπάνω κατανομή βαρών για τον $C^\perp$.

Θεώρημα 4.3.3. *(Φράγμα γραμμικού προγραμματισμού.) Για δοσμένο q και θετικούς ακέραιους n και d $(1 \le d \le n)$, έστω $f(x) = 1 + \sum_{k=1}^n f_k K_k(x)$ ένα πολυώνυμο τέτοιο ώστε $f_k \ge 0$ $(1 \le k \le n)$ και $f(i) \le 0$ για $d \le i \le n$. Τότε $B_q(n,d) \le f(0)$.*

Απόδειξη. Έστω $q^k = B_q(n,d)$. Αν C είναι ένας $[n,k]$-κώδικας πάνω από το $\mathbb{F}_q$, η κατανομή βαρών του $\{A_i(C)\}_{i=0}^n$ ικανοποιεί τις ακόλουθες συνθήκες:

(i) $A_0(C) = 1$ και $A_i(C) = 0$ για $1 \le i < d$.
(ii) $A_i(C) \ge 0$ για $0 \le i \le n$.
(iii) $\sum_{i=0}^n A_i K_k(i) \ge 0$, για $0 \le k \le n$ (από Θεώρημα 4.3.1).
(iv) $\sum_{i=0}^n A_i = q^k$.

Από τα (i),(ii) και (iv) έπεται ότι $K_k(0) \ge -\sum_{i=d}^n A_i K_k(i)$ για $0 \le k \le n$.

Η συνθήκη ότι $f(i) \leq 0$ για $d \leq i \leq n$ συνεπάγεται ότι $\sum_{i=d}^{n} A_i f(i) \leq 0$, που σημαίνει ότι

$$f(0) = 1 + \sum_{k=1}^{n} f_k K_k(0) \geq 1 - \sum_{k=1}^{n} f_k \sum_{i=d}^{n} A_i K_k(i) = 1 - \sum_{i=d}^{n} A_i \sum_{k=1}^{n} f_k K_k(i)$$

$$= 1 - \sum_{i=d}^{n} A_i (f(i) - 1) \geq 1 + \sum_{i=d}^{n} A_i = q^k = B_q(n, d).$$

□

Κάθε πολυώνυμο $f(x)$ που ικανοποιεί το Θεώρημα 4.3.3 δίνει ένα άνω φράγμα για το $B_q(n, d)$. Το φράγμα αυτό είναι καλύτερο από άλλα φράγματα που αναφέραμε στο κεφάλαιο 1. Στο παράδειγμα που ακολουθεί δείχνουμε πώς καταλήγουμε στο φράγμα του Singleton και το φράγμα του Plotkin από το φράγμα γραμμικού προγραμματισμού.

Παράδειγμα 4.3.4. (i) *(Φράγμα του Singleton.) Έστω*

$$f(x) = q^{n-d+1} \prod_{j=d}^{n} \left(1 - \frac{x}{j}\right).$$

Από την Πρόταση 4.2.1(vi), $f(x) = \sum_{k=0}^{n} f_k K_k(x)$, *όπου το* f_k *δίνεται από*

$$f_k = q^{-n} \sum_{i=0}^{n} f(i) K_i(k).$$

Έχουμε

$$f(i) = q^{n-d+1} \left(1 - \frac{i}{d}\right)\left(1 - \frac{i}{d+1}\right) \ldots \left(1 - \frac{i}{n}\right) = q^{n-d+1} \frac{(d-i)(d+1-i)\ldots(n-i)}{d(d+1)\ldots n}$$

$$= q^{n-d+1} \frac{\binom{n-i}{n-d+1}}{\binom{n}{d-1}}.$$

Οπότε

$$f_k = q^{1-d} \sum_{i=0}^{d-1} \binom{n-i}{n-d+1} K_i(k) / \binom{n}{d-1} = \binom{n-k}{d-1} / \binom{n}{d-1} \geq 0,$$

όπου η τελευταία ισότητα έπεται από την Πρόταση 4.2.1(vi). *Έχουμε* $f_0 = 1$ *και* $f(i) = 0$ *για* $d \leq i \leq n$.

Οπότε, από το Θεώρημα 4.3.3, έπεται ότι $B_q(n, d) \leq f(0) = q^{n-d+1}$, *το οποίο είναι το φράγμα του Singleton (Θεώρημα 1.5.2).*

(ii) *(Φράγμα του Plotkin για* $B_2(2l+1, l+1)$.*) Θέτουμε* $q = 2$, $n = 2l + 1$ *και* $d = l + 1$. *Παίρνουμε* $f_1 = (l+1)/(2l+1)$ *και* $f_2 = 1/(2l+1)$, *έτσι ώστε*

$$f(x) = 1 + \frac{l+1}{2l+1} K_1(x) + \frac{1}{2l+1} K_2(x)$$

$$= 1 + \frac{l+1}{2l+1}(2l+1-2x) + \frac{1}{2l+1}(2x^2 - 2(2l+1)x + l(2l+1)).$$

Προφανώς, $f_k \geq 0$ *για* $1 \leq k \leq n$, *και επειδή το* $f(x)$ *είναι ένα πολυώνυμο 2ου βαθμού με* $f(l+1) = 0 = f(2l+1)$, *έχουμε* $f(i) \leq 0$ *για* $l+1 = d \leq i \leq n = 2l+1$.

Οπότε, από το Θεώρημα 4.3.3, έπεται ότι

$$B_2(2l+1, l+1) \leq f(0) = 1 + \frac{l+1}{2l+1}(2l+1) + \frac{1}{2l+1}l(2l+1) = 2l+2,$$

το οποίο είναι ακριβώς το φράγμα του Plotkin (Θεώρημα 1.5.3).

Βιβλιογραφία

[1] Bao Luong: Fourier Analysis on Finite Abelian Groups, Birkhäuser (2009).

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

[3] W. Cary Huffman, Vera Pless: Fundamentals of Error Correcting Codes, Cambridge University Press (2003).

[4] Rodney Coleman, On Krawtchouk polynomials. arXiv:1101.1798v1 [math.CA] (2011).