ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Πίνακες Hadamard και Εφαρμογές»

ΘΕΟΔΩΡΟΣ ΧΙΟΝΙΔΗΣ

ΑΜ: GE16051

Επιβλέπων: Παναγιώτης Ψαρράκος, Καθηγητής Ε.Μ.Π.

ΑΘΗΝΑ, 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Πίνακες Hadamard και Εφαρμογές»

ΘΕΟΔΩΡΟΣ ΧΙΟΝΙΔΗΣ

ΑΜ: GE16051

Τριμελής Επιτροπή: Β. Κανελλόπουλος, Καθηγητής Ε.Μ.Π.

Π. Στεφανέας, Αναπλ. Καθηγητής Ε.Μ.Π.

Π. Ψαρράκος, Καθηγητής Ε.Μ.Π. (Επιβλέπων)

ΑΘΗΝΑ, 2023

ΕΥΧΑΡΙΣΤΙΕΣ

Στο σημείο αυτό, θα ήθελα να ευχαριστήσω τον κύριο Παναγιώτη Ψαρράκο, επιβλέποντα καθηγητή της παρούσας διπλωματικής, για την καθοδήγηση και τη βοήθεια που μου παρείχε σε όλα τα στάδια εκπόνησης αυτής της εργασίας, καθώς και την οικογένεια μου που με στήριξε στο έπακρον σε κάθε βήμα και εγχείρημα της ζωής μου.

ΠΡΟΛΟΓΟΣ

Η παρούσα διπλωματική εργασία πραγματοποιήθηκε στο πλαίσιο των σπουδών μου στη Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών του Εθνικού Μετσόβιου Πολυτεχνείου, με σκοπό την απόκτηση του Διπλώματος.

Στην εργασία παρουσιάζεται ο πίνακας Hadamard που έχει μελετηθεί από πολλούς ερευνητές για τις εκτεταμένες εφαρμογές του, παραδείγματος χάριν στην θεωρία κωδικών, στην θεωρία σχεδιασμών, στην κρυπτογραφία και σε πολλά άλλα πεδία. Πιο συγκεκριμένα, δίνεται ο ορισμός του πίνακα Hadamard, καθώς και κάποια θεωρήματα και προτάσεις, ως επί το πλείστον μαζί και με τις αποδείξεις τούς.

Καταρχάς αξίζει να γίνει λόγος σχετικά με το πώς προέκυψε η ονομασία του συγκεκριμένου πίνακα. Ο πίνακας Hadamard πήρε το όνομά του από τον Jacques Hadamard ο οποίος ενώ προσπαθούσε να βρει πίνακες που ικανοποιούν την ισότητα στην ανισότητα $|detX|^2 \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |x_{ij}|$ με τα στοιχεία τους να ανήκουν στον μοναδιαίο δίσκο, βρήκε τετραγωνικούς πίνακες των τάξεων 12 και 20, με όλα τα στοιχεία 1 ή -1, τα οποία έχουν όλες τις γραμμές τους και τις στήλες τους ορθογώνιες. Τριάντα έξι χρόνια νωρίτερα από το Hadamard, το 1857, ο J.J. Sylverster μελέτησε τέτοιούς πίνακες και μάλιστα δημιούργησε πίνακες με όλα τα στοιχεία με 1 και -1, με ανά ζεύγος ορθογώνιες γραμμές και στήλες, για τάξεις μεγέθους όλων των δυνάμεων του 2, στην φημισμένη του εργασία "Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tessellated pavements in two or more colors with application to Newton's rule, ornamental tile work and the theory of numbers".

Η εργασία αποτελείται από πέντε κεφάλαια. Στο πρώτο κεφάλαιο, παρουσιάζονται κάποιοι ορισμοί και θεωρήματα από τη γραμμική άλγεβρα, το γινόμενο Kronecker (ένας πολλαπλασιασμός μεταξύ δύο πινάκων διαφορετικός από αυτόν που ξέρουμε) και στο τέλος δίνονται κάποια στοιχεία από την άλγεβρα και από τη θεωρία των αριθμών με σκοπό τη δημιουργία ενός σώματος Galois. Τα προηγούμενα αποτελούν σημαντικό κομμάτι της εργασίας και χρησιμοποιούνται σε όλη της την έκταση, έτσι ώστε ο αναγνώστης να μπορέσει να κατανοήσει τις έννοιες που παρουσιάζονται.

Στο δεύτερο κεφάλαιο δίνεται αρχικά ο ορισμός του πίνακα Hadamard και κάποια βασικά θεωρήματα με τις ιδιότητες τους. Στη συνέχεια, παρουσιάζονται θεωρήματα και προτάσεις, τα οποία αναφέρονται στο πότε δύο πίνακες Hadamard είναι ίσοι και στο πώς μπορούμε να

μετατρέπουμε έναν πίνακα Hadamard σε έναν κανονικοποιημένο πίνακα Hadamard. Προχωρώντας, γίνεται αναφορά στην πρόταση του Hadamard σχετικά με το μέγεθος του πίνακα και καθίσταται σαφές ότι τα μόνα μεγέθη πινάκων που μπορούν να υπάρξουν είναι αυτά που πρότεινε ο Hadamard και συγκεκριμένα 1, 2 και τα πολλαπλάσια του 4. Έπειτα ορίζονται κάποια άλλα είδη πινάκων Hadamard όπως ο γενικευμένος πίνακας Hadamard, ο οποίος δεν παίρνει τιμές μόνο 1 και -1 αλλά και τιμές στον μοναδιαίο δίσκο και ο skew-Hadamard πίνακας στον οποίο στηρίζονται οι πιο ισχυρές μέθοδοι κατασκευής πινάκων Hadamard.

Αφού ορίστηκαν οι βασικές ιδιότητες του πίνακα Hadamard εξετάζονται οι πρώτες κατασκευές πινάκων Hadamard. Πρώτος ο J.J. Sylvester, αφού πήρε δύο πίνακες Hadamard και το γινόμενο Kronecker έφτιαξε ένα καινούριο πίνακα Hadamard. Θα δοθούν παραδείγματα κατασκευής πίνακα Hadamard με αυτήν τη μέθοδο καθώς και τα συμπεράσματα που αντλούνται μέσα από αυτήν. Η δεύτερή κατασκευή πίνακα Hadamard πραγματοποιήθηκε εβδομήντα χρόνια αργότερα και συγκεκριμένα το 1933, όταν ένας ακόμα επιστήμονας, ο Paley, ασχολήθηκε με τους πίνακες Hadamard , πετυχαίνοντας τη γεφύρωση του χάσματος ανάμεσα στην γραμμική άλγεβρα και την άλγεβρα στους πίνακες Hadamard. Αξίζει να σημειωθεί ότι η δεύτερή κατασκευή του Paley σε αντίθεση με την πρώτη δεν προϋποθέτει προϋπάρχοντα πίνακα Hadamard.

Στο τρίτο κεφάλαιο παρουσιάζονται πιο σύνθετοι πίνακες Hadamard, μελετάται η τελευταία κατασκευή πινάκων με το διάνυσμα του Williamsome και γίνεται λόγος για την εφαρμογή στους πίνακες Skew-Hadamard. Στην κατηγορία των πιο σύνθετων πινάκων Hadamard ανήκουν οι οικείοι (amicable) πίνακες Hadamard οι οποίοι είναι πολύ χρήσιμοι για την κατασκευή πίνακα skew-Hadamard. Εξίσου σημαντικοί για την κατασκευή πινάκων skew-Hadamard είναι η κατασκευή με το διάνυσμα του Williamsome. Ένα χαρακτηριστικό της συγκεκριμένης κατασκευής συνιστά ότι απαιτούνται για αυτήν τέσσερις κυκλικοί πίνακες που ικανοποιούν την εξίσωση του Williamsome, με αποτέλεσμα τη δημιουργία ενός πίνακα Hadamard.

Στο τέταρτο κεφάλαιο, το οποίο είναι από τα σημαντικότερα της παρούσας διπλωματικής εργασίας γίνεται λόγος για την αξιοποίηση του πίνακα Hadamard στην θεωρία κωδικών. Οι πρώτοι που χρησιμοποίησαν τον πίνακα Hadamard στην θεωρία κωδικών ήταν η οι M. Hall, L. Baumert και S. Golomb στο πλαίσιο της εργασίας τους U.S. Jet Propulsion Laboratories (JPL) για την αποστολή φωτογραφιών από δορυφόρους. Πιο συγκεκριμένα τα πρώτα διαστημικά σκάφη που έστελνε το JPL στο διάστημα, είχαν αναλάβει τη λήψη και την αποστολή φωτογραφιών πίσω στη γη, οι οποίες όμως λόγω της απόστασης και του θορύβου έφταναν θολές και σε κάποιες περιπτώσεις ολόκληρες

γραμμές έλλειπαν. Στο πλαίσιο επιλύσεως του προβλήματος αυτού, οι τρείς επιστήμονες που αναφέραμε παραπάνω χρησιμοποίησαν τους πίνακες Hadamard για να δημιουργήσουν έναν νέο κωδικό με την ονομασία κωδικός Hadamard. Χάρις στον κωδικό Hadamard, μια δεκαετία αργότερα οι φωτογραφίες που έφταναν από τον διαστημικό σταθμό ήταν έγχρωμες και μεγαλύτερης ευκρίνειας. Είναι πολύ σημαντικό να γίνει μια εκτενής αναφορά σχετικά με το τι είναι αυτός ο κωδικός, τι είναι κωδική λέξη και να παρουσιαστούν οι βασικές ιδιότητες των κωδικών διόρθωσης σφαλμάτων. Επίσης, κρίνεται σημαντική και μία αναφορά στην ευρύτερη οικογένεια κωδικών στην οποία ανήκει ο κωδικός Hadamard, η οποία είναι ο κωδικός Reed Muller.

Στο τελευταίο κεφάλαιο, παρουσιάζεται ο τέλειος κωδικός ο οποίος δημιουργείται με τη χρήση πίνακα Hadamard. Επίσης, παρουσιάζεται και ο τελευταίος πίνακας Hadamard για τον οποίον γίνεται λόγος σε αυτήν τη διπλωματική εργασία, ο πίνακας quasi-Hadamard ο οποίος προσφέρει τη δυνατότητα δημιουργίας ενός βέλτιστου κωδικού και μάλιστα με τον πίνακα αυτόν έχω δημιουργήσει μια σχετική εφαρμογή την οποία θα σας παρουσιάσω.

Σύνοψη

Η παρούσα διπλωματική εργασία εκπονήθηκε με αφορμή τη μελέτη ενός τετραγωνικού πίνακα με όλα τα στοιχεία του να είναι 1 και -1, ο οποίος ονομάζεται πίνακας Hadamard. Ιδιαίτερο χαρακτηριστικό γνώρισμα του πίνακα είναι ότι έχει τις γραμμές του και τις στήλες του ορθογώνιες μεταξύ τους. Μία ακόμη βασική ιδιότητα του πίνακα είναι ότι όταν πολλαπλασιάζουμε έναν πίνακα Hadamard με τον ανάστροφό του, το γινόμενο που προκύπτει είναι ίσο με τον μοναδιαίο πίνακα επί την τάξη του πίνακα Hadamard. Πρώτος ο J.J.Sylvester μελέτησε τέτοιου είδους πίνακες το 1857. Ήταν εκείνος που βρήκε όλους τους πίνακες Hadamard της τάξης δύναμης του 2. Λίγα χρόνια αργότερα, το 1893 ο Jacques Hadamard στον οποίον οφείλουν την ονομασία τους οι πίνακες διαπίστωσε ότι υπάρχουν πίνακες Hadamard διαφορετικών τάξεων και όχι αποκλειστικά των δυνάμεων του 2 και συγκεκριμένα διατύπωσε την εικασία ότι υπάρχει πίνακας Hadamard για την τάξη 1, 2 και για πολλαπλάσια του 4. Ένας ακόμα επιστήμονας, ο Paley το 1933 κατάφερε να δημιουργήσει μια νέα κατασκευή πινάκων Hadamard η οποία γεφυρώνει το χάσμα μεταξύ της γραμμικής άλγεβρας με την άλγεβρα και έχει πάρει το όνομά του.

Αρχικά δίνονται κάποια βασικά μαθηματικά εργαλεία που θα αξιοποιηθούν σε όλη την έκταση της παρούσας διπλωματικής εργασίας. Γίνεται αναφορά σε στοιχεία από την γραμμική άλγεβρα που είναι χρήσιμα στην ανάλυση των πινάκων Hadamard. Έπειτα, δίνεται ο ορισμός του γινόμενου Kronecker, έναν πολλαπλασιασμό διαφορετικό από τον συνηθισμένο, μεταξύ δύο πινάκων ο οποίος είναι απαραίτητος για την πρώτη κατασκευή του Sylvester. Προχωρώντας, παρουσιάζονται κάποια βασικά στοιχεία από την άλγεβρα και τη θεωρία των αριθμών, απαραίτητα για τον ορισμό του σώματος Galois, το οποίο θα αξιοποιηθεί στην δεύτερη κατασκευή του Paley.

Στην συνέχεια παρουσιάζεται ο πίνακας Hadamard με τις ιδιότητες του. Μελετάται η μέθοδος κατασκευής του J.J. Sylvester για τους πίνακες Hadamard με τη χρήση του γινομένου Kronecker, δίνονται παραδείγματα πάνω στην κατασκευή και επισημαίνονται σημαντικά συμπεράσματα για τους πίνακες Hadamard που αντλούνται από την κατασκευή του Sylvester. Προχωρώντας, παρουσιάζεται η κατασκευή του Paley και τα αναγκαία μαθηματικά εργαλεία από την θεωρία των αριθμών για να την κατασκευή πινάκων Hadamard. Δίνεται ο ορισμός διαφορετικών ειδών πινάκων Hadamard, πιο συνθέτων από τους απλούς πίνακες Hadamard. Ολοκληρώνοντας την μελέτη των πινάκων Hadamard ακολουθεί η κατασκευή του Williamsome.

Στο τελευταίο μέρος της εργασίας, αντικείμενο μελέτης αποτελεί ο κώδικάς Hadamard. Ο κώδικάς αυτός δημιουργείται από έναν πίνακα Hadamard και ανήκει σε μια ευρύτερη οικογένεια κωδικών, την Reed-Muller. Στο τέλος κατασκευάζονται τέλειοι κωδικοί με την χρήση των πινάκων Hadamard και παρουσιάζεται η εφαρμογή που έχω δημιουργήσει για την καλύτερη εμπέδωση κατασκευής τέλειων κωδικών.

Λέξεις κλειδιά: Πίνακας Hadamard, κωδικός Hadamard, κατασκευή J.J.Sylvester, κατασκευή Paley, κατασκευή Williamsome, Amicable Hadamard πίνακας, όρια Plotkin, πίνακας quasi-Hadamard.

Abstract

This thesis was carried out in the context of studying a square matrix with all its elements being 1 and -1, which is called a Hadamard matrix. A distinctive characteristic of the matrix is that its rows and columns are orthogonal pair wise to each other. Another fundamental property of the matrix is that when we multiply a Hadamard matrix by its transpose, the resulting product is equal to the identity matrix multiplied by the order of the Hadamard matrix. The first study of such matrices was conducted by J.J. Sylvester in 1857. He found all Hadamard matrices of order 2's power. A few years later, in 1893, Jacques Hadamard, after whom the matrices are named, discovered that there are Hadamard matrices of different orders, not exclusively powers of 2. He specifically formulated the conjecture that there exists a Hadamard matrix for orders 1, 2, and 4k, where k is an integer. Another scientist, Paley, managed to create a new construction of Hadamard matrices in 1933, bridging the gap between linear algebra and algebraic theory. His construction is known as the Paley construction.

Initially, some basic mathematical tools that will be utilized throughout this thesis are presented. References are made to elements from linear algebra that are useful in the analysis of Hadamard matrices. The definition of the Kronecker product is then provided, which is a multiplication different from the conventional one, used in Sylvester's first construction. Moving forward, some essential elements from algebra and number theory are presented, necessary for the definition of the Galois field, which will be utilized in Paley's second construction.

Next, the Hadamard matrix is presented along with its properties. The method of construction by J.J. Sylvester using the Kronecker product is studied, and examples are given illustrating the construction, emphasizing the significant conclusions derived from Sylvester's construction. Subsequently, Paley's construction is presented, along with the necessary mathematical tools from number theory, to construct Hadamard matrices. The definition of different types of more complex Hadamard matrices beyond simple Hadamard matrices is given. The study of Hadamard matrices concludes with the construction of the Williamson matrix.

In the last part of the thesis, the focus of study is the Hadamard code. This code is created from a Hadamard matrix and belongs to a broader family of codes, the Reed-Muller codes. Finally, perfect codes are constructed using Hadamard matrices, and the application I have developed for better understanding the construction of perfect codes is presented.

Keywords: Hadamard matrix, Hadamard code, J.J. Sylvester construction, Paley construction, Williamsome construction, Amicable Hadamard matrix, Plotkin bounds, quasi-Hadamard matrix.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

1.1 Στοιχεία Γραμμικής Άλγεβρά

Ορισμός 1.1.1:

Ένας μεταθετικός πίνακας (πίνακας μετάθεσης, permutation matrix) είναι ένας τετραγωνικός πίνακας που έχει ακριβώς ένα στοιχείο 1 σε κάθε γραμμή και κάθε στήλη και 0 σε όλα τα υπόλοιπα στοιχεία.

Παράδειγμα 1.1.2:

Μεταθετικός πίνακας $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$.

Ορισμός 1.1.3:

Αν $A = (\alpha_{ij}) \in M_{\nu x \mu}$, τότε ο πίνακας που προκύπτει από τον A με εναλλαγή μεταξύ γραμμών και στηλών του λέγεται ανάστροφος πίνακας του A και συμβολίζεται με A^T, έχουμε δηλαδή $A^T = (\alpha_{ij}) \in M_{\nu x \mu}$.

Παράδειγμα 1.1.4:

Για τον πίνακα $A_{2x3} = \begin{bmatrix} 2 & 5 & -3 \\ 4 & -9 & 3 \end{bmatrix}$, ο ανάστροφος του είναι $A^T_{3x2} = \begin{bmatrix} 2 & 4 \\ 5 & -9 \\ -3 & 3 \end{bmatrix}$.

Ορισμός 1.1.5:

Ένας τετραγωνικός πίνακας $A = (\alpha_{ij}) \in M_\nu$ λέγεται:

(i) συμμετρικός, αν $A^T = A$, δηλαδή, αν a_{ij}, για κάθε $i, j = 1,2, \dots, \nu$,

(ii) αντισυμμετρικός, αν $A^T = -A$, δηλαδή αν $a_{ij} = -a_{ij}$ για κάθε $i, j = 1,2, \dots, \nu$.

Παράδειγμα 1.1.6:

(i) $A = \begin{bmatrix} 2 & 3 & 6 \\ 3 & -8 & -1 \\ 6 & -1 & 4 \end{bmatrix}$, $A^T = \begin{bmatrix} 2 & 3 & 6 \\ 3 & -8 & -1 \\ 6 & -1 & 4 \end{bmatrix}$. Αφού $A^T = A$, ο A είναι συμμετρικός.

(ii) $A = \begin{bmatrix} 0 & 8 & -4 \\ -8 & 0 & -1 \\ 4 & 1 & 0 \end{bmatrix}$, $A^T = \begin{bmatrix} 0 & -8 & 4 \\ 8 & 0 & 1 \\ -4 & -1 & 0 \end{bmatrix}$, $-A = \begin{bmatrix} 0 & -8 & 4 \\ 8 & 0 & 1 \\ -4 & -1 & 0 \end{bmatrix}$. Αφού $A^T = -A$, ο A είναι αντισυμμετρικός.

Ορισμός 1.1.7:

Ορίζουμε ως ανάποδο (reverse) μοναδιαίο πίνακα τον πίνακα R που έχει όλα τα στοιχεία στην ανάποδη διαγώνιο ίσα με 1 και όλα τα υπόλοιπα στοιχεία μηδενικά. Τότε ισχύει $R^2 = I$.

Παράδειγμα 1.1.8 :

Ο πίνακας $R = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ είναι ένας ανάποδος μοναδιαίος πίνακας και ισχύει:

$$R^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I.$$

Ορισμός 1.1.9 :

Ορίζουμε τον κυκλικό πίνακα $C = (c_{i,j})$ τάξης n αν $c_{i,j} = c_{1,j-i+1}$, $1 \leq i, j \leq n$.

Παράδειγμα 1.1.10 :

Ο πίνακας $C = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$ είναι ένας κυκλικός πίνακας τάξης 3.

Ορισμός 1.1.11 :

Ορίζουμε τον ανάποδο (reverse) κυκλικό πίνακα $B = (b_{ij})$ τάξης n αν $b_{i,j} = b_{1,i+j-1}$, $1 \leq i, j \leq n$.

Παράδειγμα 1.1.12 :

Ο πίνακας $B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$ είναι ένας ανάποδος κυκλικός πίνακας τάξης 3.

1.2 Γινόμενο Kronecker

Ορισμός 1.2.1:

Έστω $A \in \mathbb{R}^{mxn}$, $B \in \mathbb{R}^{pxq}$. Τότε το γινόμενο Kronecker (ή τανυστικό γινόμενο) του A και B ορίζεται ως ο πίνακας:

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \in \mathbb{R}^{mpxnq}.$$

Παράδειγμα 1.2.2:

Αν $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ και $B = \begin{bmatrix} 3 & -2 \\ 4 & 9 \end{bmatrix}$, τότε το γινόμενο Kronecker θα είναι:

$$A \otimes B = \begin{bmatrix} 1B & 1B \\ 1B & -1B \end{bmatrix} = \begin{bmatrix} 3 & -2 & 3 & -2 \\ 4 & 9 & 4 & 9 \\ 3 & -2 & -3 & 2 \\ 4 & 9 & -4 & -9 \end{bmatrix}.$$

Σημείωση 1.2.3:

Το γινόμενο Kronecker δεν ικανοποιεί την αντιμεταθετική ιδιότητα, δηλαδή γενικά ισχύει:
$A \otimes B \neq B \otimes A$.

Παράδειγμα 1.2.4:

Έστω ότι έχουμε το γινόμενο Kronecker των πινάκων B και A του Παραδείγματος 1.2.2:

$$B \otimes A = \begin{bmatrix} 3A & -2A \\ 4A & 9A \end{bmatrix} = \begin{bmatrix} 3 & 3 & -2 & -2 \\ 3 & -3 & -2 & 2 \\ 4 & 4 & 9 & 9 \\ 4 & -4 & 9 & -9 \end{bmatrix} \neq \begin{bmatrix} 3 & -2 & 3 & -2 \\ 4 & 9 & 4 & 9 \\ 3 & -2 & -3 & 2 \\ 4 & 9 & -4 & -9 \end{bmatrix} = \begin{bmatrix} 1B & 1B \\ 1B & -1B \end{bmatrix} = A \otimes B.$$

Άρα, $B \otimes A \neq A \otimes B$.

Ιδιότητες του γινομένου Kronecker

Θεώρημα 1.2.5:

Έστω $A \in \mathbb{R}^{mxn}$, $B \in \mathbb{R}^{rxs}$, $C \in \mathbb{R}^{nxp}$, και $D \in \mathbb{R}^{sxt}$. Τότε:

$$(A \otimes B)(C \otimes D) = AC \otimes BD \in \mathbb{R}^{mrxpt}.$$

Απόδειξη 1.2.6:

$$\begin{aligned}(A \otimes B)(C \otimes AD) &= \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix} \begin{bmatrix} c_{11}D & \cdots & c_{1p}D \\ \vdots & \ddots & \vdots \\ c_{n1}D & \cdots & c_{np}D \end{bmatrix} \\ &= \begin{bmatrix} \sum_{k=1}^{n} a_{1k}c_{k1}\,BD & \cdots & \sum_{k=1}^{n} a_{1k}c_{kp}\,BD \\ \vdots & \ddots & \vdots \\ \sum_{k=1}^{n} a_{mk}c_{k1}\,BD & \cdots & \sum_{k=1}^{n} a_{mk}c_{kp}\,BD \end{bmatrix} \\ &= AC \otimes BD.\end{aligned}$$

Θεώρημα 1.2.7:

Για οποιουσδήποτε πίνακες A και B, ισχύει $(A \otimes B)^{T} = A^{T} \otimes B^{T}$.

Απόδειξη 1.2.8:

$$(A \otimes B)^{T} = \begin{bmatrix} A_{11}B^{T} & \cdots & A_{m1}B^{T} \\ \vdots & \ddots & \vdots \\ A_{1n}B^{T} & \cdots & A_{mn}B^{T} \end{bmatrix} = A^{T} \otimes B^{T}.$$

Συνέπεια 1.2.9:

Αν $A \in \mathbb{R}^{nxn}$, $B \in \mathbb{R}^{mxm}$ είναι συμμετρικοί πίνακες, τότε και ο πίνακας $A \otimes B$ είναι συμμετρικός.

Θεώρημα 1.2.10:

Αν $A \in \mathbb{R}^{nxn}$, $B \in \mathbb{R}^{mxm}$ δεν είναι μοναδιαίοι πίνακες τότε, $(A \otimes B)^{-1} = (A^{-1} \otimes B^{-1})$.

Απόδειξη 1.2.11:

Από το Θεώρημα 1.2.5 ορίζουμε την παρακάτω σχέση:

$$(A \otimes B)(A^{-1} \otimes B^{-1}) = (AA^{-1} \otimes BB^{\otimes -1}) = I \otimes I = I,$$

όπου I μοναδιαίος πίνακας.

Θεώρημα 1.2.12:

Αν $A \in \mathbb{R}^{nxn}$, $B \in \mathbb{R}^{mxm}$ είναι κανονικοί πίνακες, τότε και ο πίνακας $A \otimes B$ είναι κανονικός.

Απόδειξη 1.2.13:

$(A \otimes B)^{\mathrm{T}}(A \otimes B) = (A^T \otimes B^T)(A \otimes B)$ από το Θεώρημα 1.2.7

$= A^T A \otimes B^T B$ από το Θεώρημα 1.2.5

$= AA^T \otimes BB^T$ αφού A και B είναι κανονική πίνακες

$= (A \otimes B)(A \otimes B)^{\mathrm{T}}$ από το Θεώρημα 1.2.5.

Συνέπεια 1.2.14:

Αν $A \in \mathbb{R}^{nxn}$ και $B \in \mathbb{R}^{mxm}$ είναι ορθογώνιοι πίνακες, τότε και ο πίνακας $A \otimes B$ είναι ορθογώνιος.

1.3 Στοιχεία Άλγεβρας

Το σώμα Galois (Galois Field) διαδραματίζει έναν σημαντικό ρόλο στην κατασκευή των πινάκων Hadamard. Για να κατανοήσουμε αρχικά τι είναι ένα σώμα, θα υπενθυμίσουμε κάποια γνωστά στοιχεία από την άλγεβρα. Στη συνέχεια, θα εισάγουμε τον δακτύλιο $\mathbb{Z}_n$, ο οποίος θα έχει καθοριστικό ρόλο στην κατασκευή του σώματος Galois. Τέλος, θα αναλύσουμε τη διαίρεση μεταξύ πολυώνυμων, θα την ορίσουμε και θα δώσουμε κάποια παραδείγματα. Στους παρακάτω ορισμούς και θεωρήματα δεν θα παρουσιαστούν αποδείξεις για λόγους συντομίας.

Ορισμός 1.3.1:

Ομάδα <G,*> είναι ένα σύνολο G, μαζί με μια διμελή πράξη * στο G τέτοια, ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

i) Η διμελής πράξη * είναι προσεταιριστική.

ii) Υπάρχει ένα στοιχείο e στο G τέτοιο, ώστε $e * x = x * e = x$ για κάθε $x \in G$.

iii) Για κάθε α στο G, υπάρχει ένα στοιχείο α' στο G με την ιδιότητα $\alpha' * \alpha = \alpha * \alpha' = e$.

Ορισμός 1.3.2:

Ομομορφισμός: Μια απεικόνιση φ μιας ομάδας G σε μια ομάδα G' λέγεται ομομορφισμός, αν $\varphi(ab) = \varphi(a)\varphi(b)$ για κάθε $a, b \in$G.

Ορισμός 1.3.3:

Ισομορφισμός φ:G→G' είναι ένας ομομορφισμός ένα προς ένα και επί G'. Ο συνήθης συμβολισμός είναι ο G≈G'.

Ορισμός 1.3.4:

Συνάρτηση ή απεικόνιση φ από ένα σύνολο A σε ένα σύνολο B είναι ένας κανόνας μέσω του οποίου σε κάθε στοιχείο a του A αντιστοιχίζεται ακριβώς ένα στοιχείο b του B. Λέμε ότι με την φ απεικονίζεται το a στο b, και ότι με την φ απεικονίζεται το A στο B. Ο κλασικός συμβολισμός που χρησιμοποιείται για να δηλωθεί ότι μέσω τους φ απεικονίζεται το a στο b είναι $\varphi(a) = b$.

Ορισμός 1.3.5:

Μια ομάδα G λέγεται αβελιανή αν η διμελής τους πράξη $*$ είναι αντιμεταθετική.

Ορισμός 1.3.6:

Αν G είναι μία πεπερασμένη ομάδα, τότε η |G| τους G είναι το πλήθος των στοιχείων τους G. Γενικά, για κάθε πεπερασμένο σύνολο S, |S| είναι το πλήθος των στοιχείων του S.

Ορισμός 1.3.7:

Ένας δακτύλιος <R,+,*> είναι ένα σύνολο R εφοδιασμένο με δύο διμελείς πράξεις + και *, τις οποίες αποκαλούμε πρόσθεση και πολλαπλασιασμό, και ορίζοντε στο R έτσι, ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

i) <R,+> είναι μια αβελιανή ομάδα.

ii) Ο πολλαπλασιασμός είναι προσεταιριστικός.

iii) Για κάθε a,b,c∈R, ισχύουν ο αριστερός επιμεριστικός κανόνας, $a*(b + c) = (a * b) + (a * c)$ και ο δεξιός επιμεριστικός κανόνας $(a + b)* c = (a * c) + (b * c)$.

Ορισμός 1.3.8:

Ένας δακτύλιος, στον οποίο ο πολλαπλασιασμός είναι αντιμεταθετική πράξη, λέγεται αντιμεταθετικός δακτύλιος.

Ορισμός 1.3.9:

Ένας δακτύλιος με πολλαπλασιαστικό ταυτοτικό στοιχείο 1, για το οποίο $1x = x1 = x$ για κάθε $x \in R$, λέγεται δακτύλιος με μοναδιαίο στοιχείο. Κάθε ουδέτερο στοιχείο του πολλαπλασιασμού λέγεται μοναδιαίο στοιχείο.

Θεώρημα 1.3.10:

Αν R είναι ένας δακτύλιος με μοναδιαίο στοιχείο, τότε αυτό το μοναδιαίο στοιχείο 1 είναι το μόνο πολλαπλασιαστικό ταυτοτικό στοιχείο του R.

Ορισμός 1.3.11:

Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο u του R λέγεται μονάδα του R αν έχει αντίστροφο στοιχείο στο R. Αν κάθε μη μηδενικό στοιχείο του R είναι μονάδα, τότε ο R λέγεται διαιρετικός δακτύλιος. Σώμα λέγεται ένας αντιμεταθετικός διαιρετικός δακτύλιος.

Το πολλαπλασιαστικό αντίστροφο ενός στοιχείου ενός δακτυλίου R είναι το στοιχέιο που, όταν πολλαπλασιαστεί με το αρχικό στοιχείο, δίνει το μοναδικό μοναδιαίο στοιχείο του δακτυλίου.

Παράδειγμα 1.3.12:

Το $\mathbb{Z}$ δεν είναι σώμα, αφού υπάρχουν στοιχεία όπως το 4 που δεν έχουν πολλαπλασιαστικό αντίστροφο στο $\mathbb{Z}$. Οι μόνες μονάδες στο $\mathbb{Z}$ είναι οι αριθμοί 1 και -1.

Έστω $\mathbb{Z}$, και $n > 2$ είναι σταθερός ακέραιος, για κάθε $a, b \in \mathbb{Z}$, ορίζουμε $a \equiv ab \pmod{(n)}$ αν και μόνο αν το n διαιρεί ακριβώς το $a - b$.

Θεωρούμε την κυκλική ομάδα $< \mathbb{Z}_n, + >$. Εάν ορίσουμε το γινόμενο των στοιχείων a και b, όπου $a, b \in \mathbb{Z}_n$, ως το υπόλοιπο της διαίρεσης του συνήθους γινομένου των ακεραίων με το n δηλαδή $(ab) mod n$, τότε μπορούμε να δείξουμε ότι $< \mathbb{Z}_n, +, * >$ είναι δακτύλιος.

Ορισμός 1.3.13:

Αν a και b είναι δύο μη μηδενικά στοιχεία ενός δακτυλίου R τέτοια, ώστε $\alpha\beta = 0$, τότε τα a και b λέγονται διαιρέτες του 0.

Παράδειγμα 1.3.14:

Η εξίσωση $x^2 - 7x + 10$ στον δακτύλιο $\mathbb{Z}_{10}$ μπορεί να λυθεί παραγοντοποιώντας το πολυώνυμο.

Έχουμε την παραγοντοποίηση $x^2 - 7x + 10 = (x - 2)(x - 5)$, η οποία ίσχύει για κάθε στοιχείο x του $\mathbb{Z}_{10}$. Επομένως, οι λύσεις τους εξίσωσης είναι:

- Για $x = 2$: $(2 - 2)(2 - 5) = (0)(-3) = 0$.
- Για $x = 5$: $(5 - 2)(5 - 5) = (3)(0) = 0$.
- Για $x = 7$: $(7 - 2)(7 - 5) = (5)(2) = 0$, αφού στο $\mathbb{Z}_{10}$, το γινόμενο $(5)(2)$ είναι ίσο με 0.

Άρα οι λύσεις της εξίσωσης $x^2 - 7x + 10$ στον $\mathbb{Z}_{10}$ είναι $x = 2,\ x = 5$ και $x = 7$.

Στο προηγούμενο παράδειγμα τα 2, 4, 5, 6, 8 είναι διαιρέτες του 0 στο $\mathbb{Z}_{10}$. Αφού $(2)(5) = (5)(2) = (4)(5) = (5)(4) = (6)(5) = (5)(6) = (8)(5) = (5)(8)$.

Θεώρημα 1.3.15:

Στον δακτύλιο $\mathbb{Z}_n$, οι διαιρέτες του 0 είναι ακριβώς εκείνα τα στοιχεία που δεν είναι πρώτα προς το n.

Από το προηγούμενο θεώρημα συμπεραίνουμε ότι αν ο αριθμός p είναι πρώτος, τότε στον δακτύλιο $\mathbb{Z}_p$ δεν έχει διαιρέτες του 0.

Ορισμός 1.3.16:

Ακέραια περιοχή λέγεται ένας αντιμεταθετικός δακτύλιος D με μοναδιαίο στοιχείο, που δεν περιέχει διαιρέτες του 0.

Θεώρημα 1.3.17:

Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Αν ο p είναι πρώτος αριθμός, τότε το $\mathbb{Z}_p$ είναι σώμα. Αυτό συμβαίνει διότι το $\mathbb{Z}_p$ είναι ένας αντιμεταθετικός δακτύλιος με μοναδιαίο στοιχείο και δεν περιλαμβάνει διαιρέτες του 0. Σύμφωνα με τον Ορισμό 1.3.13, αυτό το καθιστά ακέραια περιοχή. Επιπλέον, σύμφωνα με το Θεώρημα 1.3.15, κάθε πεπερασμένη ακέραια περιοχή είναι σώμα. Έτσι, το $\mathbb{Z}_p$ είναι ένα σώμα.

Θεώρημα 1.3.18:

Έστω $f(x)$ και $g(x)$ δύο μη μηδενικά πολυώνυμα που ανήκουν στο δακτύλιο $\mathbb{Z}_p[x]$, όπου p είναι ένας πρώτος αριθμός, και c είναι ένας δοσμένος αριθμός που ανήκει στο $\mathbb{Z}_p$. Τότε:

i) Υπάρχει ένα μοναδικό πηλίκο $q(x)$ και υπόλοιπο $r(x)$ στο δακτύλιο $\mathbb{Z}_p[x]$ τέτοια ώστε
$$f(x) = g(x)q(x) + r(x),$$
όπου ο βαθμός του $r(x)$ είναι μικρότερος από τον βαθμό του $g(x)$. Το πολυώνυμο $g(x)$ ονομάζεται διαιρέτης.

ii) Το υπόλοιπο από τη διαίρεση του $f(x)$ με το πολυώνυμο $(x - c)$ είναι ίσο με $f(c)$ αν το *f(x)* είναι διαιρέσιμο με το $(x - c)$ στον δακτύλιο $\mathbb{Z}_p[x]$.

Παράδειγμα 1.3.19:

Έστω τα πολυώνυμα $F(x) = 4x^2 - 5x - 1$ και $g(x) = x - 2$. Κάνοντας τη διαίρεση, παρατηρούμε ότι $q(x) = 4x + 3$ και το υπόλοιπο θα είναι $r(x) = 5$. Έχουμε:

$$F(x) = g(x)q(x) + r(x)$$

$$=> (x - 2)(4x + 3) + 5 = 4x^2 - 5x - 6 + 5 = 4x^2 - 5x - 1 = F(x).$$

Συνεπώς, η πρώτη προϋπόθεση ικανοποιείται. Από τη δεύτερη προϋπόθεση έχουμε ότι το πηλίκο της διαίρεσης $F(x)$ με το $(x - 2)$ έχει υπόλοιπο ίσο με $F(2) = 5$. Άρα ισχύει αφού $r(x) = 5$.

Γενικότερα, στον δακτύλιο $\mathbb{Z}_p[x]$, λέμε ότι το πολυώνυμο $g(x)$ διαιρεί το πολυώνυμο $f(x)$ (συμβολίζουμε $g(x) \mid f(x)$) αν και μόνο αν υπάρχει πολυώνυμο $q(x)$ στον δακτύλιο $\mathbb{Z}_p[x]$ τέτοιο ώστε $f(x) = g(x)q(x)$. Το πολυώνυμο $g(x)$ ονομάζεται τέλειος διαιρέτης του $f(x)$.

Θεώρημα 1.3.20:

Αν $f(x) \in Z_p$ και $c \in Z_p$, τότε το πολυώνυμο $x - c$ στον δακτύλιο $Z_p \in [x]$ είναι τέλειος διαιρέτης του $f(x)$ αν και μόνο αν $f(c) = 0$.

Παράδειγμα 1.3.21:

Έστω $f(x) = x^2 - 6x + 5$ και παρατηρούμε ότι για c =1 έχουμε:

$$f(c) = c^2 - 6c + 5 \xrightarrow{c=1} f(1) = 1^2 - 6 + 5 = 0.$$

Άρα, το πολυώνυμο $x - 1$ είναι τέλειος διαιρέτης του $f(x)$.

Λήμμα 1.3.22:

Έστω $f(x) \in Z_p$ και $c \in Z_p$, με p έναν τυχαίο πρώτο αριθμό.

i) Το πολυώνυμο $f(x)$ έχει έναν γραμμικό παράγοντα $x - c$ αν και μόνο αν $f(c) = 0$.

ii) Το πολυώνυμο $f(x)$ βαθμού 2 ή 3 είναι ανάγωγο αν και μόνο αν $f(c) \neq 0$ για τυχαιο c.

iii) Πάνω σ΄ ένα οποιοδήποτε σώμα ισχύει:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Ορισμός 1.3.23:

Αν για κάποιο σώμα F υπάρχει ένας θετικός ακέραιος n τέτοιος, ώστε $nx = 0$ για κάθε $x \in$ F, τότε ο μικρότερος τέτοιος φυσικός λέγεται χαρακτηριστική του F. Αν δεν υπάρχει τέτοιος φυσικός αριθμός, λέμε ότι ο F έχει χαρακτηριστική 0.

Λήμμα 1.3.24:

Έστω F ένα σώμα. Τότε ισχύει ότι είτε το σώμα F έχει χαρακτηριστική (character) μηδέν, δηλαδή F είναι ένα άπειρο σύνολο και περιέχει έναν ισομορφισμό αντιγραφής ρητών είτε η χαρακτηριστική του F είναι ένας πρώτος αριθμός. Αυτό σημαίνει ότι το σώμα F μπορεί να είναι είτε ένα πεπερασμένο σύνολο είτε άπειρο σύνολο που περιέχει ένα αντίγραφο ισομορφισμού του δακτυλίου Z_p, όπου ο αριθμός p είναι πρώτος.

Έστω Z_n ο δακτύλιος των ακέραιων mod n. Μπορεί να εκφραστεί με την παρακάτω μορφή: $f(x) = a + \alpha_1 x + \cdots + \alpha_k x^k$, όπου το x είναι η μεταβλητή και οι αριθμοί $\alpha_i \in Z_n$ καλούνται συντελεστές του πολυωνύμου πάνω Z_p. Περαιτέρω, όταν $\alpha_\kappa \neq 0$, τότε το κ ονομάζεται βαθμός του $f(x)$ και συμβολίζεται με deg $f(x)$. Αν $\alpha_\kappa = [1]$ το πολυώνυμο ονομάζεται μονικό (monic).

Ορισμός 1.3.25:

Ένα πολυώνυμο $f(x) \in$F$[x]$ λέγεται ανάγωγο πολυώνυμο (irreducible polynomial) πάνω από το σώμα F, αν δεν μπορούμε να γράψουμε το $f(x)$ ως γινόμενο δύο πολυωνύμων $g(x)$ και $h(x)$ στον F$[x]$, τα οποία να έχουν, και τα δύο, βαθμό μικρότερο από τον βαθμό του $f(x)$.

Παράδειγμα 1.3.26:

Το πολυώνυμο $f(x) = x^2 + 2x + 3$ δεν μπορεί να παραγοντοποιηθεί πάνω από το σώμα $\mathbb{Z}_5$. Διαφορετικά, αν υπήρχε ένα πολυώνυμο $h(x) = (x - a)(x - b)$ για κάποια στοιχεία $a, b \in \mathbb{Z}_5$, θα είχαμε τα εξής:

- $h(0) = 3 \neq 0$,
- $h(1) = 6 \bmod 2 = 1 \neq 0$,
- $h(2) = 11 \bmod 5 = 1 \neq 0$,
- $h(3) = 18 \bmod 5 = 3 \neq 0$,
- $h(4) = 27 \bmod 5 = 2 \neq 0$.

Από τους παραπάνω εκφράσεις, βλέπουμε ότι καμία από τους τιμές $h(0), h(1), h(2), h(3), h(4)$ δεν είναι ίση με το μηδέν. Αυτό σημαίνει ότι το πολυώνυμο $h(0)$ δεν μπορεί να παραγοντοποιηθεί από το $\mathbb{Z}_5$.

1.4 Σώμα Galois

Αφού τώρα έχουμε το μαθηματικό υπόβαθρο, είναι η κατάλληλη στιγμή να εξηγήσουμε το σώμα Galois. Το σώμα Galois είναι μια σημαντική μαθηματική έννοια που σχετίζεται με τη θεωρία των πεπερασμένων σωμάτων και τη θεωρία της αλγεβρικής επέκτασης.

Ορισμός 1.4.1:

Έστω $q = p^n$, όπου p είναι πρώτος. Τότε F_q ή GF(q) δηλώνει ένα μοναδικό σώμα τάξης q που ονομάζεται σώμα Galois τάξης q.

Το σώμα Galois F είναι ένα σώμα F του οποίου το σετ F έχει πεπερασμένο αριθμό στοιχείων. Από Λήμμα 1.3.22, το $\mathbb{Z}_p$ είναι ένα σώμα Galois GF(p), όπου p είναι πρώτος αριθμός.

Θεώρημα 1.4.2:

Έστω F=GF(S), είναι ένα σώμα Galois με s στοιχεία και F^*=F- {0}. Τότε:

i) Αν s είναι ένας τυχαίος αριθμός της μορφής $s = p^n$, όπου $n \geq 1$ και ο p είναι ένας πρώτος αριθμός, τότε η χαρακτηριστική του F είναι ο αριθμός p.

ii) Η ομάδα F^* υπό τον πολλαπλασιασμό του F είναι κυκλική ομάδα. Αυτό σημαίνει ότι υπάρχει ένα στοιχείο $a \in F^*$ τέτοιο, ώστε $F^*=\{ a^0=1, a^1, a^2, \ldots, a^{s-2}\}$. Το στοιχείο "$a$" το οποίο παράγει F^* καλείται πρωτογενές στοιχείο(primitive element).

iii) Έστω $q(x) \in \mathbb{Z}_p$ είναι ανάγωγο πολυώνυμο στον δακτύλιο $\mathbb{Z}_p$, όπου p είναι ένας πρώτος αριθμός και είναι επίσης η χαρακτηριστική του F. Τότε το πολυώνυμο $q(x)$ διαιρεί το πολυώνυμο $x^{s-1} - 1$.

iv) Το πολυώνυμο $x^s - x$ είναι το γινόμενο όλων των μονικών ανάγωγων πολυώνυμων στον $\mathbb{Z}_p[x]$ με βαθμό που διαιρεί τον αριθμό n, όπου p είναι ένας πρώτος αριθμός και είναι η χαρακτηριστική του F και $s = p^n$.

v) Υπάρχουν σώμα Galois με p^n στοιχεία για κάθε πρώτο αριθμό p.

Θεώρημα 1.4.3:

Έστω F={0, a_1, a_2,…, a_{s-1}} είναι GF(s), $s= p^n$ όπου p είναι πρώτος αριθμός. Τότε το πολυώνυμο $x^s - x$ στον $\mathbb{Z}_p[x]$ παραγοντοποιείται στο γραμμικό παράγοντα:

$$x^s - x = x(x - a_1)(x - a_2) \dots (x - a_{s-1}).$$

Έστω σώμα Galois F με $s=p^n$ στοιχεία. Τότε το ανάγωγο πολυώνυμο $f(x) \in \mathbb{Z}_p$ καλείται πρωτογενές ανάγωγο πολυώνυμο (primitive irreducible polynomial) αν και μόνο αν το $f(x)$ διαιρεί το $x^m - 1$ για $m = p^n - 1 = s - 1$ αλλά για όχι μικρότερο m.

Κατασκευή σώματος Galois

Θα κατασκευάσουμε σώμα Galois τάξης s, όπου $s= p^n$, p είναι πρώτος αριθμός, και n είναι ακέραιος.

Πρώτη περίπτωση

Όταν $n = 1$, έχουμε $s = p$ τότε από το Λήμμα 1.3.22 ο δακτύλιος Z_p είναι ένα σώμα Galois GF(p) κάτω από την πρόσθεση και τον πολλαπλασιασμό mod p.

Παράδειγμα 1.4.4:

Κατασκευάζουμε το F=GF(7). Το 7 είναι πρώτος αριθμός, οπότε εμείς έχουμε $F=Z_7$={0,1,2,3,4,5,6} υπό την πρόσθεση και τον πολλαπλασιασμό mod7. Όπως στους παρακάτω πίνακες:

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Δεύτερη περίπτωση

Όταν $n \geq 2$, μπορούμε να ορίσουμε το πολυώνυμο $x^s - x$ στον δακτύλιο $\mathbb{Z}_p[x]$. Για να υλοποιήσουμε την παρακάτω δομή, ακολουθούμε τα εξής βήματα:

1. **Βήμα πρώτο:** Παραγοντοποιούμε το πολυώνυμο $x^s - x$ σε ανάγωγα πολυώνυμα στον $\mathbb{Z}_p[x]$. Διαλέγουμε όλα τα ανάγωγα πολυώνυμα σε αυτήν την παραγοντοποίηση που έχουν βαθμό n. Έστω ότι έχουμε k τέτοια πολυώνυμα και τα ονομάζουμε $g_1(x)$, $g_2(x)$, …, $g_k(x)$.
2. **Βήμα δεύτερο:** Από τους παράγοντες $g_i(x)$ διαλέγουμε τα $g_i(x)$ τα οποία είναι πρωτογενή. Έτσι μπορούμε να δημιουργήσουμε ένα σώμα Galois χρησιμοποιώντας οποιοδήποτε από τα ανάγωγα πολυώνυμα $g_i(x)$.
3. **Βήμα τρίτο:** Υποθέτουμε ότι έχουμε επιλέξει ένα πρωτογενές ανάγωγο πολυώνυμο τάξης n από το βήμα δύο. Έστω ότι καλούμε αυτή την επιλογή $g(x)$. Αν δεν μπορούμε να αποφασίσουμε ποιο πρωτογενές πολυώνυμο να επιλέξουμε, μπορούμε απλά να διαλέξουμε οποιοδήποτε $g_i(x)$ από το δεύτερο βήμα.
4. **Βήμα τέταρτο:** Έστω F = { $f(x) \in \mathbb{Z}_p[x]$: βαθμός του $f(x) \leq n$-1} F είναι ένα σύνολο πολυώνυμων της μορφής $a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$ με $a_i \in \mathbb{Z}_p[x]$. Έστω πολυώνυμα f_1(x), f_2(x) από την F. Για να προσθέσουμε $f_1(x)$ και $f_2(x)$, προσθέτουμε όρο με όρο κάτω από το mod$(p, g(x))$. Για να πολλαπλασιάσουμε $f_1(x)$ με $f_2(x)$, πολλαπλασιάζουμε όρο με όρο κάτω από το mod$(p, g(x))$. Ονομάζουμε αυτήν τη διαδικασία πρόσθεσή και πολλαπλασιασμό κάτω από τη mod$(p, g(x))$ αριθμητική (arithmetic).
5. **Βήμα πέμπτο**: Το σύνολο F ορίζεται κάτω από το mod$(p,g(x))$ αριθμητική είναι σώμα Galois τάξεως p^n.

Θα παραθέσουμε παραδείγματα GF(9).

Παράδειγμα 1.4.5:

Κατασκευάζουμε GF(9). Παρατηρούμε ότι $9=3^2$, και αφού ο 3 είναι πρώτος αριθμός, θα δουλέψουμε για το σώμα Galois με το Z_3.

Παραγοντοποιούμε $x^9 - x$ σε ανάγωγο πολυώνυμο στο Z_3[x]:

$$x^9 - x = x(x^8 - 1) = x(x^4 - 1)(x^4 + 1)$$
$$= x(x - 1)(x + 1)(x^2 + 1)(x^2 + 2x + 2)(x^2 + x + 2).$$

Από το θεώρημα υπολοίπων, τα πολυώνυμα $g_1(x) = x^2 + 1$, $g_2(x) = x^2 + 2x + 2$ και $g_3(x) = x^2 + x + 2$ είναι ανάγωγα. Από αυτά τα πολυώνυμα το $g_1(x)$ δεν είναι πρωτογενές, αφού

$x^2 + 1 / x^4 + 1$. Από την παραγοντοποιήσει του $x^9 - x$ το $g_2(x)$ και $g_3(x)$ είναι και τα δύο πρωτογενή ανάγωγα πολυώνυμα. Θα εργαστούμε με το $g_2(x)$.

Θεωρούμε ότι το σετ F= $\{a+a_1x: a \in Z_3[x]\}$, κάτω από το mod(3, $g_2(x)$). Τότε F έχει 9 στοιχεία τους παρακάτω: a = 0, 1, 2 και a_1 = 0, 1, 2 και από το Θεώρημα 1.4.2(ii):
F^* = F-{0} = {1, x, 1+x, 2x, 1+2x, 2, 2+x, 2+2x } είναι μία κυκλική πολλαπλασιαστική ομάδα και x είναι πρωτογενές στοιχείο του F^*. Για να το επιβεβαιώσουμε αυτό υπολογίζουμε τις δυνάμεις του x χρησιμοποιώντας το mod(3, $g_3(x)$) αριθμητικά, οπότε έχουμε:

0, x^0=1, x^1= x, x^2= x+1 (αντικαθιστώντας το x^2 με x+1), $x^3 = x\,x^2 = x + 1 + x = 2x + 1$,

$x^4 = x\,x^3 = 2x^2 + x = 2x + x + 2 = 2$, $x^5 = x\,x^4 = 2x$, $x^6 = x\,x^5 = 2\,x^2 = 2(x+1) = x + 2$,

$x^7 = x\,x^6 = 2x^2 + 2x = 2x + 2x + 2 = x + 2$, $x^8 = x^2 + 2\,x = x + 2\,x + 1 = 1$.

Επομένως, οι δυνάμεις του x παράγουν τα πρωτογενή στοιχεία του F^* και έχουμε τους παρακάτω πίνακες:

$+_3$	**0**	**1**	**X**	**X+1**	**2X+1**	**2**	**2X**	**2X+2**	**X+2**
0	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
1	1	2	x+1	x+2	2x+2	0	2x+1	2x	x
X	x	x+1	2x	2x+1	1	x+2	0	2	2x+2
X+1	x+1	x+2	2x+1	2x+2	2	x	1	0	2x
2X+1	2x+1	2x+2	1	2	x+2	2x	x+1	x	0
2	2	0	x+2	x	2x	1	2x+2	2x+1	X+1
2X	2x	2x+1	0	1	x+1	2x+2	x	x+2	2
2X+2	2x+2	2x	2	0	x	2x+1	x+2	x+1	1
X+2	x+2	x	2x+2	2x	0	x+1	2	1	2x+1

$*_3$	**0**	**1**	**X**	**X+1**	**2X+1**	**2**	**2X**	**2X+2**	**X+2**
0	0	0	0	0	0	0	0	0	0
1	0	1	x	x+1	2x+1	2	2x	2x+2	x+2
X	0	x	x+1	2x+1	2	2x	2x+2	x+2	1
X+1	0	x+1	2x+1	2	2x	2x+2	x+2	1	x
2X+1	0	2x+1	2	2x	2x+2	x+2	1	x	x+1
2	0	2	2x	2x+2	x+2	1	x	x+1	2x+1
2X	0	2x	2x+2	x+2	1	x	X+1	2x+1	2
2X+2	0	2x+2	x+2	1	x	x+1	2x+1	2	2x
X+2	0	x+2	1	x	x+1	2x+1	2	2x	2x+2

Τετραγωνικό υπόλοιπο

Το τετραγωνικό υπόλοιπο είναι ένας όρος που χρησιμοποιείται στη θεωρία αριθμών και την αριθμητική. Έστω ένα σώμα Galois GF(s) τάξεις s, όπου $s = p^n$, με p είναι περιττός πρώτος αριθμός, ορίζουμε τον όρο "τετραγωνικό υπόλοιπο" για ένα στοιχείο $a \in GF(s)$ ως εξής. Ένα στοιχείο α είναι τετραγωνικό υπόλοιπο αν και μόνο αν υπάρχει ένα στοιχείο $b \in GF(s)$ τέτοιο ώστε $a = b^2$. Αν δεν υπάρχει τέτοιο b, τότε υπάρχει 'a' που ονομάζεται "μη τετραγωνικό υπόλοιπο". Σημειώνουμε ότι το 0 και 1 είναι πάντα τετραγωνικά υπόλοιπα.

Έστω x είναι πρωτογενές στοιχείο της πολλαπλασιαστικής ομάδας $F^*=F-\{0\}$, όπου F είναι $GF(s)$, $s = p^n$, p είναι περιττός πρώτος αριθμός. Τότε όλα τα τετραγωνικά υπόλοιπα της F ανήκουν στο σύνολο QR={ $x^0, x^2, x^4,\ldots, x^{s-3}$} όπου το QR σημαίνει "quadratic residuals", δηλαδή τετραγωνικά υπόλοιπα.

Παράδειγμα 1.4.6:

Θα βρούμε τα QR του GF(7) και GF(9).

Για GF(7) το 3 είναι ο πρωτόγονος αριθμός του F αφού:

$$(3^1, 3^2, 3^3, 3^4, 3^5, 3^6) = (3,2,6,4,5,1).$$

Τα τετραγωνικά υπόλοιπα θα είναι QR={$0,3^0,3^2,3^4$}={0,1,2,4}.

Για GF(9) το x είναι ο πρωτόγονος αριθμός του F αφού:

$$(x^1, x^2, x^3, x^4, x^5, x^6, x^7, x^8) = (x, x+1, 2x+1, 2, 2x, 2x+2, x+2, 1).$$

Τα τετραγωνικά υπόλοιπα θα είναι QR={0, x^0, x^2, x^4, x^6 }={0, 1, x+1, 2, 2x+2 }.

ΚΕΦΑΛΑΙΟ 2. ΠΙΝΑΚΕΣ HADAMARD

Έστω X=(x_{ij}) ένας πίνακας τάξης n με στοιχεία του βρίσκονται στον μοναδιαίο δίσκο, δηλαδή $|x_{ij}| \leq 1$ για κάθε i, j. Στα τέλη του 19 αιώνα, το 1893, ο Jacques Hadamard απέδειξε ότι $|detX| \leq n^{\frac{n}{2}}$. Η συγκεκριμένη ανισότητα είναι γνωστή ως ανισότητα ορίζουσας Hadamard. Η ισότητα ισχύει όταν τα στοιχεία έχουν μέτρο $|x_{i,j}|$=1 και οι γραμμές (ή στήλες) του πίνακα είναι ορθογώνιες μεταξύ τους (pairwise orthogonal). Συνεπώς, ισχύει $X\overline{X^T} = nI$, όπου I είναι ο μοναδιαίος πίνακας τάξης n.

Όταν ένας πίνακας X έχει τους ακόλουθες ιδιότητες, δηλαδή τα στοιχεία του είναι 1 ή -1 και οι γραμμές και οι στήλες του είναι ορθογώνιες, τότε ο πίνακας X έχει μέγιστη ορίζουσα. Ο Hadamard ανακάλυψε πίνακες με αυτές τις ιδιότητες για μεγέθη 12 και 20, και έτσι το όνομα του έγινε συνώνυμο με πίνακες τέτοιου είδους.

2.1. Πίνακας Hadamard

Ορισμός 2.1.1: (Πίνακας Hadamard)
Ένας τετραγωνικός πίνακας H ο οποίος έχει στοιχεία 1 ή -1 καλείται πίνακας Hadamard (Hadamard matrix) αν και μόνο αν οι γραμμές (στήλες) του είναι ορθογώνιες μεταξύ τους.

Λήμμα 2.1.2:
Έστω H, ένας πίνακας Hadamard τάξης n. Τότε ισχύει:

i) $HH^T = nI$, όπου I είναι ο μοναδιαίος πίνακας τάξης n.

ii) $|detH| = n^{\frac{1}{2}n}$.

iii) $HH^T = H^T H$.

Απόδειξη 2.1.3:
Από τον ορισμό του πίνακα Hadamard έχουμε άμεσα τις ιδιότητες (i) και (ii).
Για την ιδιότητα (iii) έχουμε $HH^T = hI_h$, $H^T = hH^{-1}$, και τότε ισχύει ότι $H^T H = hI_h$.

Συνέπεια 2.1.4:
Αν ο πίνακας H είναι πίνακας Hadamard τάξης n, τότε και ο H^{T} είναι πίνακας Hadamard.

Απόδειξη 2.1.5: Αφού $HH^T = nI_n$, τότε $H^{-1} = \frac{1}{n}H^T$. Άρα το $H^T(H^T)^T$=$nH^{-1}H$=nI_n.

Παράδειγμα 2.1.6:

Έστω πίνακας $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Θέλουμε να ελέγξουμε αν είναι πίνακας Hadamard. Υπολογίζουμε τον ανάστροφο $A^T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, και $AA^T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 2I_2$.

Άρα ισχύει η σχέση $HH^T = nI_2$ και A είναι ένας πίνακας Hadamard τάξης 2.

Η αναστροφή δεν είναι η μόνη λειτουργία που μπορούμε να εφαρμόσουμε σε έναν πίνακα Hadamard για να παραχθεί ένας νέος πίνακα Hadamard. Δεδομένου ότι οι γραμμές και οι στήλες ενός πίνακα Hadamard είναι ορθογώνιες μεταξύ τους, είναι εύκολο να δούμε ότι αν πολλαπλασιάσουμε τις γραμμές η τις στήλες με -1 ενός πίνακα Hadamard, ο προκύπτων πίνακας έχει ορθογώνιες γραμμές και στήλες μεταξύ τους, και επομένως είναι ένας πίνακας Hadamard.

Αντίστοιχα, εάν αναδιατάξουμε τις γραμμές ή τις στήλες ενός πίνακα Hadamard, ο πίνακας που προκύπτει μπορεί να θεωρηθεί ως πίνακας Hadamard. Αυτές οι παρατηρήσεις συνοψίζονται παρακάτω.

Ορισμός 2.1.7:

Δύο πίνακες Hadamard ονομάζονται Hadamard-ισοδύναμοι ή H-ισοδύναμοι αν ο ένας μπορεί να αποκτηθεί από τις παρακάτω πράξεις:

i) Αλλαγή γραμμής ή στήλης.

ii) Πολλαπλασιασμός οποιασδήποτε γραμμής ή στήλης με -1.

Συνέπεια 2.1.8:

Έστω H πίνακας Hadamard τάξης n και έστω P_1, P_2 τετραγωνικοί πίνακες μεταθέσεων τάξης n. Τότε ο πίνακας P_1HP_2 είναι ένας πίνακας Hadamard της τάξης n.

Απόδειξη 2.1.9:

Έστω P_1 και P_2 είναι πίνακες μετάθεσης τότε ισχύει ότι $P_1P_1^{\mathrm{T}} = P_2P_2^{\mathrm{T}} = I_n$. Χρησιμοποιώντας το προηγούμενο έχουμε: $(P_1HP_2)(P_1HP_2)^{\mathrm{T}} = P_1HP_2P_1^{\mathrm{T}}H^{\mathrm{T}}P_2^{\mathrm{T}} = P_1HH^{\mathrm{T}}P_1^{\mathrm{T}} = nP_1P_1^{\mathrm{T}} = nI_n$.

Παράδειγμα 2.1.10:

Έχουμε τον πίνακα $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ και τους πίνακες $P_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $P_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Θέλουμε να δείξουμε ότι ο πίνακας P_1AP_2 είναι πίνακας Hadamard. Οπότε έχουμε

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

Άρα έχουμε

$$(P_1AP_2)(P_1AP_2)^{\mathrm{T}} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 2I_n.$$

Ο πίνακας P_1AP_2 είναι πίνακας Hadamard τάξης 2.

Ο Ορισμός 2.1.7 μας έδωσε μια μέθοδο μετατροπής ενός πίνακα Hadamard τάξης n σε έναν άλλο μέσω μεταθέσεων και αλλαγής προσήμων γραμμών και στηλών.

Ορισμός 2.1.11: Ονομάζουμε δύο πίνακες Hadamard H και K τάξης n, ισοδύναμους εάν υπάρχουν δύο πίνακες μεταθέσεων P_1 και P_2 τέτοιοι ώστε $H = P_1 K P_2$.

Ο M. Hall είναι ο πρώτος που αναγνώρισε ισοδυναμία των πινάκων Hadamard το 1961 στην αναφορά ερευνών του JPL (Jet Propulsion Laboratory). Ανακάλυψε ότι οι πίνακες Hadamard τάξεων 1, 2, 4, 8 και 12 είναι μοναδικοί, ενώ υπάρχουν 5 ισοδύναμες κλάσεις για μέγεθος 16 και 3 ισοδύναμες κλάσεις για μέγεθος 20. Αυτή τη στιγμή έχουν βρεθεί 60 ισοδύναμοι πίνακες Hadamard για πίνακες μεγέθους 24 και 487 ισοδύναμες κλάσεις για πίνακες μεγέθους 28.

Ορισμός 2.1.12: Ονομάζουμε έναν πίνακα Hadamard κανονικοποιημένο πίνακα Hadamard αν η πρώτη γραμμή και η πρώτη στήλη αποτελείται αποκλειστικά από 1.

Παράδειγμα 2.1.13*:* Ο παρακάτω πίνακας είναι ένας κανονικοποιημένος Hadamard πίνακας:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Θεώρημα 2.1.14:
Κάθε πίνακας Hadamard είναι ισοδύναμος με έναν κανονικοποιμένο πίνακα Hadamard.

Απόδειξη 2.1.15:
Αν έχουμε έναν μη κανονικοποιημένο πίνακα Hadamard, μπορούμε να τον μετατρέψουμε σε κανονικοποιημένο πίνακα Hadamard με την εξής διαδικασία:

1) Αν το στοιχείο α_{11} είναι -1 πολλαπλασιάζουμε την πρώτη γραμμή με -1.
2) Στην συνέχεια, για κάθε στοιχείο της πρώτης γραμμής που είναι ίσο με -1, αλλάζουμε το πρόσημο στην αντίστοιχη στήλη.
3) Ακολουθώντας τη διαδικασία για κάθε στοιχείο της πρώτης στήλης που είναι ίσο με -1, αλλάζοντας το πρόσημο στην αντίστοιχη γραμμή.

Με αυτόν τον τρόπο, το αποτέλεσμα θα είναι ένας κανονικοποιημένος πίνακας Hadamard, καθώς όλα τα στοιχεία της πρώτης γραμμής και της πρώτης στήλης θα είναι ίσα με 1. Αυτό συμβαίνει επειδή οι πίνακες Hadamard είναι κλιμακωτοί και η μεταβολή του πρόσημου μιας γραμμής ή στήλης δεν επηρεάζει την ιδιότητα Hadamard του πίνακα.

Παράδειγμα 2.1.16:

Έχουμε τον πίνακα Hadamard $A=\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$ που δεν είναι κανονικοποιημένος πίνακας Hadamard και θέλουμε να τον κάνουμε. Αρχικά πολλαπλασιάζουμε με -1 τη δεύτερη γραμμή και παίρνουμε τον πίνακα:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}.$$

Έπειτα πολλαπλασιάζουμε με -1 την τέταρτη γραμμή και παίρνουμε τον πίνακα:

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \qquad (2.1)$$

Συνεπώς, ο πίνακας (2.1) είναι ένας κανονικοποιημένος πίνακας Hadamard και ισοδύναμος με τον A.

Το επόμενο λήμμα θα είναι ιδιαίτερα χρήσιμο στην θεωρία κωδικών και διόρθωσης σφαλμάτων. Οπότε στο Κεφάλαιο 4 θα δούμε πως οι πίνακες Hadamard μπορούν να χρησιμοποιηθούν για να δημιουργήσουμε έναν κωδικό διορθώσεις σφαλμάτων.

Λήμμα 2.1.17:

Σε κάθε κανονικοποιημένο πίνακα Hadamard ισχύει ότι για οποιοδήποτε ζευγάρι γραμμών, το ήμισυ των στοιχείων τους ίσα. Επιπλέον, οποιεσδήποτε τρείς γραμμές του πίνακα θα έχουν το ένα τέταρτο των στοιχείων τους ίσα.

Αυτές οι ιδιότητες είναι χαρακτηριστικές των κανονικοποιημένων πινάκων Hadamard και μας παρέχουν μια καλύτερη κατανόηση του τρόπου με τον οποίο τα στοιχεία τους συσχετίζονται μεταξύ τους.

Παράδειγμα 2.1.18:

Έχουμε τον παρακάτω πίνακα και συγκρίνουμε ανά δύο τις γραμμές ένα, δύο και δύο, τρία, και ανά τρείς τις γραμμές ένα, τρία και τέσσερα για να παρατηρήσουμε πόσα στοιχεία έχουν ισοδύναμα.

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

(i) Οι γραμμές ένα και δύο έχουν δύο ίσα στοιχεία στα τέσσερα.
(ii) Οι γραμμές δύο και τρία έχουν δύο ίσα στοιχεία στα τέσσερα.
(iii) Οι γραμμές ένα, τρία και τέσσερα έχουν ένα ίσο στοιχείο στα τέσσερα.

Έχοντας ορίσει τους πίνακες Hadamard, το ερώτημα που προκύπτει φυσικά είναι εάν υπάρχει πίνακας Hadamard για κάθε τάξης μεγέθους ή μόνο για συγκεκριμένες τάξεις μεγέθους. Το παρακάτω θεώρημα και η απόδειξή του απαντούν σε αυτό το ερώτημα.

Θεώρημα 2.1.19*:*
Αν υπάρχει πίνακας Hadamard τάξης n, τότε ο αριθμός n είναι είτε 1, 2 ή θετικός πολλαπλάσιο του 4.

Απόδειξη 2.1.20:
Για μεγέθη 1 και 2 έχουμε τους πίνακες [1] και $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ αντίστοιχα, οι οποίοι είναι πίνακες Hadamard.

Για έναν πίνακα Hadamard H τάξης n >2 υποθέτουμε, χωρίς βλάβη της γενικότητας, ότι είναι ένας κανονικοποιημένος πίνακας Hadamard. Αν δεν είναι κανονικοποιημένος, τότε μπορούμε να τον κανονικοποιήσουμε χρησιμοποιώντας το Θεώρημα 2.1.14.

Στη συνέχεια, μεταθέτουμε τις στήλες του H έως ότου οι πρώτες στήλες "a" έχουν τα πρώτα τρία στοιχεία 1, 1, 1, οι επόμενες στήλες "b" έχουν τα πρώτα τρία στοιχεία 1, 1, -1, οι επόμενες στήλες "c" έχουν τα πρώτα τρία στοιχεία 1, -1, 1 και οι τελευταίες στήλες "d" έχουν τα πρώτα τρία στοιχεία 1, -1, -1. Η τάξης του H είναι n, μαζί με την ορθογωνιότητα των γραμμών του H έχουμε το παρακάτω σύστημα εξισώσεων:

$$\begin{cases} a+b+c+d=n \ \ (H\ \tau\acute{\alpha}\xi\eta\ του\ H\ \epsilon\acute{\iota}ναι\ n) \\ a+b-c-d=0 (H\ \gamma\rho\alpha\mu\mu\acute{\eta}\ \acute{\epsilon}να\ και\ \delta\acute{\upsilon}ο\ \epsilon\acute{\iota}ναι\ ορθογώνιες\ ) \\ a-b+c-d=0 (H\ \gamma\rho\alpha\mu\mu\acute{\eta}\ \acute{\epsilon}να\ και\ τρία\ \epsilon\acute{\iota}ναι\ ορθογώνιες\ ) \\ a-b-c+d=0 (H\ \gamma\rho\alpha\mu\mu\acute{\eta}\ \delta\acute{\upsilon}ο\ και\ τρία\ \epsilon\acute{\iota}ναι\ ορθογώνιες\ ) \end{cases}.$$

Έχοντας ένα σύστημα με τέσσερις αγνώστους (a, b, c, d) και τέσσερις εξισώσεις, το σύστημα έχει μοναδική λύση. Αυτή η μοναδική λύση είναι $a=b=c=d=n/4$. Φυσικά οι μεταβλητές a, b, c, d πρέπει να είναι ακέραιοι, και επομένως το n είναι πολλαπλάσιο του 4.

Έχοντας βρει ότι το n είναι είτε 1, 2 ή πολλαπλάσιο του 4, αυτό είναι μια απαραίτητη προϋπόθεση για την ύπαρξη πινάκων Hadamard τάξης n. Ωστόσο, δεν γνωρίζουμε αν αυτή η συνθήκη είναι επίσης επαρκής για την ύπαρξη πινάκων Hadamard για όλα αυτά τα μεγέθη. Οπότε το ερώτημα αυτό αποτελεί το πιο σημαντικό ανοιχτό ερώτημα στην έρευνα των πινάκων Hadamard. Δεν έχει

απαντηθεί ακόμα εάν για όλα αυτά τα μεγέθη πράγματι υπάρχουν πίνακες Hadamard. Ο Hadamard προσπάθησε να δώσει μια εικασία για αυτό το ερώτημα με την ακόλουθη πρόταση:

Εικασία 2.1.21:
(The Hadamard Conjecture): Ένας πίνακας Hadamard τάξης n υπάρχει όταν το n είναι 1, το 2 ή ένα πολλαπλάσιο του 4.

Πέρα από τους κανονικοποιημένους πίνακες Hadamard, υπάρχουν και άλλα είδη πινάκων Hadamard που έχουν επιπλέον ιδιαιτερότητες.

Ορισμός 2.1.22:
Ένας πίνακας Hadamard H ονομάζεται συμμετρικός όταν είναι ένας συμμετρικός πίνακας.

Παράδειγμα 2.1.23: $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$ οι πίνακες A και B είναι πίνακες Hadamard από προηγούμενα παραδείγματα. Υπολογίζουμε τους ανάστροφους:

$$A^T = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad B^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Οπότε έχουμε $A^T = A$ και $B^T = B$ άρα είναι και οι δυο συμμετρικοί πίνακες Hadamard.

Ορισμός 2.1.24:
Ένας πίνακας Hadamard H θεωρείται κανονικός αν το άθροισμα όλων των στοιχείων του σε κάθε γραμμή ή στήλη του είναι ίσο με μια σταθερά k. Συνεπώς, για να ισχύει η κανονικότητα, πρέπει να ισχύει η σχέση *HJ=JH=KJ*, όπου *J* είναι ένας πίνακας με όλα τα στοιχεία του να είναι ίσα με ένα.

Παράδειγμα 2.1.25:
Θέλουμε να δείξουμε ότι ο παρακάτω πίνακας H είναι κανονικός πίνακας Hadamard.

$$H = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \quad \text{και} \quad H^T = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix},$$

$$HH^T = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4I.$$

Επομένως, ο πίνακας Η είναι και κανονικός πίνακας Hadamard, καθώς το άθροισμα κάθε γραμμής και κάθε στήλης του είναι 2. Επιπλέον, παρατηρούμε ότι ο H είναι συμμετρικός.

Ορισμός: 2.1.26:

Ένας πίνακας Hadamard ονομάζεται κυκλικός πίνακας Hadamard όταν είναι ένας κυκλικός πίνακας.

Παράδειγμα: 2.1.27:

$$H=\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

Ο πίνακας H είναι ένας πίνακας Hadamard και κυκλικός πίνακας, δηλαδή είναι ένας κυκλικός πίνακας Hadamard.

Επομένως, ο πίνακας Η από τα προηγούμενα παραδείγματα είναι ένας συμμετρικός πίνακας Hadamard, ένας κανονικός πίνακας Hadamard και επίσης ένας κυκλικός πίνακας Hadamard.

Αξίζει να σημειωθεί ότι οι κυκλικοί πίνακες Hadamard είναι επίσης κανονικοί. Αυτό μας οδηγεί στην εικασία του Ryser, η οποία παραμένει ανοιχτή και δεν έχει απαντηθεί ακόμα.

Εικασία του Ryser's 2.1.28:

Δεν υπάρχει κυκλικός πίνακας Hadamard τάξης μεγαλύτερης του 4.

Η εικασία του Ryser προκαλεί ερωτήματα σχετικά με την έκταση την ισχύος της στην περίπτωση των κανονικών πινάκων Hadamard και εάν υπάρχουν κανονικοί πίνακες Hadamard για κάθε δυνατή τάξη μεγέθους. Το ερώτημα αυτό μπορεί να απαντηθεί με βάση το παρακάτω θεώρημα.

Θεώρημα 2.1.29:

Ένας κανονικός πίνακας Hadamard τάξης μεγαλύτερης του 4 είναι $4m^2$, όπου m είναι ένας θετικός αριθμός.

Απόδειξη 2.1.30:

Έστω H είναι κανονικός πίνακας Hadamard τάξης $4n$ με t το άθροισμα των γραμμών και στηλών. Έστω e είναι $1\ x\ n$ με όλα τα στοιχεία μονάδες. Τότε ισχύει $eH = te$. Χρησιμοποιώντας τη σχέση $HH^T = 4nI_{4n}$, παίρνουμε:

$$eH(eH)^T = t^2ee^T = 4nt^2 \quad \text{και} \quad eHH^Te^T = 4nee^T = 16n^2.$$

Παρατηρούμε ότι $4n = t^2$, και αφού τόσο ο n και ο t είναι ακέραιοι, προκύπτει ότι $n = m^2$, όπου m είναι ένας θετικός αριθμός. Επομένως, η σχέση ισχύει.

Συνεχίζοντας, αξίζει να αναφέρουμε την ύπαρξη των πινάκων skew-Hadamard, οι οποίοι διαδραματίζουν έναν ιδιαίτερο ρόλο στη θεωρία των πινάκων Hadamard.

Ορισμός 2.1.31:

Ένας πίνακας Hadamard $M + I$ ονομάζεται ένας πίνακας skew-Hadamard αν ικανοποιεί τη σχέση $M^T = -M$.

Παράδειγμα 2.1.32:

Ο πίνακας $C=\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ είναι ένας πίνακας Hadamard. Έχουμε ότι

$$M_c = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ -M_c = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ {M_C}^T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

Επομένως, ισχύει ότι ${M_C}^T = -M_C$. Συνεπώς, ο πίνακας C είναι ένας πίνακας skew-Hadamard.

Ο πίνακας $D=\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix}$ είναι ένας πίνακας Hadamard. Έχουμε ότι:

$$\mathrm{M}_D = \begin{bmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & -1 & 1 \\ -1 & 1 & 0 & -1 \\ -1 & -1 & 1 & 0 \end{bmatrix},\ -\mathrm{M}_D = \begin{bmatrix} 0 & -1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{bmatrix},$$

$${M_D}^T = \begin{bmatrix} 0 & -1 & -1 & -1 \\ 1 & 0 & 1 & -1 \\ 1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{bmatrix}.$$

Επομένως, ισχύει ότι ${M_D}^T = -M_D$. Συνεπώς, ο πίνακας D είναι ένας πίνακας skew-Hadamard.

Έχοντας εξετάσει διάφορα είδη πινάκων Hadamard, θα παρουσιάσουμε το γενικευμένο πίνακα Hadamard (complex Hadamard matrix) που διαφέρει σημαντικά από τους γνωστούς πίνακες, καθώς περιλαμβάνει και μιγαδικούς αριθμούς.

Ορισμός 2.1.33:

Έστω X είναι ένας πίνακας τάξης n του οποίου όλα τα στοιχεία του είναι $1, -1, i, -i$ όπου $i = \sqrt{-1}$. Αν όλες οι γραμμές και στήλες είναι ανά δύο ορθογώνιες ο X καλείται ένας γενικευμένος πίνακας Hadamard.

Ορισμός 2.1.34:

Έστω X είναι ένας πίνακας τάξης n του οποίου όλα τα στοιχεία του είναι $1, -1, i, -i$ όπου $i = \sqrt{-1}$. Ο X είναι ένας γενικευμένος πίνακας Hadamard αν και μόνο αν $X\overline{X^T} = nI$ όπου $\bar{X}$ είναι ο συζυγής του X.

Παράδειγμα 2.1.35:

Ο πίνακας $A=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & i & -1 & -i\\ 1 & -1 & 1 & -1\\ 1 & -i & -1 & i\end{bmatrix}$ είναι ένας πίνακας τάξης 4. Θέλουμε να ερευνήσουμε αν ο A είναι ένας γενικευμένος πίνακας Hadamard.

Αρχικά υπολογίζουμε τον πίνακα $\overline{A^T}=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -i & -1 & i\\ 1 & -1 & 1 & -1\\ 1 & i & -1 & -i\end{bmatrix}$, οπότε έχουμε

$$A\overline{A^T}=\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & i & -1 & -i\\ 1 & -1 & 1 & -1\\ 1 & -i & -1 & i\end{bmatrix}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -i & -1 & i\\ 1 & -1 & 1 & -1\\ 1 & i & -1 & -i\end{bmatrix}=\begin{bmatrix}4 & 0 & 0 & 0\\ 0 & 4 & 0 & 0\\ 0 & 0 & 4 & 0\\ 0 & 0 & 0 & 4\end{bmatrix}=4\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}=4I_4.$$

Άρα ο A είναι ένας γενικευμένος πίνακας Hadamard.

2.2 Κατασκευή πινάκων Hadamard με τη μέθοδο του Sylverster

Ο Hadamard δεν ήταν ο πρώτος που ασχολήθηκε με τους πίνακες που ονομάζουμε Hadamard. Ηταν ο J. J. Sylvester το 1857, στην δημοσίευσή του με τίτλο "Thoughts on inverse orthogonal matrices, simultaneous sign-successions and tessellated pavements in two or more colors with application to Newton's rule, ornamental tile work and the theory of numbers", ανακάλυψε τους πίνακες Hadamard για όλες τις δυνάμεις του 2 χρησιμοποιώντας το γινόμενο Kronecker που είδαμε στο προηγούμενο κεφάλαιο.

Θεώρημα 2.2.1:

Αν H_1 και H_2 είναι πίνακες Hadamard της τάξης n_1 και n_2 αντίστοιχα, τότε $H_1 \otimes H_2$ είναι ένας πίνακας Hadamard της τάξης $n_1 n_2$.

Απόδειξη 2.2.2:

Έστω H_1 και H_2 είναι πίνακες Hadamard της τάξης n_1 και n_2 αντίστοιχα. Τότε

$$(H_1 \otimes H_2)(H_1 \otimes H_2)^T = (H_1 \otimes H_2)(H_1^T \otimes H_2^T) = H_1 H_1^T \otimes H_2 H_2^T = n_1 I_{n_1} \otimes n_2 I_{n_2} = n_1 n_2 I_{n_1 n_2}$$

και αποδείχτηκε το ζητούμενο.

Παράδειγμα 2.2.3:

Από το Παράδειγμα 2.1.6 είχαμε ότι ο πίνακας $A=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ και ο πίνακας $P_1AP_2=\begin{bmatrix}1 & 1\\ -1 & 1\end{bmatrix}$ με $P_1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $P_2=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ να είναι πίνακες Hadamard. Θα δείξω ότι ο πίνακας $A \otimes P_1AP_2$ είναι πίνακας Hadamard τάξης 4. Οπότε έχουμε:

$$A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix} \quad \text{και} \quad A_2^T = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$$

κι επομένως,

$$A_2 A_2{}^{\mathrm{T}} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = 4I_4.$$

Άρα ο πίνακας $A \otimes P_1 A P_2$ είναι ένας πίνακας Hadamard τάξης 4.

Θεώρημα 2.2.4:

Αφού υπάρχει πίνακας Hadamard τάξης 2, τότε θα υπάρχει και πίνακας Hadamard τάξεως 2^n για κάθε θετικό ακέραιο n.

Απόδειξη 2.2.5:

Έστω $H_2{}^n = H_2 \otimes H_2 \otimes \ldots \otimes H_2$, τότε το γινόμενο Kronecker H_2 με τον εαυτό του n φορές μας δίνει τον Hadamard πίνακα τάξης 2^n.

Παράδειγμα 2.2.6:

Ο πίνακας $A = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ είναι πίνακας Hadamard. Θα δείξουμε ότι ο πίνακας $B = A \otimes A \otimes A$ είναι επίσης πίνακας Hadamard.

$$B = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix},$$

$$(A^3)^T = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix},$$

$$BB^T=\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{bmatrix}\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{bmatrix}$$

$$=\begin{bmatrix}8&0&0&0&0&0&0&0\\0&8&0&0&0&0&0&0\\0&0&8&0&0&0&0&0\\0&0&0&8&0&0&0&0\\0&0&0&0&8&0&0&0\\0&0&0&0&0&8&0&0\\0&0&0&0&0&0&8&0\\0&0&0&0&0&0&0&8\end{bmatrix}=8\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}=8\,I_8.$$

Άρα Β είναι ένας πίνακας Hadamard τάξης 8.

Θεώρημα 2.2.7:

Αν ο πίνακας Η είναι ένας πίνακας Hadamard τάξης k, για κάποιο θετικό ακέραιο κ, τότε υπάρχει πίνακας Hadamard της τάξεως $2^n k$ για κάθε ακέραιο n.

Απόδειξη 2.2.8

Έστω $H_1=H\otimes H_2^n$, όπου H είναι πίνακας Hadamard τάξης k, και H_2^n είναι πίνακας Hadamard τάξης 2^n, όπως προκύπτει από το Θεώρημα 2.2.4. Τότε, από το Θεώρημα 2.2.1, ο πίνακας H_1 είναι πίνακας Hadamard τάξης $2^n k$.

Παράδειγμα 2.2.9:

Έστω ο πίνακας $A=\begin{bmatrix}1&1&1&1\\-1&1&-1&1\\1&1&-1&-1\\-1&1&1&-1\end{bmatrix}$ μεγέθους 4 και ο πίνακας $B=\begin{bmatrix}1&1\\1&-1\end{bmatrix}$ μεγέθους 2. Και οι δύο είναι πίνακες Hadamard και θέλουμε να κατασκευάσουμε ένα πίνακα Hadamard μεγέθους 16. Από το Θεώρημα 2.2.7 γνωρίζουμε ότι μπορούμε να φτιάξουμε έναν πίνακα μεγέθους $2^n k$. Θέτουμε όπου n=2 και k=4, οπότε κατασκευάζουμε έναν πίνακα μεγέθους 16. Επομένως,

$$A\otimes B\otimes B=\begin{bmatrix}1&1&1&1\\-1&1&-1&1\\1&1&-1&-1\\-1&1&1&-1\end{bmatrix}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}\otimes\begin{bmatrix}1&1\\1&-1\end{bmatrix}$$

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

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Από το Θεώρημα 2.2.1 είναι ένας πίνακας Hadamard τάξης 16.

2.3 Μέθοδος κατασκευής του Paley

Η μέθοδος κατασκευής πινάκων Hadamard του J.J. Sylvester περιορίζεται μόνο στην κατασκευή συγκεκριμένο μεγεθών πινάκων Hadamard. Ωστόσο, από την εικασία του Hadamard έχουμε διαπιστώσει ότι υπάρχουν πίνακες μεγέθους πολλαπλάσιων του 4. Επομένως, αν θελήσουμε να κατασκευάσουμε έναν πίνακα Hadamard μεγέθους 12 ή 20 χρησιμοποιώντας τη μέθοδο του Sylvester δεν είναι δυνατόν. Για να ξεπεράσουμε αυτό το περιορισμό, ο Paley το 1933 εισήγαγε δύο εναλλακτικές μεθόδους για την κατασκευή πινάκων Hadamard.

Πρόταση 2.3.1:
Ένας πίνακας Hadamard τάξης $n=s+1$ μπορεί να κατασκευαστεί, όπου s είναι δύναμη ενός πρώτου ή $s=p^r$, με τον p να είναι πρώτος αριθμός και $s=3(\text{mod}4)$.

Πρόταση 2.3.2:
Ένας πίνακας Hadamard τάξης $n=2(s+1)$ μπορεί να κατασκευαστεί, όπου s είναι δύναμη ενός πρώτου ή $s=p^r$, με τον p να είναι πρώτος αριθμός και $s=1(\text{mod}4)$.

Αυτές οι μέθοδοι κατασκευής προσφέρουν μεγαλύτερη ευελιξία σε σχέση με τη μέθοδο του Sylvester, αφού δεν περιορίζονται σε δυνάμεις του 2. Επιπλέον, δεν απαιτούν την ύπαρξη ενός προϋπάρχοντάς πίνακα.

Σε αυτό το κεφάλαιο, θα αναλύσουμε λεπτομερώς τη μέθοδο κατασκευής του Paley, η οποία χρησιμοποιεί το σώμα Galois που παρουσιάστηκε στο προηγούμενο κεφάλαιο.

Έστω F=GF(s) ένα σώμα Galois τάξης s, οπού $s = p^r$ και p είναι ένας πρώτος αριθμός. Αντιπροσωπεύουμε την πολλαπλασιαστική υποομάδα των μηδενικών πραγματικών αριθμών με H={1,-1}. Παίρνοντας τα μη μηδενικά στοιχεία της F, έχουμε την F*, η οποία αποτελεί μια κυκλική ομάδα υπό τον πολλαπλασιασμό. Θα εξετάσουμε λεπτομερώς τη μέθοδο κατασκευής του Paley μέσω του χαρακτήρα, ο οποίος συμβολίζεται ως c και παρουσιάζεται στον ακόλουθο ορισμό.

Σημείωση: Στην συνέχεια της εργασίας όταν θα λέμε τετραγωνικό θα εννοούμε το τετραγωνικό υπόλοιπο που είδαμε στο προηγούμενο κεφάλαιο.

Ορισμός 2.3.3:

Έστω p είναι ένας πρώτος αριθμός και $q=p^t$. Έχοντας τον τετραγωνικό χαρακτήρα Ψ και F=GF(q) ορίζουμε:

$$\psi(\beta) = \begin{cases} 0 \ \alpha\nu \ \beta = 0. \\ 1 \ \alpha\nu \ \beta \ \epsilon\acute{\iota}\nu\alpha\iota \ \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o}. \\ -1 \ \alpha\nu \ \beta \ \delta\epsilon\nu \ \epsilon\acute{\iota}\nu\alpha\iota \ \tau\epsilon\tau\rho\alpha\gamma\omega\nu\iota\kappa\acute{o} \end{cases} .$$

Λήμμα 2.3.4:

Ο χαρακτήρας $x: F^* \longrightarrow H$ είναι μια ομάδα ομομορφισμού μεταξύ δυο πολλαπλασιαστικών ομάδων.

Απόδειξη 2.3.5:

Το γινόμενο δύο μη τετραγωνικών υπολοίπων ή το γινόμενο δυο τετραγωνικών υπολοίπων είναι τετραγωνικό υπόλοιπο. Επιπλέον, το γινόμενο ενός μη τετραγωνικού υπολοίπου με ένα τετραγωνικό υπόλοιπο είναι τετραγωνικό υπόλοιπο και αντίστροφα, το γινόμενο ενός τετραγωνικού υπολοίπου με ένα μη τετραγωνικό υπόλοιπο είναι τετραγωνικό υπόλοιπο. Συνεπώς, ως αποτέλεσμα έχουμε ότι $x(ab)=x(a)x(b)$ για όλα a,b στο F^*.

Λήμμα 2.3.6:

Στην F υπάρχουν ακριβώς (s+1)/2 τετραγωνικά υπόλοιπα και (s-1)/2 μη τετραγωνικά υπόλοιπα. Επομένως, ισχύει η εξίσωση:

$$\sum_{y \in F} \psi(\alpha) = 0.$$

Απόδειξη 2.3.7:

Από το Λήμμα 2.4.4 γνωρίζουμε ότι ο πυρήνας του ψ αποτελείται από τετραγωνικά υπόλοιπα της F^* και τα υπόλοιπα του ψ αποτελούνται από μη τετραγωνικά υπόλοιπα. Αφού το πλήθος της F^* είναι $|F^*| = s - 1$, γνωρίζοντας ότι η F^* περιέχει (s-1)/2 τετραγωνικά υπόλοιπα και (s-1)/2 μη τετραγωνικά υπόλοιπα. Επιπλέον, το 0 είναι τετραγωνικό υπόλοιπο. Άρα ο συνολικός αριθμός των τετραγωνικών υπολοίπων είναι (s+1)/2. Επόμενος, έχουμε και: $\sum_{y \in F^*} \psi(\alpha) = 0$. Επιπλέον, αφού ψ(0)=0, καταλήγουμε στο συμπέρασμα ότι $\sum_{y \in F} \psi(\alpha) = 0$.

Παράδειγμα 2.3.8:

Έστω q=7 . Παίρνουμε το 3 ως γεννήτρια του GF(7)

F	**0**	**1=3^0**	**2=3^2**	**3=3^1**	**4=3^4**	**5=3^5**	**6=3^3**
Ψ(α)	0	1	1	-1	1	-1	-1

Αν το s είναι το πλήθος του F, τότε s=7. Άρα, ισχύει (s+1)/2=(7+1)/2=8/2=4 τετραγωνικά υπόλοιπα και (s-1)/2=(7-1)/2=6/2=3 μη τετραγωνικά υπόλοιπα. Παρατηρούμε ότι τα τετραγωνικά υπόλοιπα είναι τα {0,1,2,4} και τα μη τετραγωνικά υπόλοιπα είναι τα {3,5,6}.

Υπολογίζουμε το άθροισμα:

$$\sum_{y\in F}\psi(\alpha)=\sum_{y\in F^*}\psi(\alpha)=1+1-1+1-1-1=0.$$

Έτσι, επιβεβαιώνεται το Λήμμα 2.4.6.

Λήμμα 2.3.9:

i) Όταν $s=p^r=1(mod4)$, τότε -1 είναι τετραγωνικό υπόλοιπο στην F.

ii) Όταν $s=p^r=3(mod4)$, τότε -1 είναι μη τετραγωνικό υπόλοιπο στην F.

Απόδειξη 2.3.10:

Έστω ψ, η γεννήτρια της κυκλικής ομάδας F^*. Επειδή το πλήθος της F^* είναι s-1 συμπεραίνουμε ότι $\psi^{s-1}=1$. Έτσι προκύπτει ότι $(\psi^{(s-1)/2}-1)(\psi^{(s-1)/2}+1)=0$. Αφού το F είναι σώμα και η τάξη του ψ είναι s-1, συμπεραίνουμε ότι:

$$\psi^{(s-1)/2}+1=0 \text{ ή } \psi^{(s-1)/2}=-1.$$

Όταν $s=1(mod4)$ άρα $s=4k+1$ για κάποιο ακέραιο k. Τότε:

$$\psi^{(s-1)/2}=\psi^{2k}=(\psi^2)^k=-1,$$

το -1 είναι τετραγωνικό υπόλοιπο. Έτσι αποδείξαμε το (i).

Όταν $s=3(mod4)$, άρα $s=4m+3$ για κάποιο ακέραιο m. Τότε:

$$\psi^{(s-1)/2}=\psi^{2m+1}=-1,$$

οπότε το ψ δεν είναι τετραγωνικό υπόλοιπο. Άρα αποδείξαμε το (ii).

Πρόταση 2.3.11:

i) Όταν $s=p^r=1(mod4)$, τότε $\psi(-\alpha)=\psi(\alpha)$ για όλα τα α στο F^*.

ii) Όταν $s=p^r=3(mod4)$, τότε $\psi(-\alpha)=-\psi(\alpha)$ για όλα τα α στο F^*.

Απόδειξη 2.3.12:

Σύμφωνα με το Λήμμα 2.4.6, για κάθε $\alpha \in F$ ισχύει:

$$\psi(-\alpha) = \psi\big((-1)(\alpha)\big) = \psi(-1)\psi(\alpha).$$

Επομένως, όταν $s = 1(mod4)$, τότε $\psi(-1) = 1$ και όταν $s = 3(mod4)$, τότε $\psi(-1) = -1$, που αποδεικνύεται από το Λήμμα 2.4.9 και τον ορισμού του ψ.

Λήμμα 2.3.13:

Έστω Ψ είναι μη τετριμμένος τετραγωνικός χαρακτήρας του F =GF(q):

$$\sum_{y \in F} \psi(b)\psi(b+c) = -1, \alpha\nu\ c \neq 0.$$

Απόδειξη 2.3.14:

Για $c \neq 0$, θα χρησιμοποιήσουμε την ιδιότητα της αντιστροφής στο F. Για κάθε b στο F, διάφορο από το 0, υπάρχει ένα αντιστρέψιμο στοιχείο b^{-1} τέτοιο ώστε $bb^{-1} = 1$. Ορίζουμε ένα νέο στοιχείο z του F ως εξής: $z = b^{-1}(b + c)$. Αν z είναι διάφορο από το 0, τότε:

$$z = b^{-1}(b + c) = b^{-1}b + b^{-1}c.$$

Παρατηρούμε ότι z είναι ένα μοναδικό στοιχείο του F τέτοιο ώστε $bz = b + c$. Ορίζουμε το σύνολο K ως εξής: $K = \{z = b^{-1}(b + c)\}: b \neq -c\}$. Επειδή το F είναι ένα πεπερασμένο πεδίο, έχουμε ότι κάθε αντιστρέψιμο στοιχείο b είναι διάφορο από το -c. Συνεπώς, το σύνολο K περιέχει στοιχεία που είναι διάφορα από το 1, εφόσον $b^{-1}c$ δεν μπορεί να είναι 1, καθώς κανένα από τα δύο δεν μπορεί να είναι 0. Συνεπώς, έχουμε $K \subseteq F^* - \{1\}$, είναι το σύνολο των αντιστρέψιμων στοιχείων του F. Τώρα, επιλέγοντάς ένα στοιχείο x στο $F^* - \{1\}$ (δηλαδή, ένα στοιχείο διάφορο από το 1). Στη συνέχεια, ορίζουμε b ως εξής: $b = c(x - 1)^{-1}$. Επειδή x≠1, τότε x-1≠0 και αντιστρέψιμο στοιχείο του F.

Τώρα, εξετάζουμε την έκφραση $\psi(bz)$, όπου $z = b^{-1}(b + c)$:

$$\psi(bz) = \psi\big[b\big(b^{-1}(b + c)\big)\big] = \psi[(x - 1)^{-1}c(x - 1)(x - 1 + c)].$$

Χρησιμοποιώντας την αντιστροφή του x-1, έχουμε:

$$\psi[(x - 1)^{-1}] = [\psi(x - 1)]^{-1}.$$

Αφού x είναι διάφορο από το 1, το χαρακτηριστικό της μη τετριμμένης χαρακτήρας ψ είναι διάφορο από το 1. Έτσι, $[\psi(x - 1)]^{-1} \neq 1$.

Συνεπώς, $\psi(bz) \neq 1$, οπότε μπορούμε να συμπεράνουμε ότι η έκφραση,

$$\sum_{y \in F} \psi(b)\psi(b+c) \neq 1, \alpha\nu\ c \neq 0.$$

Άρα ισχύει:

$$\sum_{y \in F} \psi(b)\psi(b+c) = -1, \alpha\nu\ c \neq 0.$$

Παράδειγμα 2.3.15:

Έστω q=5 . Παίρνουμε το 2 ως γεννήτρια του GF(5):

F	**0**	**1=2^0**	**1=2^1**	**3=2^3**	**4=2^2**
Ψ(α)	0	1	-1	-1	1

Θέλουμε να υπολογίσουμε το:

$$\sum_{y\in F} \psi(b)\psi(b+c) \quad \alpha\nu\ c = 1.$$

Οπότε:

$$\begin{aligned}\sum_{y\in F} \psi(b)\psi(b+1) &= \sum_{y\in F^*} \psi(b)\psi(b+1)\\ &= \psi(1)\psi(2) + \psi(2)\psi(3) + \psi(3)*\psi(4) + \psi(4)\psi(5)\\ &= 1(-1) + (-1)(-1) + (-1)1 + 0 = -1.\end{aligned}$$

Το αποτέλεσμα αυτό το περιμέναμε σύμφωνα με το Λήμμα 2.3.13.

Κάποιος θα απορήσει πως τα προηγούμενα αλγεβρικά εργαλεία συνδέονται με τους πίνακες που έχουμε μάθει στην γραμμική άλγεβρα. Θα ορίσουμε έναν πίνακα Q τάξης $s = p^r$ και ένα σώμα Galois ίδιας τάξης F, με p να είναι πρώτος αριθμός και έχοντας τον χαρακτήρα χ στην F. Έστω $F = \{a, a_1, a_2, \dots, a_{s-1}\}$ τα στοιχεία του s στο F με α=0. Ορίζουμε τον πίνακα $Q = (q_{ij})_{sxs}$, όπου $q_{ij} = x(a_j - a_i)$. Ο πίνακας Q έχει βασικό ρόλο και στις δύο κατασκευές του Paley. Το παρακάτω λήμμα δίνει τις ιδιότητες του πίνακα Q.

Λήμμα 2.3.16: Ο πίνακας Q είναι ένας πίνακας με όλα τα στοιχεία του να είναι {-1,0,1}.

i) Όταν $s = p^r = 1(mod4)$, τότε ο πίνακας Q είναι συμμετρικός πίνακας.

ii) Όταν $s = p^r = 3(mod4)$, τότε ο πίνακας Q είναι αντι-συμμετρικός πίνακας.

Απόδειξη 2.3.17:

Το πρώτο μέρος του λήμματος προκύπτει από τον ορισμό του Ψ. Ακολούθως έχουμε:

$$\begin{aligned}q_{ij} = \psi(a_j - a_i) &= \psi\left((-1)(a_i - a_j)\right)\\ &= \begin{cases}-\chi(a_i - a_j), \text{όταν } p^r = 3(mod4)\\ \chi(a_i - a_j), \text{όταν } p^r = 1(mod4)\end{cases}\\ &= \begin{cases}-q_{ji}, \text{όταν } p^r = 3(mod4)\\ q_{ji}, \text{όταν } p^r = 1(mod4)\end{cases}.\end{aligned}$$

Χρησιμοποιώντας την Πρόταση 3.3.11 έχουμε το ζητούμενο.

Ο πίνακας Q από το θεώρημα ονομάζεται πυρήνας του Paley.

Λήμμα 2.3.18: Έστω ο πίνακας Q, ο πυρήνας του Paley, και ο πίνακας J, ένας πίνακας με όλα τα στοιχεί του ίσα με ένα. Ο Q ικανοποιεί τις παρακάτω σχέσεις:

i) $Q\,Q^T = s\,I_s - J.$

ii) $Q\,J = J\,Q = 0.$

Απόδειξη 2.3.19:

i) Ας θεωρήσουμε $Q'Q = B = (b_{ij})$, όπου b_{ij} είναι το εσωτερικό γινόμενο της i-οστης γραμμής του Q με τη j-οστής γραμμή του Q:

$b_{ij} = \sum_k q_{ik}q_{jk} = \sum_k \chi(\alpha_\kappa - \alpha_i)\chi(a_k - a_j) = s - 1$, αν i=j,

$b_{ij} = \sum_k q_{ik}q_{jk} = \sum_k \chi(\alpha_\kappa - \alpha_i)\chi(a_k - a_j) = -1$, αν i≠j.

Αυτό προκύπτει από το Λήμμα 2.3.13 χρησιμοποιώντας $b = a_k - a_i$ και $c = a_i - a_j \neq 0$ και από το γεγονός ότι ο πίνακας Q είναι είτε συμμετρικός η αντισυμμετρικός από το Λήμμα 2.3.16.

$Q\,J = 0$ προκύπτει από την εξίσωση $\sum_j \chi(\alpha_i - a_j) = 0$ χρησιμοποιώντας το Λήμμα 2.3.6. και από το γεγονός ότι ο πίνακας Q είναι είτε συμμετρικός η αντισυμμετρικός από το Λήμμα 2.3.16.

Λήμμα 2.3.20:

Έστω $s = p^r,$ οπού p είναι περιττός πρώτος αριθμός με $p = 3(mod4)$. Τότε ο πίνακας S ορίζεται ως $S=\begin{pmatrix} 0 & -J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)}$ ικανοποιεί τις παρακάτω ιδιότητες:

i) $S^T = -S,$ δηλαδή ο S είναι αντι-συμμετρικός πίνακας.

ii) $S^T S = s\,I_{s+1}.$

Απόδειξη 2.3.21:

i) Ακολουθώντας το Λήμμα 2.3.16, ο Q είναι αντι-συμμετρικός όταν $p = 3(mod4)$, κι έτσι και ο S είναι αντι-συμμετρικός πίνακας.

ii) $SS^T = \begin{pmatrix} 0 & -J_{1xs} \\ J_{sx1} & Q \end{pmatrix}\begin{pmatrix} 0 & J_{1xs} \\ -J_{sx1} & Q' \end{pmatrix} = \begin{pmatrix} s & 0' \\ 0 & QQ' + J_{sxs} \end{pmatrix} = sI_{s+1}.$

Θεώρημα 2.3.22(πρώτη κατασκευή του Paley) :

Έστω $s = p^r$, όπου p είναι περιττός πρώτος αριθμός με $p = 3(mod4)$. Τότε ο πίνακας $H_{s+1} = I_{s+1} + S$, όπου S ορίζεται ως $S=\begin{pmatrix} 0 & -J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)}$, τότε ο H είναι ένας πίνακας skew-Hadamard τάξης s+1.

Απόδειξη 2.3.23:

$$H^T H = (I + S)(I + S^T) = I + S + S^T + SS^T = I + S - S + sI_{s+1} = (s + 1)I_{s+1}.$$

Χρησιμοποιώντας το Λήμμα 3.3.20. Επομένως, ο H είναι ένας πίνακας skew-Hadamard τάξης s+1

Παράδειγμα 2.3.24:

Κατασκευάζουμε πίνακα Hadamard τάξης 4. Παρατηρούμε ότι 4=3+1, οπότε χρησιμοποιούμε το τετραγωνικό υπόλοιπο του GF(3) που είναι ίσα με QR={0,1} και το μη τετραγωνικό υπόλοιπο που είναι {2}. Οπότε χρησιμοποιώντας το προηγούμενο θεώρημα κατασκευάζουμε το πίνακα Q και τον πίνακα S:

$$Q=\begin{bmatrix}0&1&-1\\-1&0&1\\1&-1&0\end{bmatrix},\quad S=\begin{pmatrix}0&-J_{1x3}\\J_{3x1}&Q_{3x3}\end{pmatrix}_{4x4}=\begin{bmatrix}0&-1&-1&-1\\1&0&1&-1\\1&-1&0&1\\1&1&-1&0\end{bmatrix}.$$

Από το θεώρημα έχουμε τον πίνακα Hadamard $H_4 = I_4 + S$:

$$H_4=\begin{bmatrix}1&-1&-1&-1\\1&1&1&-1\\1&-1&1&1\\1&1&-1&1\end{bmatrix}.$$

Ήδη με τη μέθοδο του Sylvester είχαμε κατασκευάσει έναν πίνακα Hadamard τάξης 4. Ωστόσο, τώρα θα αξιοποιήσουμε τη μέθοδο του Paley για να κατασκευάσουμε, για πρώτη φορά, έναν πίνακα Hadamard που δεν είναι δύναμη του δύο.

Παράδειγμα 2.3.25:

Κατασκευάζουμε τον πίνακα Hadamard τάξης 20. Παρατηρούμε ότι 20=19+1. Το τετραγωνικό υπόλοιπο του GF(19)={0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18} είναι ίσα με QR={0,1,4,5,6,7,9,11,16,17} και τα μη τετραγωνικά υπόλοιπά είναι {2,3,8,10,12,13,14,15,18}. Οπότε, χρησιμοποιώντας την πρώτη κατασκευή του Paley, κατασκευάζουμε το πίνακα Q και τον πίνακα S:

Q =

$$\begin{bmatrix}
0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1\\
-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1\\
1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1\\
1&1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1\\
-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1\\
-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1\\
-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1&-1\\
-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1&1\\
1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1&1&-1\\
-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1&1\\
1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1&-1\\
-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1&1\\
1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1&1\\
1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1&1\\
1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1&1\\
1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1&-1\\
-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1&-1\\
-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0&1\\
1&-1&-1&1&1&1&1&-1&1&-1&1&-1&-1&-1&-1&1&1&-1&0
\end{bmatrix},$$

$$S = \begin{pmatrix} 0 & -J_{1x19} \\ J_{19x1} & Q_{19x19} \end{pmatrix}_{20x20}.$$

Από το θεώρημα έχουμε $H_{20} = I_{20} + S$.

$H =$

$$\begin{bmatrix}
1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1
\end{bmatrix},$$

όπου ο Η είναι ένας πίνακας Hadamard τάξης 20.

<u>Δεύτερη κατασκευή του Paley</u>

Η δεύτερή κατασκευή του Paley βασίζεται στους πίνακες συνοδού(conference). Ένας πίνακας συνόδου είναι ένας τετραγωνικός πίνακας που έχει όλα τα στοιχεία του ίσα με 1 ή -1, εκτός από τη διαγώνιο που έχει όλα τα στοιχεία ίσα με 0. Όταν πολλαπλασιάζουμε έναν πίνακα συνόδου τάξης n με τον ανάστροφο του, το αποτέλεσμα είναι $(n-1)I_n$, όπου I_n είναι ο ταυτοτικός πίνακας τάξης n. Από αυτό προκύπτει ότι οι γραμμές και οι στήλες των πινάκων συνόδου είναι ορθογώνιες.

Οι πίνακες συνόδου είχαν αρχικά εφαρμογή στην θεωρητική οπτική των ηλεκτρικών δικτύων και πρωτομελετήθηκαν από τον Belevitch, έναν Βέλγο μαθηματικό το 1950. Αργότερα, η έρευνα σε αυτούς τους πίνακες επεκτάθηκε από τους Goethals και Seidel το 1967. Αυτή η έρευνα ήταν πιο εκτεταμένη και ανέδειξε περαιτέρω ιδιότητες και εφαρμογές των πινάκων συνόδου.

Για την κατανόηση των πινάκων συνόδου, θα παρουσιάσουμε συνοπτικά απαραίτητους ορισμούς και θεωρήματα από τη θεωρία αριθμών.

Ορισμός 2.3.26:

Έστω m ένας θετικός ακέραιος που μπορεί να γραφεί ως $m = n^2(p_1p_2 \dots p_k)$, όπου $p_i(1 \leq i \leq k)$ είναι διαφορετικοί πρώτοι αριθμοί. Τότε ο αριθμός $t = p_1p_2 \dots p_k$ ονομάζεται τετραγωνικό ελεύθερο κομμάτι του m.

Θεώρημα 2.3.27:

Ένας θετικός ακέραιος m μπορεί να γραφεί ως $m = x^2 + y^2$, για κάθε ακέραιο x και y, αν και μόνο αν το τετραγωνικό ελεύθερο κομμάτι του m περιέχει πρώτους αριθμούς που είναι ίσοι με $1(mod4)$.

Θεώρημα 2.3.28:

Για την ύπαρξη τετραγωνικού ρητού πίνακα M τάξης n, όπου $n = 2(mod4)$, απαιτείται η συνθήκη $M^TM = mI_n$ να ικανοποιείται, όπου M^T είναι ανάστροφος πίνακας του M και I_n είναι ο ταυτοτικός πίνακας τάξης n. Ο ακέραιος m πρέπει να είναι θετικός και μπορεί να γραφεί ως $m = a^2 + b^2$, για κάποιους ακεραίους a και b.

Θα συμβολίζουμε τον πίνακα συνόδου ως C-πίνακα.

Ορισμός 2.3.29:

Για να υπάρχει ένας C-πίνακας τάξης $n \equiv 2(mod4)$, υπάρχει μια απαραίτητη προϋπόθεση που αφορά το τετραγωνικό ελεύθερος κομμάτι του $n - 1$. Αυτό το κομμάτι πρέπει να αποτελείται από πρώτος αριθμούς, και κάθε πρώτος αριθμός πρέπει να είναι ίσος με $1(mod4)$.

Λήμμα 2.3.30:

Υποθέτουμε ότι η τάξη $s = p^r$, όπου p είναι περιττός πρώτος αριθμός και ισχύει $s = 1(mod4)$. Έστω T ο πίνακας τάξης s +1 που ορίζεται ως $T = T_{s+1} = \begin{pmatrix} 0 & J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1)}$. Τότε ο T είναι συμμετρικός C-πίνακας.

Απόδειξη 2.3.31:

Βασιζόμενοι στο Λήμμα 2.3.16 και επειδή $s = 1(mod4)$, ο πίνακας Q είναι συμμετρικός. Από την απόδειξη του Λήμματος 2.3.20 είχαμε:

$$TT^T = \begin{pmatrix} 0 & J_{1xs} \\ J_{sx1} & Q \end{pmatrix}\begin{pmatrix} 0 & J_{1xs} \\ J_{sx1} & Q^T \end{pmatrix} = \begin{pmatrix} s & 0^T \\ 0 & QQ^T + J_{sxs} \end{pmatrix} = sI_{s+1} \ .$$

Συνεπώς, ο πίνακας T αποτελείται από στοιχεία που είναι είτε 1 είτε -1, με τα στοιχεία της διαγώνιου να είναι όλα 0. Επιπλέον, ισχύει η σχέση $TT^T = sI_{s+1}$, που σημαίνει ότι ο πίνακας T είναι ένας C-πίνακας. Λόγω της συμμετρίας του, ο πίνακας T είναι επίσης ένας συμμετρικός C-πίνακας.

Παράδειγμα 2.3.32:

Ας κατασκευάσουμε έναν C-πίνακα T_{14}. Αρχικά, ορίζουμε το πεπερασμένο σώμα GF(13) για την πρόσθεση και τον πολλαπλασιασμό modulo13. Τα στοιχεία του GF(13)={0,1,2,3,4,5,6,7,8,9,10,11,12}. Τα τετραγωνικά υπόλοιπα του GF(13) είναι QR = {0,1,3,4,9,10,12}, ενώ τα μη τετραγωνικά υπόλοιπα είναι NQR = {2,5,6,7,8,11}. Συνεπώς έχουμε τον παρακάτω πίνακα Q:

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

Από το Λήμμα 2.3.30, έχουμε τον παρακάτω πίνακα

$$T_{14} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}.$$

Έτσι, ο πίνακας T_{14} είναι ένας C-πίνακας τάξης 14, με όλα τα στοιχεία του να είναι 1 ή -1 και με τα στοιχεία της κύριας διαγώνιου να είναι 0.

Μετά από τον ορισμό του πίνακα συνόδου, μπορούμε να προχωρήσουμε στην κατασκευή ενός πίνακα Hadamard χρησιμοποιώντας μια δεύτερη μέθοδο βασισμένη στην κατασκευής του Paley.

Θεώρημα 2.3.33:

i) Αν υπάρχει ένας συμμετρικός C-πίνακας M τάξης n, τότε μπορούμε να κατασκευάσουμε τον πίνακα H, ως εξής:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes M + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n.$$

Ο πίνακας H είναι ένας συμμετρικός πίνακας Hadamard τάξης $2n$.

ii) Αν T είναι ένας συμμετρικός C-πίνακας τάξης $s+1$, ορίζεται ως:

$$T = T_{s+1} = \begin{pmatrix} 0 & J_{1xs} \\ J_{sx1} & Q \end{pmatrix}_{(s+1)x(s+1).}$$

Όπου $s = p^r = 1(mod4)$ και p είναι περιττός πρώτος αριθμός, τότε μπορούμε να κατασκευάσουμε τον πίνακα H ως εξής:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes T + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n.$$

Ο πίνακας H είναι ένας συμμετρικός πίνακας Hadamard τάξης $2s+2$.

Απόδειξη 2.3.34:

i) Έχουμε ότι

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes M + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n$$
$$= \begin{pmatrix} M & M \\ M & -M \end{pmatrix} + \begin{pmatrix} I_n & -I_n \\ -I_n & -I_n \end{pmatrix} = \begin{pmatrix} M + I_n & M - I_n \\ M - I_n & -M - I_n \end{pmatrix}.$$

Συνεπώς, $H^T = \begin{pmatrix} M^T + I_n & M^T - I_n \\ M^T - I_n & -M^T - I_n \end{pmatrix}$. Άρα, για να είναι ο H πίνακας Hadamard πρέπει $HH^T = 2nI_{2n}$. Πράγματι:

$HH^T =$

$$\begin{pmatrix} (M + I_n)(M^T + I_n) + (M - I_n)(M^T - I_n) & (M - I_n)(M^T + I_n) + (-M - I_n)(M^T - I_n) \\ (M - I_n)(M^T + I_n) + (-M - I_n)(M^T - I_n) & (M - I_n)(M^T - I_n) + (-M - I_n)(-M^T - I_n) \end{pmatrix} =$$

$$\begin{pmatrix} MM^T + M + M^T + I_n^2 + MM^T + M - M^T + I_n^2 & MM^T + M - M^T - I_n^2 - MM^T + M - M^T + I_n^2 \\ MM^T + M - M^T - I_n^2 - MM^T + M - M^T + I_n^2 & MM^T - M - M^T + I_n^2 + MM^T + M - M^T + I_n^2 \end{pmatrix} =$$

$$\begin{pmatrix} 2(MM^T + I_n) & 0 \\ 0 & 2(MM^T + I_n) \end{pmatrix} = \begin{pmatrix} 2((n-1)I_n + I_n) & 0 \\ 0 & 2((n-1)I_n + I_n) \end{pmatrix} =$$

$$\begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} = 2n \begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix} = 2nI_{2n}.$$

Άρα, βρήκαμε το ζητούμενο, ο Η είναι πίνακας Hadamard.

ii) Έχουμε ότι:

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes T + \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \otimes I_n$$
$$= \begin{pmatrix} T & T \\ T & -T \end{pmatrix} + \begin{pmatrix} I_n & -I_n \\ -I_n & -I_n \end{pmatrix} = \begin{pmatrix} T + I_n & T - I_n \\ T - I_n & -T - I_n \end{pmatrix}.$$

Συνεπώς, $H^T = \begin{pmatrix} T^T + I_n & T^T - I_n \\ T^T - I_n & -T^T - I_n \end{pmatrix}$. Άρα, για να είναι ο H πίνακας Hadamard πρέπει να ισχύει $HH^T = (2n+2)I_{2n+2}$. Πράγματι,

$$HH^T =$$
$$\begin{pmatrix} (T+I_n)(T^T+I_n)+(T-I_n)(T^T-I_n) & (T-I_n)(T^T+I_n)+(-T-I_n)(T^T-I_n) \\ (T-I_n)(T^T+I_n)+(-T-I_n)(T^T-I_n) & (T-I_n)(T^T-I_n)+(-T-I_n)(-T^T-I_n) \end{pmatrix} =$$
$$\begin{pmatrix} TT^T+T+T^T+I_n^2+TT^T+T-T^T+I_n^2 & TT^T+T-T^T-I_n^2-TT^T+T-T^T+I_n^2 \\ TT^T+T-T^T-I_n^2-TT^T+T-T^T+I_n^2 & TT^T-T-T^T+I_n^2+TT^T+T-T^T+I_n^2 \end{pmatrix} =$$
$$\begin{pmatrix} 2(TT^T+I_n) & 0 \\ 0 & 2(TT^T+I_n) \end{pmatrix} = \begin{pmatrix} 2((n-1)I_n+I_n) & 0 \\ 0 & 2((n-1)I_n+I_n) \end{pmatrix} \begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} =$$
$$2n\begin{pmatrix} I_n & 0 \\ 0 & I_n \end{pmatrix} = 2nI_{2n} = 2(s+1)I_{2(s+1)} = (2s+2)I_{2s+2}.$$

Παράδειγμα 2.3.35:

Για την κατασκευή ενός πίνακα Hadamard τάξης 28 με τη δεύτερη κατασκευή Paley, παρατηρούμε ότι 28=2(13+1), οπού 13 είναι πρώτος αριθμός και $13 + 1 \equiv 2(mod4)$. Αυτό σημαίνει ότι μπορούμε να χρησιμοποιήσουμε το πεπερασμένο σώμα GF(13) με πράξεις πρόσθεσης και πολλαπλασιασμού modulo 13 για την κατασκευή του. Τα στοιχεία του GF(13) είναι: {0,1,2,3,4,5,6,7,8,9,10,11,12}. Τα τετραγωνικά υπόλοιπα του GF(13) είναι QR={0,1,3,4,9,10,12}, ενώ τα μη τετραγωνικά υπόλοιπα είναι NQR={2,5,6,7,8,11}. Επομένως, χρησιμοποιώντας το παράδειγμα, κατασκευάζουμε τον

$$T_{14}=\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}.$$

Από το Θεώρημα 2.3.33 κατασκευάζουμε τον H_{28} που είναι πίνακας Hadamard

$$H_{28} = \begin{pmatrix} T_{14}+I_{14} & T_{14}-I_{14} \\ T_{14}-I_{14} & -(T_{14}+I_{14}) \end{pmatrix} =$$

1	1	1	1	1	1	1	1	1	1	1	1	1	1	-1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1
1	1	1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	1	-1
1	-1	1	1	1	-1	1	1	-1	-1	-1	-1	1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	1
1	1	-1	1	1	1	-1	1	1	-1	-1	-1	-1	1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	1
1	1	1	-1	1	1	1	-1	1	1	-1	-1	-1	-1	1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1
1	-1	1	1	-1	1	1	1	-1	1	1	-1	-1	-1	1	-1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1
1	-1	-1	1	1	-1	1	1	1	-1	1	1	-1	-1	1	-1	-1	1	1	-1	1	-1	1	-1	1	1	-1	-1
1	-1	-1	-1	1	1	-1	1	1	1	-1	1	1	-1	1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	1	-1
1	-1	-1	-1	-1	1	1	-1	1	1	1	-1	1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	1
1	1	-1	-1	-1	-1	1	1	-1	1	1	1	-1	1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	1
1	1	1	-1	-1	-1	-1	1	1	-1	1	1	1	-1	1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1
1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	1	1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	1
1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	1	1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	-1
-1	1	1	1	1	1	1	1	1	1	1	1	1	1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
1	-1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	-1	-1	1	-1	-1	1	1	1	1	-1	-1	1	-1
1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	-1	-1	-1	-1	1	-1	-1	1	1	1	1	-1	-1	1
1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	-1	-1	1	-1	-1	1	1	1	1	-1	-1
1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	-1	-1	1	-1	-1	-1	1	-1	-1	1	1	1	1	-1
1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	-1	-1	-1	1	-1	-1	-1	1	-1	-1	1	1	1	1
1	-1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	-1	1	-1	-1	1	-1	-1	-1	1	-1	-1	1	1	1
1	-1	-1	1	1	-1	1	-1	1	-1	1	1	-1	-1	-1	1	1	-1	-1	1	-1	-1	-1	1	-1	-1	1	1
1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	1	-1	-1	1	1	1	-1	-1	1	-1	-1	-1	1	-1	-1	1
1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	1	-1	1	1	1	1	-1	-1	1	-1	-1	-1	1	-1	-1
1	1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	-1	-1	1	1	1	1	-1	-1	1	-1	-1	-1	1	-1
1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	-1	-1	-1	1	1	1	1	-1	-1	1	-1	-1	-1	1
1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	1	-1	1	-1	-1	1	1	1	1	-1	-1	1	-1	-1	-1
1	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1	-1	-1	-1	1	-1	-1	1	1	1	1	-1	-1	1	-1	-1

Κεφάλαιο 3. ΠΙΝΑΚΕΣ SKEW-HADAMARD

Μερικές από τις πιο ισχυρές μεθόδους κατασκευής πινάκων Hadamard βασίζονται στην ύπαρξη του πίνακα skew-Hadamard. Οι ιδιότητες αυτών των πινάκων παρατηρήθηκαν αρχικά από τον Paley και τον Williamson. Για την κατασκευή ενός πίνακα skew-Hadamard, είναι πολύ χρήσιμοι οι πίνακες Hadamard που θα ορίσουμε παρακάτω. Αυτοί οι πίνακες Hadamard έχουν συγκεκριμένες ιδιότητες που μας επιτρέπουν να κατασκευάσουμε τον πίνακα skew-Hadamard.

Με τη χρήση των οικείων(amicable) πινάκων Hadamard, μπορούμε να κατασκευάσουμε πίνακες skew-Hadamard μεγαλύτερης τάξης. Οι πίνακες Hadamard αυτοί έχουν σημαντική συνεισφορά στη θεωρία των πινάκων και βρίσκουν εφαρμογές σε πολλούς τομείς, όπως η κωδικοποίηση.

3.1 Οικείοι Πίνακες Hadamard

Ορισμός: 3.1.1:
Οι πίνακες X και Y ονομάζονται οικείοι όταν ικανοποιούν τη σχέση $XY^T = YX^T$.

Ορισμός: 3.1.2:
Δύο πίνακες $M = I + U$ και N ονομάζονται οικείοι πίνακες Hadamard όταν ο πίνακας M είναι ένας πίνακας skew-Hadamard, δηλαδή $M^T = -M$, και ο πίνακας N είναι ένας συμμετρικός πίνακας Hadamard, δηλαδή $N^T = N$, που ικανοποιεί τη σχέση:

$$MN^T = NM^T.$$

Λήμμα 3.1.3:
Έστω ότι $M = W + I$ και N είναι οικείοι πίνακες Hadamard, τότε ισχύει ότι:

$$WN^T = NW^T.$$

Απόδειξη 3.1.4:
Από τη σχέση $MN^T = NM^T$ έχουμε:

$MN^T = (W + I)N^T = WN^T + N^T = WN^T + N$ και $NM^T = N(W^T + I) = NW^T + N$.

Άρα $WN^T + N = NW^T + N$ οπότε $WN^T = NW^T$.

Θεώρημα (Wallis) 3.1.5:
Έστω ότι υπάρχουν οικείοι πίνακες Hadamard τάξης n και m. Τότε υπάρχει ένας οικείος πίνακας τάξης mn.

Απόδειξη 3.1.6:

Έστω $I + M_1$ και N_1 είναι οικείοι πίνακες Hadamard τάξης m, και $I + M_2$ και N_2 είναι οικείοι πίνακες Hadamard τάξης n. Θέλουμε να αποδείξουμε τα παρακάτω:

- Ο πίνακας $M_{12} = I \otimes (I + M_2) + M_1 \otimes N_2$ είναι ένας πίνακας skew-Hadamard.
- Ο πίνακας $N_{12} = N_1 \otimes N_2$ είναι ένας συμμετρικός πίνακας Hadamard.
- Οι πίνακες M_{12} και N_{12} οικείοι πίνακες Hadamard τάξης nm.

Αρχικά θα αποδείξουμε ότι ο πίνακας M_{12} και ο πίνακας N_{12} είναι πίνακες Hadamard μεγέθους nmI. Για τον πίνακα N_{12} από το Θεώρημα 2.2.1 ξέρουμε ότι όταν έχουμε δύο πίνακες Hadamard N_1 μεγέθους n και N_2 μεγέθους m τότε υπάρχει πίνακας $N_{12} = N_1 \otimes N_2 = nmI$.

Για τον πίνακα M_{12} για να είναι πίνακας Hadamard μεγέθους nm πρέπει να ισχύει ότι $M_{12}M_{12}^T = nmI$, οπότε θα έχουμε:

$M_{12}M_{12}^T = (I \otimes (I + M_2) + M_1 \otimes N_2)(I \otimes (I + M_2^T) + M_1^T \otimes N_2^T).$

$= I \otimes (I + M_2)(I + M_2^T) + (-M_1) \otimes (I + M_2)N_2^T + M_1 \otimes N_2(I + M_2^T) +$
$M_1M_1^T \otimes M_2M_2^T.$

Από τη στιγμή που $I + M_1$, N_1 και $I + M_2$, N_2 είναι οικείοι πίνακες, έχουμε:

$$= I \otimes mI + (n-1)I \otimes mI = nI \otimes mI = nmI.$$

Συνεχίζοντας αποδεικνύομε ότι ο πίνακας M_{12} είναι skew-Hadamard:

$$\begin{aligned}(I \otimes (I + M_2) + M_1 \otimes N_2 - I \otimes I)^T &= (I \otimes (I + M_2))^T + (M_1 \otimes N_2)^T - I \otimes I \\ &= I \otimes (I + M_2^T) + (M_1^T \otimes N_2^T) - I \otimes I \\ &= I \otimes (I - M_2) - M_1 \otimes N_2 - I \otimes I \\ &= I \otimes I - I \otimes M_2 - M_1 \otimes N_2 - I \otimes I \\ &= -I \otimes (I + M_2) - M_1 \otimes N_2 + I \otimes I \\ &= -(I \otimes (I + M_2) + M_1 \otimes N_2 - I \otimes I)\end{aligned}$$

Επομένως, ο πίνακας M_{12} είναι skew-Hadamard.

Έπειτα, θα αποδείξουμε ότι ο πίνακας N_{12} είναι συμμετρικός πίνακας Hadamard:

$$N_{12}^T = (N_1 \otimes N_2)^T = N_1^T \otimes N_2^T = N_1 \otimes N_2 = N_{12}\ .$$

Επομένως, ο πίνακας N_{12} είναι συμμετρικός πίνακας Hadamard.

Τέλος, θα δείξουμε ότι είναι οικείοι πίνακες Hadamard:

$$\begin{aligned}(I \otimes (I + M_2) + M_1 \otimes N_2)(N_1^T \otimes N_2^T) &= N_1^T \otimes (I + M_2)N_2^T + M_1N_1^T \otimes N_2N_2^T \\ &= N_1 \otimes N_2(I + M_2^T) + N_1M_1^T \otimes N_2N_2^T \\ &= (N_1 \otimes N_2)(I \otimes (I + M_2^T) + M_1^T \otimes N_2^T).\end{aligned}$$

Οπότε, οι πίνακες N_{12} και M_{12} είναι οικείοι πίνακες Hadamard τάξης nm.

Συνέπεια 3.1.7:

Υπάρχουν οικείοι πίνακες Hadamard της τάξης 2^t, όπου t είναι θετικός ακέραιος.

Οι οικείοι πίνακες μεγέθους τάξης 2^t, όπου t είναι θετικός ακέραιος, κατασκευάζονται αναδρομικά χρησιμοποιώντας τους παρακάτω πίνακες και την μέθοδό κατασκευής της παραπάνω απόδειξης.

$I + M_1 = I + M_2$ και $N_1 = N_2$ είναι δοσμένοι οικείοι πίνακες Hadamard.

$I + M_1 = I + M_2 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ και $N_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Η κατασκευή οικείου πίνακα Hadamard τάξης 2^t θα γίνει ποιο κατανοητή στο παρακάτω παράδειγμα.

Παράδειγμα 3.1.8:

Θέλουμε να κατασκευάσουμε έναν οικείο πίνακα Hadamard τάξης 16

$$I + M_4 = I \otimes (I + M_2) + M_1 \otimes N_2 = \begin{bmatrix} I + M_2 & 0 \\ 0 & I + M_2 \end{bmatrix} + \begin{bmatrix} 0 & N_2 \\ -N_2 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{bmatrix},$$

$$N_4 = N_1 \otimes N_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix},$$

$$M_4 = I \otimes (I + M_4) + M_4 \otimes N_4$$

$$= \begin{bmatrix} I + M_4 & 0 & 0 & 0 \\ 0 & I + M_4 & 0 & 0 \\ 0 & 0 & I + M_4 & 0 \\ 0 & 0 & 0 & I + M_4 \end{bmatrix} + \begin{bmatrix} 0 & N_4 & N_4 & N_4 \\ -N_4 & 0 & N_4 & -N_4 \\ -N_4 & -N_4 & 0 & N_4 \\ -N_4 & N_4 & -N_4 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} I + M_4 & N_4 & N_4 & N_4 \\ -N_4 & I + M_4 & N_4 & -N_4 \\ -N_4 & -N_4 & I + M_4 & N_4 \\ -N_4 & N_4 & -N_4 & I + M_4 \end{bmatrix}$$

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

και

$$N_{16} = N_4 \otimes N_4 = \begin{bmatrix} N_4 & N_4 & N_4 & N_4 \\ N_4 & -N_4 & N_4 & -N_4 \\ N_4 & N_4 & -N_4 & -N_4 \\ N_4 & N_4 & -N_4 & N_4 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \end{bmatrix}.$$

Συνεπώς, ο N_{16} και ο $I + M_{16}$ είναι οικείοι πίνακες Hadamard τάξης 16.

<u>Λήμμα 3.1.9:</u>

Υπάρχουν οικείοι πίνακες Hadamard τάξης $s + 1$, όπου $s \equiv 3(mod4)$ και q είναι ένας πρώτος αριθμός.

Απόδειξη 3.1.10:

Έστω *J* είναι ένα διάνυσμα-γραμμή μεγέθους s με όλα τα στοιχεία του να είναι 1 και *Q* να είναι ένας skew-συμμετρικός πίνακας για $s \equiv 3(mod4)$.

Ορίζουμε τον πίνακας $S = \begin{pmatrix} 0 & -J \\ J & Q \end{pmatrix}$ μεγέθους s και έχει τις παρακάτω ιδιότητες:

$$S^T = -S, \quad S\,S^T = s\,I_{s+1}$$

Θέτοντας h=s+1 και $M = I_h + S$. Ο πίνακας *M* είναι ένας skew-Hadamard πίνακας τάξης s+1.

Έστω $U = (u_{i,j})_{0 \le i,j \le q-1}$ ως ένας πίνακας τάξης s ορισμένος ως εξής:

$$u_{i,j} = \begin{cases} 1 & \alpha\nu\ i + j = q\ \eta\ i = j = 0 \\ 0 & \alpha\lambda\lambda\iota\acute{\omega}\varsigma. \end{cases}.$$

Παρατηρούμε ότι ο πίνακας *U* έχει τη μορφή $\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. Επομένως:

$$U^T = U \quad \kappa\alpha\iota \quad U^2 = I.$$

Έχουμε τον πίνακα *N*:

$$N = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix}\begin{bmatrix} 0 & -J \\ J & Q \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} + \begin{bmatrix} 0 & -J \\ J & -UQ \end{bmatrix} = \begin{bmatrix} 1 & J \\ J & -U - UQ \end{bmatrix}.$$

Ορίζουμε τον πίνακα $U\,Q = (c_{i,j})$. Τότε:

$$c_{0,j} = \sum_{k=0}^{q-1} u_{0k}\psi(\alpha_k - \alpha_j) = u_{00}\psi(\alpha_0 - \alpha_j) = \psi(-\alpha_j),$$

$$c_{j,0} = \sum_{k=0}^{q-1} u_{jk}\psi(a_k - a_0) = u_{0,q-j}\psi(\alpha_{q-j}) = -\psi(a_j).$$

Για $i \neq 0$, έχουμε:

$$c_{i,j} = \psi(\alpha_{q-i} - a_j) = \psi(-\alpha_j - a_j) = \psi(-1)\psi(\alpha_i + a_j) = -\psi(\alpha_i + a_j).$$

Επομένως, ο πίνακας $U\,Q$ είναι συμμετρικός, οπότε και ο πίνακας *N* είναι συμμετρικός. Έτσι, έχουμε ότι $NN^T = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} MM^T \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = nI_n$.

Οπότε αφού ο *N* είναι συμμετρικός πίνακας και πίνακας Hadamard έχουμε:

$$MN^T = MM^T \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = nI_n \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -U \end{bmatrix} MM^T = NM^T.$$

Άρα, οι πίνακες *M* και *N* είναι οικείοι πίνακες Hadamard.

3.2 Μέθοδος κατασκευής Williamson

Ορισμός 3.2.1:

Αν υπάρχουν οι τετραγωνικοί πίνακες *A, B, C, D* τάξης *n* που ικανοποιούν τη σχέση:

$$AA^T + BB^T + CC^T + DD^T = 4nI \tag{3.1}$$

και για κάθε *X, Y* πίνακες διαφορετικούς από *A, B, C* και *D* ισχύει η σχέση $X\,Y^T = Y\,X^T$, τότε υπάρχει πίνακας:

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}.$$

Ο πίνακας *H* είναι ένας πίνακας Hadamard τάξης 4 *n*.

Απόδειξη 3.2.2:

Για να αποδείξουμε ότι ο πίνακας *H* είναι πίνακας Hadamard τάξης 4n, θα πρέπει να ισχύει ότι $HH^T = 4nI$, όπου I είναι μοναδιαίος πίνακας τάξης 4*n*. Οι τετραγωνικοί πίνακες *A, B, C, D* είναι οικείοι πίνακες μεταξύ τους, αφού ισχύει η σχέση $XY^T = YX^T$ για οποιοδήποτε πίνακα *X, Y,* και ισχύει η σχέση $AA^T + BB^T + CC^T + DD^T = 4nI$. Χρησιμοποιώντας αυτές τις ιδιότητες, θα υπολογίσουμε τον πίνακα HH^T. Ο πίνακας *H* είναι:

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}.$$

Και ο H^T είναι:

$$H^T = \begin{bmatrix} A^T & -B^T & -C^T & -D^T \\ B^T & A^T & D^T & -C^T \\ C^T & -D^T & A^T & B^T \\ D^T & C^T & -B^T & A^T \end{bmatrix}.$$

Έτσι έχουμε:

$$HH^T = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \begin{bmatrix} A^T & -B^T & -C^T & -D^T \\ B^T & A^T & D^T & -C^T \\ C^T & -D^T & A^T & B^T \\ D^T & C^T & -B^T & A^T \end{bmatrix} =$$

$$\begin{vmatrix} \mathrm{A}A^T + BB^T + CC^T + DD^T & \mathrm{BA}^{\mathrm{T}} - A\mathrm{B}^{\mathrm{T}} - D\mathrm{C}^{\mathrm{T}} + \mathrm{CD}^{\mathrm{T}} & CA^T + DB^T - AC^T - BD^T & DA^T - CB^T + BC^T - AD^T \\ AB^T - BA^T - CD^T + DC^T & \mathrm{A}A^T + BB^T + CC^T + DD^T & CB^T - DA^T + AD^T - BC^T & DB^T + CA^T - BD^T - AC^T \\ AC^T + BD^T - CA^T - DB^T & BC^T - AD^T + DA^T - CB^T & \mathrm{A}A^T + BB^T + CC^T + DD^T & DC^T - CD^T - BA^T + AB^T \\ AD^T - BC^T + CB^T - DA^T & BD^T + AC^T - DB^T - CA^T & CD^T - DC^T - AB^T + BA^T & \mathrm{A}A^T + BB^T + CC^T + DD^T \end{vmatrix}$$

Οπότε από την σχέση $XY^T = YX^T$ συμπεραίνουμε ότι:

$$\mathrm{BA^T} - A\mathrm{B^T} - D\mathrm{C^T} + \mathrm{CD^T} = A\mathrm{B^T} - A\mathrm{B^T} + \mathrm{CD^T} - \mathrm{CD^T} = 0.$$

Άρα κάνοντας το ίδιο και για τα υπόλοιπα στοιχεία έχουμε τον παρακάτω πίνακα

$$=\begin{bmatrix} 4I_n & 0 & 0 & 0 \\ 0 & 4I_n & 0 & 0 \\ 0 & 0 & 4I_n & 0 \\ 0 & 0 & 0 & 4I_n \end{bmatrix} = 4\begin{bmatrix} I_n & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 \\ 0 & 0 & I_n & 0 \\ 0 & 0 & 0 & I_n \end{bmatrix} = 4I_{4n}.$$

Άρα ο H είναι πίνακας Hadamard.

Συμπέρασμα 3.2.3:

Αν υπάρχουν τετραγωνικοί πίνακες A, B, C, D τάξης n, με στοιχεία {1,-1}, που είναι κυκλικοί, συμμετρικοί και ικανοποιούν την εξίσωση $AA^T + BB^T + CC^T + DD^T = 4nI$, τότε υπάρχει πίνακας

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix},$$

ο οποίος είναι ένας πίνακας Hadamard.

Παράδειγμα 3.2.4:

Κατασκευάζουμε έναν πίνακα Hadamard πίνακα τάξης 12 με τη μέθοδο Williamson. Δίνονται οι πίνακες $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ και $B = C = D = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}$,

$$A\,B^T = B\,A^T = \begin{bmatrix} -1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & -1 \end{bmatrix}.$$

Αφού $B = C = D$ ισχύει ότι $A\,C^T = C\,A^T$ και $A\,D^T = D\,A^T$

Συνεχίζοντας έχουμε $AA^T = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}$ και $BB^T = CC^T = DD^T = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$.

Επομένως, πρέπει να δείξουμε ότι ισχύει $AA^T + BB^T + CC^T + DD^T = 4nI = 12I$, δηλαδή,

$$\begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix} + \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} + \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} + \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} = \begin{bmatrix} 12 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 12 \end{bmatrix}.$$

Αφού ικανοποιούνται όλες οι προϋποθέσεις του Ορισμού 3.3.1, κατασκευάζουμε τον παρακάτω πίνακα Hadamard.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Η μέθοδος του Williamson μας επιτρέπει να κατασκευάσουμε πίνακες Hadamard τάξης $4t$ χρησιμοποιώντας 4 κυκλικούς πίνακες τάξης *t*, οι οποίοι ικανοποιούν τη σχέση (3.1). Έστω *R* ένας ανάποδος μοναδιαίος πίνακας τάξης *t* και δύο κυκλικοί πίνακες *A* και *B* τάξης *t*. Αν θέσουμε $X = A$ ως κυκλικό πίνακα και $Y = BR$ ως ανάποδο κυκλικό πίνακα τάξης 4t, τότε ισχύει η σχέση $XY^T = YX^T$. Συνεπώς οι πίνακες *X, Y* είναι οικείοι.

Οι Goethals και Seidel τροποποίησαν τον πίνακα του Williamson έτσι ώστε οι πίνακες εισόδου να μην χρειάζεται να είναι κυκλικοί και συμμετρικοί. Ο δικός τους πίνακας ήταν χρήσιμος στην κατασκευή πολλών νέων Hadamard πινάκων, αλλά ο κύριος στόχος τους ήταν η κατασκευή ενός skew-Hadamard πίνακα τάξης 36.

Ορισμός: 3.2.5:

Το διάνυσμα Goethals-Seidel χρησιμοποιεί κυκλικούς πίνακες *A, B, C, D* τάξης *m* που ικανοποιούν $AA^T + BB^T + CC^T + DD^T = 4mI_m$ και τον *R* ανάποδο μοναδιαίο πίνακα τάξης *m*.

$$W = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & RD & -RC \\ -CR & -RD & A & RD \\ -DR & RC & -RB & A \end{bmatrix}.$$

Θεώρημα: 3.2.6:

Αν *A, B, C, D* είναι τετραγωνικοί κυκλικοί πίνακες τάξης *m*, και *R* ανάποδος μοναδιαίος πίνακας τάξης *m*, τότε αν ο (*A-I)* είναι Skew πίνακας(δηλαδή ο *A* ικανοποιεί τη σχέση $(A - I)(A - I)^T = -I$) και ισχύει:

$$AA^T + BB^T + CC^T + DD^T = 4mI_m.$$

Τότε από το διάνυσμα Goethals-Seidel ο πίνακας που προκύπτει είναι ένας πίνακας skew-Hadamard.

Με αυτήν την κατασκευή βρέθηκε ο πρώτος πίνακας skew-Hadamard τάξης 36 και 56. Δεν θα δείξουμε την κατασκευή αυτόν τον πινάκων γιατί δεν είναι ο στόχος της παρούσας εργασίας.

ΚΕΦΑΛΑΙΟ 4. ΚΩΔΙΚΕΣ ΔΙΟΡΘΩΣΗΣ ΣΦΑΛΜΑΤΩΝ ΚΑΙ ΠΙΝΑΚΕΣ HADAMARD

Σε πολλούς τομείς της επιστήμης και της τεχνολογίας, η μεταφορά πληροφοριών από τη μια πηγή στην άλλη είναι απαραίτητη. Για παράδειγμα, όταν μεταφέρονται δεδομένα από έναν υπολογιστή σε έναν άλλο, απαιτείται η μετατροπή των πληροφορίων σε έναν κώδικα που μπορεί εύκολα να αποκωδικοποιηθεί από τον αποδέκτη. Κατά τη μετάδοση, ωστόσο, ο κώδικας μπορεί να υποστεί τροποποιήσεις λόγω ανθρώπινων ή τυχαίων σφαλμάτων.

Συνήθως, όταν παρουσιαστεί κάποιο σφάλμα, ο κώδικας μπορεί να αναμεταδοθεί ξανά και το σφάλμα να διορθωθεί. Ωστόσο, σε πολλές περιπτώσεις δεν είναι εφικτή η επαναμετάδοση του μηνύματος. Επομένως, είναι απαραίτητο να καθοριστεί μια διαδικασία για τον εντοπισμό και τη διόρθωση σφαλμάτων στον κώδικα, χωρίς να χρειάζεται να γίνεται επανάληψη της αποστολής του μηνύματος.

Ένα παράδειγμα είναι η μετάδοση τεράστιων αρχείων που στους ηλεκτρονικούς υπολογιστές και στα κινητά μας, όπου η επαναμετάδοση του αρχείου από την αρχή σε κάθε σφάλμα δεν είναι εφικτή. Συνεπώς, οι κωδικοί διόρθωσης σφαλμάτων είναι σημαντικοί για την ορθή λειτουργία των δικτιών τηλεπικοινωνιών.

Θα ξεκινήσουμε το κεφάλαιο με κάποιες βασικές εννοείς και ύστερά θα δούμε πως ο πίνακας Hadamard συσχετίζετε με τους κωδικούς διόρθωσης σφαλμάτων.

4.1 Εισαγωγή στην θεωρία διόρθωσης σφαλμάτων

Ιδιότητες των κωδικών

Αρχικά θα ορίσουμε τις ιδιότητες των κωδικών και διόρθωσης σφαλμάτων.

Ορισμός 4.1.1:
Μια λέξη αποτελείται από n στοιχεία, τα οποία μπορούν να είναι δυαδικά ψηφία, δηλαδή μπορούν να πάρουν τις τιμές 0 ή 1. Ένας δυαδικός κώδικας μήκους n αναπαρίσταται από ένα υποσύνολο C του καρτεσιανού γινομένου $V(n,2)$, όπου $V(n,2)$ αναφέρεται στο σύνολο των δυαδικών αριθμών με n ψηφία, δηλαδή $\{0,1\}x\{0,1\}x\ldots x\{0,1\}$.

Τα στοιχεία του C λέγονται κωδικές λέξεις και προφανώς κάθε κωδική λέξη έχει μήκος n.

Ορισμός 4.1.2:
Ένας $[n,k]$ γραμμικός, δυαδικός κώδικας είναι ένα σετ από γραμμικούς συνδυασμούς των k ανεξάρτητων διανυσμάτων στο V.

Ένας δυαδικός κώδικας ορίζεται κάτω από το modulo 2.

Ο Robert W. Hamming ήταν ένας Αμερικάνος μαθηματικός που στα τέλη τις δεκαετίας του 1940 δούλευε για την τηλεφωνική εταιρία Bell Telephone. Ο Hamming ασχολούταν με υπολογιστές που έκαναν μακρούς και πολύπλοκούς υπολογισμούς από την εποχή που ήταν στο Manhattan project. Μια παρασκευή ρυθμίζει τα μηχανήματα να πραγματοποιήσουν μια πολύπλοκή διαδικασία που θα χρειαζόταν όλο το σαββατοκύριακο. Τη Δευτέρα που επέστρεψε, προς έκπληξή του και απογοήτευσή του, παρατήρησε ότι η διαδικασία είχε σταματήσει λόγω ενός σφάλματός σε ένα bit. Λόγω αυτού του συμβάντος, ο Hamming αφιέρωσε τον χρόνο του στην λύση αυτού του προβλήματος. Το 1950, ο Hamming δημοσίευσε μια εργασία για τον εντοπισμό και τη διόρθωση σφαλμάτων για γραμμικούς κώδικες, η οποία πρωτοστάτησε σε περαιτέρω έρευνα στη θεωρία κωδικοποίησης.

Ορισμός 4.1.3:

Η απόσταση Hamming(προς τιμή του Richard Wesley Hamming) δύο κωδικών λέξεων a, b συμβολίζεται με $d(a,b)$ και ορίζεται ως το πλήθος των ψηφίων στα οποία οι δύο κωδικές λέξεις διαφέρουν.

Σημείωση 4.1.4:

Μπορεί να γραφεί ως $d(a,b) = \sum_{i=1}^{n} |a_i - b_i|$ για όλες τις κωδικές λέξεις a και b μήκους n.

Παράδειγμα 4.1.5:

d(1010,1011)=1, αφού $d(a,b) = \sum_{i=1}^{n} |a_i - b_i| = |1-1| + |0-0| + |1-1| + |0-1| = 1$.

Θεώρημα 4.1.6:

Η απόσταση Hamming ικανοποιεί τις τέσσερις παρακάτω ιδιότητες:

(i) $d(a,b) \geq 0$ για κάθε a,b.

(ii) $d(a,b) = 0$ αν και μόνο αν $a=b$.

(iii) $d(a,b) = d(b,a)$ για όλα a,b.

(iv) $d(a,c) \leq d(a,b) + d(a,c)$ για όλα τα a,b,c.

Απόδειξη 4.1.7:

(i) Από τη στιγμή που $d(a,b)$ είναι απόλυτη ποσότητα τότε δεν μπορεί να είναι μικρότερη του μηδενός.

(ii) Αν $d(a,b) = 0$, τότε $a_i = b_i$. Συνεπώς, ο a πρέπει να είναι ισοδύναμος του b.

(iii) Ξέρουμε $(a,b) = \sum_{i=1}^{n} |a_i - b_i|$. Από τις ιδιότητες του απολύτου $\sum_{i=1}^{n} |a_i - b_i| = \sum_{i=1}^{n} |b_i - a_i| = d(b,a)$. Συνεπώς, $d(a,b) = d(b,a)$.

(iv) $(a,c) = \sum_{i=1}^{n} |a_i - c_i| = \sum_{i=1}^{n} |a_i - b_i + b_i - c_i| \leq \sum_{i=1}^{n} (|a_i + b_i|) - (|b_i - c_i|)$
$= \sum_{i=1}^{n} (a_i - b_i) + \sum_{i=1}^{n} (b_i - c_i) = d(a,b) + d(b,c)$.
Άρα, $d(a,c) \leq d(a,b) + d(a,c)$.

Ορισμός 4.1.8:

Το βάρος Hamming wt(x) του διανύσματος x είναι η απόσταση Hamming μεταξύ του x και του 0, όπου 0 το διάνυσμα που έχει όλα τα στοιχεία ίσα με το μηδέν.

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

Παράδειγμα 4.1.9:

Έστω ότι έχουμε ένα διάνυσμα x=(10101) και θέλουμε να υπολογίσουμε το βάρος Hamming. Τότε

$$\text{wt}(x) = d(x,0) = d(10101,00000) = 3.$$

Εντοπισμός σφαλμάτων

Για να εντοπίσουμε ένα σφάλμα, το σφάλμα πρέπει να μετατρέπει μια κωδική λέξη σε μία μη κωδική λέξη. Έτσι, πρέπει να υπάρχει ο ελάχιστος αριθμός ψηφίων μεταξύ των κωδικών λέξεων. Αυτή η ελάχιστη απόσταση Hamming (συμβολίζεται ως d) που αναφέρθηκε στον Ορισμό 4.1.4 αποτελεί τη βάση για τη θεωρία ανίχνευσης και διόρθωσης σφαλμάτων.

Αν d=1, τότε οι κωδικές λέξεις μπορούν να διαφέρουν μόνο κατά ένα ψηφίο, οπότε είναι αδύνατον να εντοπιστούν σφάλματα κατά ένα ψηφίο. Για παραδείγματος, αν στέλνουμε την κωδική λέξη 10101 και ο παραλήπτης λάβει την κωδική λέξη 10111, τότε δεν μπορούμε να εντοπίσουμε το σφάλμα, αφού και οι δύο λέξεις είναι κωδικές λέξεις. Ο μέγιστος αριθμός σφαλμάτων που μπορούμε να εντοπίσουμε σε έναν κώδικα είναι (d-1).

Ωστόσο, ο εντοπισμός σφαλμάτων διαφέρει από τη διόρθωση σφαλμάτων. Ενώ μπορούμε να εντοπίσουμε (d-1) σφάλματα, μπορούμε να διορθώσουμε ακόμα λιγότερα. Για παράδειγμα, αν χρησιμοποιήσουμε έναν κώδικα με δύο λέξεις, 0000 και 1111, άρα το d=4 (ελάχιστη απόσταση Hamming), τότε μπορούμε να εντοπίσουμε μέχρι 3 σφάλματα. Για παράδειγμα, αν στείλουμε τη συμβολοσειρά 0100, μπορούμε να εντοπίσουμε το σφάλμα αφού δεν είναι καμία από τις δύο λέξεις, αλλά δεν μπορούμε να το διορθώσουμε, καθώς δεν μπορούμε να αποφασίσουμε ποια κωδική λέξη θα έπρεπε να στείλουμε.

Χρησιμοποιώντας έναν κώδικά διόρθωσης e-σφαλμάτων, στέλνουμε τον κωδικό 0000 αφού d(0000,0100)=1 και d(1111,0100)=3. Αυτή η μέθοδος διόρθωσης σφαλμάτων ονομάζεται κανόνας του κοντινότερου γείτονα. Αυτός ο κανόνας μπορεί να διορθώσει d/2 ψηφία από όλα τα σφάλματα που μπορούν να συμβούν. Αν τα σφάλματα είναι λιγότερα από d/2, τότε υπάρχει ακριβώς μια κωδική λέξη πιο κοντά στη λάθος συμβολοσειρά και μπορεί να διορθωθεί. Αν τα σφάλματα είναι περισσότερα από d/2, τότε υπάρχουν περισσότερες κωδικές λέξεις που έχουν ίση απόσταση και η συμβολοσειρά δεν μπορεί να διορθωθεί.

Χρησιμοποιώντας το παραπάνω παράδειγμα, έχουμε τη λέξη 0101, η οποία έχει 2 σφάλματα που εντοπίζουμε, άρα d/2 σφάλματα. Δεν είναι δυνατή η διόρθωση αυτού του σφάλματος, καθώς η απόσταση από τις κωδικές λέξεις 0000 και 1111 είναι ίση.

Παράδειγμα 4.1.10:

Για n=4 υπάρχουν συνολικά 2^4=16 δυνατές λέξεις που μπορούν να δημιουργηθούν. Ας εξετάσουμε κάθε βάρος ξεχωριστά.

Για λέξεις βάρους 0, υπάρχει μόνο μία λέξη: 0000. Έτσι, έχουμε $\binom{4}{0} = 1$ λέξης με βάρος 0.

Για λέξεις βάρους 1, χρησιμοποιώντας την προηγούμενη σχέση, έχουμε $\binom{4}{1}$=4 λέξεις: 1000, 0100, 0010, 0001.

Συνεχίζουμε με τον ίδιο τρόπο για βάρος 2 έχουμε $\binom{4}{2}$=6 λέξεις: 1100, 1010, 1001, 0110, 0101, 0011.

Με το βάρος 3, έχουμε $\binom{4}{3} = 4$ λέξεις: 1110, 1101, 1011, 0111.

Τέλος, για βάρος 4, υπάρχει μόνο μία λέξη 1111. Επομένως, έχουμε $\binom{4}{4}$=1, με βάρος 4.

Συνολικά, οι λέξεις για κάθε βάρος είναι οι εξής:

Βάρος 0: 0000.
Βάρος 1: 1000, 0100, 0010, 0001.
Βάρος 2: 1100, 1010, 1001, 0110, 0101, 0011.
Βάρος 3: 1110, 1101, 1011, 0111.
Βάρος 4: 1111.

Θεώρημα (Hamming) 4.1.11 :

Έστω C ένας δυαδικός κώδικας μήκους n που μπορεί να διορθώσει μέχρι και r σφάλματα. Τότε για το πλήθος των κωδικών λέξεων M=$M(n,r)$ ισχύει:

$$M \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}}.$$

Απόδειξη 4.1.12:

Το σύνολο των δυνατών λέξεων μήκους n με ψηφία 0 και 1 είναι προφανώς 2^n. Αφού ο κώδικας μας μπορεί να διορθώνει μέχρι και r λάθη, για κάθε μία από τις M κωδικές λέξεις θα υπάρχουν λέξεις που δεν θα είναι κωδικές λέξεις. Αυτές οι λέξεις θα είναι όλες οι λέξεις σε απόσταση 1 από την κωδική λέξη, όλες οι λέξεις σε απόσταση 2, κ.ο.κ. μέχρι και όλες οι λέξεις σε απόσταση r από την κωδική λέξη (καθώς και η κωδική λέξη σε απόσταση 0 από τον εαυτό της).

Άρα κάθε μία από τις M κωδικές λέξεις αποκλείει ακριβώς $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}$ από τις συνολικές 2^n λέξεις. Οι M κωδικές λέξεις θα αποκλείουν $M\left[\binom{n}{0} + \binom{n}{1} + \binom{n}{r}\right]$ λέξεις. Επομένως, $M \leq \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}}$.

Παράδειγμα: 4.1.13:

Θέλουμε να κατασκευάσουμε έναν κώδικα μήκους 5 που να διορθώνει μέχρι 2 λάθη. Έστω ότι έχουμε την κωδική λέξη 10100. Τότε υπάρχουν 5 λέξεις που διαφέρουν κατά ένα ψηφίο και 10 λέξεις που διαφέρουν κατά δύο ψηφία. Οι λέξεις αυτές είναι: 00100, 11100, 10000, 10110, 10101 για ένα ψηφίο και 01100, 00000, 00110, 00101, 11000, 11110, 11101, 10010, 10001, 10111, για δύο ψηφία. Άρα κάθε κωδική λέξη "διώχνει" 5+10+1=16 λέξεις. Συνολικά, για μήκος 5, υπάρχουν 2^5=32 δυνατές λέξεις. Οπότε έχουμε $M \leq \frac{32}{16}$, δηλαδή $M \leq 2$. Άρα ο κωδικός θα είναι 10100 και η λέξει που διαφέρει κατά 5 ψηφία είναι 01011.

Ορισμός 4.1.14:

Για έναν κώδικα C, η ελάχιστη απόσταση ορίζεται ως η μικρότερη απόσταση μεταξύ των διακεκριμένων κωδικών λέξεων. Δηλαδή:

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

Θεώρημα 4.1.15:

(i) Ένας κώδικας C μπορεί να ανιχνεύσει μέχρι και s σφάλματα σε μία κωδική λέξη αν $d(\mathrm{C}) \geq s + 1$.

(ii) Ένας κώδικας C μπορεί να διορθώσει μέχρι και t σφάλματα σε μία κωδική λέξη αν $d(\mathrm{C}) \geq 2t + 1$.

Απόδειξη 4.1.16:

Για το πρώτο σκέλος του θεωρήματος υποθέτουμε ότι $d(\mathrm{C}) \geq s + 1$. Υποθέτουμε επίσης ότι μεταδίδεται μία κωδική λέξη x και ότι γίνονται s ή λιγότερα σφάλματα. Τότε το λαμβανόμενο διάνυσμα δεν μπορεί να είναι μία διαφορετική κωδική λέξη, και έτσι τα σφάλματα μπορούν να ανιχνευθούν.

Για το δεύτερο σκέλος του θεωρήματος, υποθέτουμε ότι $d(C) \geq 2t + 1$. Έστω ότι μεταδίδεται μία κωδική λέξη x και έστω ότι y είναι το λαμβανόμενο διάνυσμα στο οποίο εμφανίζονται t ή λιγότερα σφάλματα, έτσι ώστε $d(x,y) \leq t$. Αν x' είναι μία οποιαδήποτε κωδική λέξη διαφορετική από τη x, τότε $d(x',y) \geq t + 1$. Διότι αν ήταν $d(x',y) \leq t$, αυτό συνεπάγεται από την τριγωνική ανισότητα, ότι $d(x,x') \leq d(x,y) + d(x',y) \leq 2t$, που έρχεται σε αντίφαση με το γεγονός ότι $d(\mathrm{C}) \geq 2t + 1$. Έτσι η x είναι η πιο κοντινή κωδική λέξη στην y και η πιο κοντινή γειτονική αποκωδικοποίηση διορθώνει τα σφάλματα.

Πόρισμα 4.1.17:

Αν ένας κώδικας C έχει ελάχιστη απόσταση d, τότε ο C μπορεί να χρησιμοποιηθεί είτε (i) να ανιχνεύσει μέχρι και d-1 σφάλματα, ή (ii) να διορθώσει μέχρι και (d-1)/2 σφάλματα σε κάθε κωδική λέξη.

Παράδειγμα 4.1.18:

Έστω ότι έχουμε δύο κωδικούς C_1={000000,111111} με ελάχιστη απόσταση $d(C_1)$=6 και C_2={11010000, 01101000, 00110100, 00011010, 00001101, 10000110, 01000011, 10100001} με ελάχιστη απόσταση $d(C_2)$=4. Από αυτό ακολουθεί ότι ο κώδικας C_1 μπορεί να διορθώσει μέχρι 2 σφάλματα, ενώ ο C_2 διορθώνει μέχρι 1 σφάλμα.

Για παράδειγμα, αν λάβουμε στον κώδικα C_1 την κωδική λέξη 01001, τότε μπορεί να διορθωθεί σε 00000. Ωστόσο, αν η πραγματική κωδική λέξη ήταν 11111, τότε θα είχαμε τρία σφάλματα και δεν θα μπορούσαμε να τη διορθώσουμε. Επίσης, αν στον κώδικα C_2 αλλάξουμε ένα στοιχείο, ο C_2 θα μπορούσε να διορθώσει το σφάλμα. Αυτό συμβαίνει επειδή η απόσταση της λαμβανόμενης κωδικής λέξης από τη σωστή κωδική λέξη θα ήταν 1, ενώ από όλες τις άλλες κωδικές λέξεις θα ήταν κατά 3. Έστω έχουμε την κωδική λέξη 11010000 και λαμβάνουμε την κωδική λέξη 01010000, τότε έχει μόνο ένα σφάλμα και μπορεί διορθωθεί. Ωστόσο, αν λάβουμε τη λέξη 00000000 και ανιχνεύσουμε ότι έχουν γίνει 3 σφάλματα, δεν μπορούμε να τη διορθώσουμε, αφού απέχει από όλες τις κωδικές λέξεις απόσταση 3. Έτσι, η αρχική κωδική λέξη έχει χαθεί .

Λήμμα 4.1.19:

Αν x και y είναι δύο κωδικές λέξεις ενός κώδικα C, τότε $d(x,y) = w(x-y) = w(x+y) = w(x) + w(y) - 2w(x \cap y)$, όπου $w(x \cap y)$ συμβολίζει τον αριθμό των συντεταγμένων που τα x και y έχουν και τα δύο 1.

Απόδειξη 4.1.20:

Έστω $d(x,y) = w(x-y) = w(x+y)$ = (αριθμός των 1 στο x) + (αριθμός των 1 στο y)-2(αριθμός των συντεταγμένων που τα x και y έχουν και τα δύο 1) = $w(x) + w(y) - 2w(x \cap y)$.

Παράδειγμα 4.1.21:

Έστω ότι έχω τις κωδικές λέξεις x=10100 και y=10000. Αρχικά υπολογίζουμε το βάρος σε κάθε λέξη: $w(x)$=w(10100)=2 και $w(y)$=w(10000)=1.

Στην συνέχεια υπολογίζουμε το $w(x \cap y)$= w(10100∩10000)=1. Τώρα, μπορούμε να υπολογίσουμε την απόσταση Hamming $d(x,y)$ χρησιμοποιώντας την ισότητα από το Λήμμα 4.1.14: $d(x,y) = w(x-y) = w(x+y) = w(x) + w(y) - 2w(x \cap y)$.

Αντικαθιστούμε τις τιμές: $d(x,y)$ = 2 + 1 – 2 (1) = 1, όποτε $w(x-y)$=(10100-10000)=1, $w(x+y)$=(10100+10000)=1.

Επιβεβαιώνεται ότι η απόσταση Hamming $d(x,y)$ είναι ίση με 1, ανεξάρτητα από τη μέθοδο υπολογισμού $(x-y)$ ή $(x+y)$.

Θεώρημα 4.1.22:

Υποθέτουμε ότι d είναι περιττός. Τότε ένας (n,M,d) κώδικας υπάρχει αν και μόνο αν ένας $(n+1,M,d+1)$ κώδικας υπάρχει.

Απόδειξη 4.1.23:

Υποθέτουμε ότι C είναι ένας (*n*,*M*,*d*) κώδικας, όπου το *d* είναι περιττός. Έστω $\hat{C}$ είναι ο κώδικας μήκους *n*+1 που προκύπτει από τον C επεκτείνοντας κάθε λέξη *x* του C σύμφωνα με τον κανόνα:

$$x = x_1x_2 \dots x_n \to \hat{x} = \begin{cases} x_1x_2 \dots x_n 0 \ \alpha\nu \ w(x) \quad \epsilon\acute{\iota}\nu\alpha\iota \ \acute{\alpha}\rho\tau\iota o\varsigma \\ x_1x_2 \dots x_n 1 \ \alpha\nu \ w(x) \ \epsilon\acute{\iota}\nu\alpha\iota \ \pi\epsilon\rho\iota\tau\tau\acute{o}\varsigma \end{cases}.$$

Ισοδύναμα ορίζουμε $\hat{x} = x_1x_2 \dots x_nx_{n+1}$ όπου $x_{n+1} = \sum_{i=1}^{n} x_i$, πάντα κάτω από την πράξη mod 2. Αυτή η κατασκευή του $\hat{\mathrm{C}}$ από τον C ονομάζεται προσθέτοντας έναν συνολικό έλεγχο ισοτιμίας στον κώδικα C.

Αφού $w(\hat{x})$ είναι άρτιος για κάθε κωδική λέξη $\hat{x}$ και $\hat{y}$, από το Λήμμα 4.1.17, προκύπτει ότι $d(\hat{x}, \hat{y})$ είναι άρτιος για όλα τα $\hat{x}$ και $\hat{y}$ του $\hat{\mathrm{C}}$. Επομένως $d(\hat{\mathrm{C}})$ είναι άρτιος. Προφανώς d≤ $d(\hat{C}) \leq d + 1$, και έτσι αφού ο *d* είναι περιττός, έχουμε $d(\hat{\mathrm{C}})$=*d*+1. Συνεπώς ο $\hat{\mathrm{C}}$ είναι ένας (*n*+1,*M*,*d*+1) κώδικας.

Αντίστροφα, υποθέτουμε ότι D είναι ένας (*n*+1,*M*,*d*+1) κώδικας, όπου ο *d* είναι περιττός. Επιλέγουμε δύο κωδικές λέξεις *x* και *y* του D έτσι ώστε *d*(*x*,*y*)=*d*+1. Επιλέγουμε μια συντεταγμένη στην οποία οι λέξεις *x* και *y* διαφέρουν και τη διαγράφουμε απ' όλες τις κωδικές λέξεις. Το αποτέλεσμα είναι ένας (*n*, *M*, *d*) κώδικας.

Παράδειγμα 4.1.24:

Έστω ότι είχαμε τον κώδικα C_1={00000,11111} με περιττό αριθμό αποστάσεων *d*=5, *n*=5 και *M*=2. Θέλουμε να κατασκευάσουμε έναν κώδικα (6,2,6).

Σύμφωνα με την απόδειξη που παρουσιάστηκε, υπολογίζουμε το w(00000)=0 (άρτιος) και w(11111)=5 (περιττός). Άρα, ο νέος κωδικός θα είναι {000000,111111}. Έχουμε *n*=6, *M*=2 και *d*=6.

Παρακάτω θα παρουσιάσουμε ένα πολύ σημαντικό θεώρημα που θα το χρειαστούμε και στο επόμενο κεφάλαιο.

Θεώρημα 4.1.25:

Για κάθε (*n*,*M*,*d*) κώδικα C για τον οποίο *n*<2*d*, ισχύει:

$$M \leq 2\left[\frac{d}{2d - n}\right]. \qquad (1).$$

Απόδειξη 4.1.26:

Θα υπολογίσουμε το άθροισμα $\sum_{u\in C}\sum_{v\in C} d(u, v)$ με δύο τρόπους. Πρώτα, παρατηρούμε ότι αφού *d*(*u*,*v*)≥ d αν *u*≠*v*, το άθροισμα είναι ≥ $M(M - 1)d$. Από την άλλη μεριά, έστω *A* είναι ο *M* x *n* πίνακας, όπου οι γραμμές είναι οι κωδικές λέξεις. Υποθέτουμε ότι η *i*-στήλη του *A* περιέχει x_i

μηδενικά και M-x_i άσσους. Τότε αυτή η στήλη συνεισφέρει $2x_i$(M-x_i) στο άθροισμα, άρα το άθροισμα είναι ίσο με $\sum_{i=1}^{n} 2x_i(M - x_i)$. Αν ο M είναι άρτιος, αυτή η παράσταση μεγιστοποιείται αν όλα τα $x_\iota = M/2$, και το άθροισμα είναι $\leq nM^2/2$. Έτσι, έχουμε

$$M\,(M\text{-}1)\,d \leq n\,M^2/n \rightarrow M \leq \frac{2d}{2d-n}\,. \qquad (2).$$

Αντίστροφα, αν ο M είναι περιττός, τότε το άθροισμα είναι $\leq n\frac{(M^2-1)}{2}$, και αντί για την (1) παίρνουμε $M \leq \frac{n}{2d-n} = \frac{2d}{2d-n} - 1$.

Αυτό συνεπάγεται $M \leq \left[\frac{2d}{2d-1}\right] - 1 \leq 2\left[\frac{d}{2d-n}\right]$ χρησιμοποιώντας την ιδιότητα $[2x] \leq [2x]+1$.

Παράδειγμα 4.1.27:

Θα εξετάσουμε τους παρακάτω δυαδικούς κωδικούς για να δούμε αν μπορούν να υπάρχουν: (12,7,7), (12,6,7).

Πρώτα, θα εφαρμόσουμε το φράγμα του Plotkin για τον κωδικό (12,7,7)

$$M \leq 2\left[\frac{d}{2d-n}\right].$$

Εφαρμόζουμε την ανισότητα:

$$7 \leq 2\left[\frac{7}{2*7-12}\right] = 2[3{,}5] = 2*3 = 6\,.$$

Αυτό οδηγεί σε άτοπο, και δεν υπάρχει κώδικας με αυτά τα χαρακτηριστικά.

Στη συνέχεια, θα εξετάσουμε τον κωδικό (12,6,7) με το φράγμα του Plotkin:

$$M \leq 2\left[\frac{d}{2d-n}\right].$$

Εφαρμόζουμε την ανισότητα, έχουμε:

$$6 \leq 2\left[\frac{7}{2*7-12}\right] = 2[3] = 6.$$

Σε αυτή την περίπτωση, η ανισότητα ισχύει, και μπορεί να υπάρχει κωδικός με αυτά τα χαρακτηριστικά.

Ένας κωδικός καλείται $[n,k]$ δυαδικός κώδικας αν είναι ένα υποσύνολο του διανυσματικού χώρου V_n μεγέθους k πάνω στο πεδίο F_2. Αυτό σημαίνει ότι ο κωδικός θα έχει λέξεις μεγέθους n με k ψηφία μηνύματος.

Ορισμός 4.1.28:

Η σφαίρα του Hamming $B_e(c)$ γύρω από την κωδική λέξη c του C ορίζεται ως εξής:

$$B_e(c) = \{x \in S(n): d(x,c) \leq e\},$$

όπου $S(n)$ συμβολίζει το σύνολο όλων των δυαδικών ακολουθιών μήκους n. Έτσι η $B_e(c)$ αποτελείται από όλες τις δυαδικές ακολουθίες μήκους n που έχουν απόσταση από το c μικρότερη η ίση από το e.

Λήμμα: 4.1.29:

Ένας κώδικας C είναι κώδικας διόρθωσης e-σφαλμάτων αν και μόνον αν οι σφαίρες του Hamming $B_e(c)$, $c \in C$ είναι ξένες μεταξύ τους.

Απόδειξη 4.1.30:

Ας υποθέσουμε ότι C είναι κώδικας διόρθωσης e-σφαλμάτων, αλλά $B_e(c) \cap B_e(c') \neq \emptyset$. Τότε υπάρχει $x \in S(n)$ έτσι ώστε $x \in B_e(c)$ και $x \in B_e(c')$. Τότε, από τον ορισμό της σφαίρας του Hamming, έχουμε ότι η απόσταση Hamming μεταξύ των *c* και *x* είναι επίσης μικρότερη ή ίση από το *e*. Αυτό σημαίνει ότι $d(x, c) \leq e$. Σύμφωνα με την τριγωνική ανισότητα, έχουμε:

$$d(c, c') \leq d(c, x) + d(x, c') \leq 2e < 2e + 1.$$

Αυτό είναι σε αντίφαση με το γεγονός ότι ο C είναι κώδικας διόρθωσης *e*-σφαλμάτων.

Αντίστροφα, ας υποθέσουμε ότι $B_e(c) \cap B_e(c') = \emptyset$ για όλα τα $c,\ c' \in C\ c \neq c'$. Αν ο C δεν είναι κώδικας διόρθωσης e-σφαλμάτων, τότε υπάρχουν $c,\ c' \in C$ έτσι ώστε $d(c, c') = f \leq 2e$.

Ας υποθέσουμε ότι τα *c, c'* διαφέρουν στις θέσεις $i_1, \ldots, i_f$. Τότε αλλάζουμε τα ψηφία του *c* στις θέσεις $i_1, \ldots, i_{[f/2]}$ για να συμφωνούν με το *c'* αυτές τις θέσεις, και ονομάζουμε την ακολουθία που προκύπτει *b*. Τότε:

$$d(c, b) = [f/2] \leq e$$

και

$$d(b, c') = f - \left[\frac{f}{2}\right] \leq e.$$

Έτσι, τότε $b \in B_e(c) \cap B_e(c)$, που έρχεται σε αντίφαση με την υπόθεση.

Ορισμός 4.1.31:

Ένας κώδικας C είναι ένας τέλειος κώδικας διόρθωσης *e*-σφαλμάτων αν κάθε $x \in S(n)$ μπορεί να διορθωθεί σε μία κωδική λέξη δεδομένου ότι δεν έχουν γίνει περισσότερα από e-σφάλματα.

Παράδειγμα: 4.1.32:

Δίνονται οι δύο ακόλουθοι κωδικές C_1={0000,11111} και C_2={000000,111111}. Ο κωδικός C_1 θεωρείται τέλειος, καθώς μπορεί να διορθώσει μέχρι 2 σφάλματα. Δηλαδή, μπορεί να διορθώσει οποιοδήποτε μήνυμα που λάβει, υπό την προϋπόθεση ότι το μήνυμα έχει το πολύ 2 σφάλματα. Για παράδειγμα, αν λάβει το μήνυμα 01010, μπορεί να το διορθώσει σε 00000.

Αντίθετα, ο κωδικός C_2 δεν θεωρείται τέλειος κωδικός, καθώς υπάρχουν λέξεις που δεν μπορεί να διορθώσει. Για παράδειγμα, το μήνυμα 000111 απέχει από το 000000 απόσταση 3 και από το 111111 απόσταση 3. Επομένως, αν ο κώδικας C_2 λάβει αυτό το μήνυμα, δεν μπορεί να το διορθώσει, καθώς υπάρχουν δύο κωδικές λέξεις στον C_2 που απέχουν το πολύ 2 σφάλματα από το μήνυμα.

Συνεπώς, με βάση αυτά τα παραδείγματα, μπορούμε να συμπεράνουμε ότι ο τέλειος κώδικας διόρθωσης *e*-σφαλμάτων είναι ένας κώδικας που μπορεί να διορθώσει μηνύματα με το πολύ e σφάλματα και να τα επαναφέρει στη σωστή μορφή.

Λήμμα 4.1.33:

Ένας κώδικας διόρθωσης *e*-σφαλμάτων C μήκους *n* με *M* κωδικές λέξεις είναι τέλειος αν και μόνο αν $\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)M=2^n$.

Απόδειξη 4.1.34:

Υπάρχουν 2^n δυαδικές ακολουθίες στο $S(n)$. Κάθε $B_e(c)$ περιέχει $\binom{n}{i}$ ακολουθίες σε απόσταση *i* από το *c*, και έτσι περιέχει $\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}$ μέλη του $S(n)$. Αφού ο C είναι κώδικας διόρθωσης *e*-σφαλμάτων, αυτές οι σφαίρες είναι όλες ξένες μεταξύ τους και έτσι περιέχουν στην ένωσή τους $M\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)$ μέλη του $S(n)$. Έτσι, ο C είναι τέλειος κώδικας αν και μόνο αν αυτός ο αριθμός είναι 2^n.

Παράδειγμα: 4.1.35:

Έχουμε τούς παρακάτω κωδικούς: C_1={0000,11111} και C_2={000000,111111}. Και οι δύο κώδικες αποτελούνται από 2 κωδικές λέξεις, με μήκη κωδικής λέξης 5 για τον κώδικα C_1 και 6 για τον κώδικα C_2. Παρατηρούμε ότι και οι δύο κωδικοί μπορούν να διορθώσουν μέχρι 2 σφάλματα. Για τον κώδικα C_1, από το λήμμα, έχουμε:

$$M\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)=2\left(\binom{5}{0}+\binom{5}{1}+\binom{5}{2}\right)=2(1+5+10)=32.$$

Παρατηρούμε ότι ο αριθμός *M* είναι ίσος με 2^n, δηλαδή 2^5=32. Άρα ο κώδικας C_1 είναι τέλειος κώδικας. Για τον κώδικα C_2 από το προηγούμενο λήμμα, έχουμε:

$$M\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}\right)=2\left(\binom{6}{0}+\binom{6}{1}+\binom{6}{2}\right)=2(1+6+18)=50$$

Παρατηρούμε ότι ο αριθμός *M* δεν είναι ίσος με 2^n, δηλαδή $2^6=64$. Άρα ο κώδικας C_2 δεν είναι τέλειος κώδικας, όπως αναμέναμε.

4.2 Κωδικός Hadamard

Οι κωδικοί διόρθωσης σφαλμάτων Hadamard έχουν πολλές εφαρμογές στις τηλεπικοινωνίες. Ο Plotkin ήταν ο πρώτος που ανακάλυψε τη δύναμη της διόρθωσης σφαλμάτων που προσφέρουν οι πίνακες Hadamard, το 1960. Ο Levenshtein, από την άλλη πλευρά, εισήγαγε έναν αλγόριθμο για την κατασκευή κωδικών διόρθωσης σφαλμάτων με πίνακες Hadamard.

Μία από τις πιο διάσημες εφαρμογές αυτών των κωδικών διόρθωσης σφαλμάτων ήταν η διαστημική αποστολή των διαστημικών σκαφών Sailor και Voyager της Nasa το 1969. Χάρης στις ισχυρές δυνατότητες διόρθωσης σφαλμάτων αυτού του κώδικα, ήταν δυνατή η σωστή αποκωδικοποίηση των υψηλής ποιότητας εικόνων του Άρη, του Δία, του Κρόνου και του Ουρανού.

Έτσι, οι κωδικοί διόρθωσης σφαλμάτων Hadamard προσφέρουν αξιόπιστη δυνατότητα ανίχνευσης και διόρθωσης σφαλμάτων, επιτρέποντας τη μετάδοση και λήψη δεδομένων με υψηλή ακρίβεια και αξιοπιστία.

Θεώρημα: 4.2.1:

Έστω H_n είναι ένας πίνακας Hadamard τάξης $n=4m$. Για οποιοδήποτε k=1,2,…,n, ορίζουμε ένα διάνυσμα u_k με 1 και -1 ώστε το πολύ m-1 στοιχεία του διανύσματος $v_k = h_k + u_k$ να είναι διαφορετικά από τη συνιστώσα h_k του H_n. Έστω $s_k = u_k H_n^t$, τότε το k -οστού στοιχείο είναι το πολύ 2(m-1).

Απόδειξη 4.2.2:

Αφού ισχύει $H_n H_n^T = nI_n$, έχουμε $r_k = h_k H_n^T = 4ne_k = 4me_{4m}$. Παρατηρούμε ότι εάν το διάνυσμα w είναι ένα διάνυσμα n τάξης με στοιχεία (-1,1), τότε το k-οστό στοιχείο του wH_n δεν μπορεί να υπερβαίνει το n. Παρατηρούμε επίσης ότι αν το h_k και το v_k διαφέρουν μόνο σε ένα στοιχείο, τότε το k-οστό στοιχείο του διανύσματος $r_k - s_k$ είναι δυο και η απόλυτη τιμή των υπόλοιπων στοιχείων του $r_k - s_k$ δεν μπορεί να υπερβαίνει το 2. Ακόμη, κάθε φορά που η συνιστώσα του μη μηδενικού αριθμού u_k αυξάνεται σε j, το κ-οστό στοιχείο του s_k μειώνεται κατά 2j και η απόλυτη τιμή των υπόλοιπων στοιχείων του s_k μπορεί να αυξάνεται το πολύ κατά 2j.

Ο κώδικας Hadamard n-ψηφίων είναι ένας μη γραμμικός κώδικας C που προκύπτει από τις γραμμές ενός πίνακα Hadamard τάξης n. Ο πίνακας αναπαρίσταται ως $A = \begin{bmatrix} H_n \\ -H_n \end{bmatrix}$ και ο κώδικας C προκύπτει αντικαθιστώντας κάθε στοιχείο -1 με 0.

Αν x και k είναι δύο διακεκριμένες γραμμές του C, τότε η απόσταση Hamming $d(x,y)$ είναι ίση με n/2. Οι γραμμές του C αποτελούν έναν δυαδικό (n, 2n, n/2) κώδικα.

Συνεπώς, ο κώδικας Hadamard είναι ουσιαστικά ένας δυαδικός κώδικας $(2^m, 2^{m+1}, 2^{m-1})$.

Παράδειγμα 4.2.3:

Για *m*=1,2, κατασκευάζουμε τους κώδικες Hadamard $(2^m, 2^{m+1}, 2^{m-1})$ για:

(i): *m*=1, χρησιμοποιούμε τον πίνακας Hadamard τάξης 2:

$$H_1 = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}.$$

Και ο κωδικός Hadamard που προκύπτει είναι:

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

C=(11,01,00,10).

(ii): Για *m*=2, χρησιμοποιούμε τον παρακάτω πίνακα Hadamard τάξης 4:

$$H_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}.$$

Ο κωδικός Hadamard που προκύπτει είναι:

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

C= (1111,0101,1100,0110,0000,1010,0011,1001).

4.3 Reed muller

Ο κώδικας Reed-Muller είναι ένας γραμμικός μπλοκ κωδικάς που περιλαμβάνει μια επέκταση του κώδικα Hamming. Δημιουργήθηκε το 1954 από τον I.S. Reed και D.E. Muller. Αρχικά, θα παρουσιάσουμε το παρακάτω λήμμα, το οποίο περιγράφει τρόπο κατασκευής νέων κωδίκων από προϋπάρχοντάς κωδικούς.

Λήμμα 4.3.1:

Έστω ένας $(n, M_1, d_1; 2)$ δυαδικός κώδικας C_1 και ένας άλλος $(n, M_2, d_2; 2)$ κώδικας C_2. Ορίζουμε έναν τρίτο κώδικα $\mathrm{C}_3 = \mathrm{C}_1 * \mathrm{C}_2$ από τη σχέση:

$$\mathrm{C}_3 = \{(u, u+v) : u \in \mathrm{C}_1, v \in \mathrm{C}_2\}$$

Τότε, ο C_3 είναι ένας $(2n, M_1 M_2, d_3)$ κώδικας, όπου $d_3 = \min\{2d_1, 2d_2\}$.

Απόδειξη 4.3.2:

Αν $(u_1, v_1) = (u_2, v_2)$ τότε ισχύει $(u_1, u_1 + v_1) = (u_1, u_2 + v_2)$. Ο αριθμός των κωδικών λέξεων στο C_3 είναι $M_1 M_2$. Έστω $a = (u, u + v)$ και $b = (u', u' + v')$ είναι διακεκριμένες κωδικές λέξεις του C_3. Αν $v = v'$, τότε $d(a, b) = 2d(u, u') \geq 2d_1$. Αν $v = v'$, τότε

$$\begin{aligned} d(a,b) &= d(u,u') + d(u+v, u'+v') \\ &= w(u+u') + w(u+v+u'+v') \\ &= d(u+u', 0) + d(u+u', v+v') \geq d(0, v+v') \text{ (από την τριγωνική ανισότητα)} \\ &= d(v, v') \geq d_2. \end{aligned}$$

Ο δυαδικός κώδικας Reed-Muller C(r,m) ορίζεται επαναληπτικά με τους παρακάτω κανόνες:

Για κάθε ακέραιο m και r, με $0 \leq r \leq m$, ορίζουμε C(r,m) ως έναν κώδικα με μήκος $n = 2^m$, με τις εξής σχέσεις :

I) C(0,m)={00…,11…},

II) C(r,m)={$(x, y + x)$: $x \in C(r, m-1), y \in C(r-1, m-1)$} για r=1, 2,…, m-1,

III) C(m,m)=είναι όλες οι κωδικές λέξεις μήκους 2^m.

Θεώρημα 4.3.3:

Για κάθε θετικό ακέραιο m και r, με $0 \leq r \leq m$, ο κώδικας Reed-Muller C(r,m) είναι ένας (n_r,M_r,d_r) δυαδικός κώδικας, όπου:

(α) $M_r = 2^a$,)όπου $\alpha = 1 + \binom{m}{1} + \ldots + \binom{m}{r}$,

(b) $n_r = 2^m$,

(c) $d_r = 2^{m-r}$.

Παραδείγματα:

C(0,0) = {0,1},

C(0,1) = {00,11},

C(0,2) = {0000,1111},

C(1,1) = {00,01,10,11},

C(1,2) = C(1,1)*C(0,1) = {(x,y+x): x∈C(1,1), y∈C(0,1)}

= {0000,0011,1010,1001,0101,0110,1111,1100}.

Παρατήρηση 4.3.4:

Αν r=1, τότε έχουμε έναν κωδικό Reed-Muller C(1,m). Από το προηγούμενο θεώρημα παρατηρούμε ότι $M = 2^{m+1}$, $n = 2^m$ και $d = 2^{m-1}$, άρα είναι ένας κωδικός $(2^m, 2^{m+1}, 2^{m-1})$ που ταυτίζετε με των κωδικό Hadamard. Άρα κάθε κωδικός Hadamard είναι ένας κωδικός Reed-Muller με r=1.

Από την προηγούμενη παρατήρηση παρατηρούμε ότι ο κωδικός Hadamard ανήκει στην οικογένεια κωδικών Reed-Muller.

Παράδειγμα 4.3.5:

Είχαμε ορίσει στο προηγούμενο παράδειγμα των κώδικα (2,4,1) χρησιμοποιώντας έναν πίνακα Hadamard τάξης 2. Ο κωδικός Hadamard είναι ο εξής:

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

Από την άλλη πλευρά, είχαμε ορίσει των κώδικα Reed-Muller C(1,1), ο οποίος είναι ο εξής:

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

Παρατηρούμε ότι ο κώδικας Hadamard και Reed-Muller για r=1 είναι ίδιοι. Αυτό είναι αποτέλεσμα της παρατήρησης που αναφέρθηκε προηγουμένως, ότι κάθε κωδικός Hadamard είναι ένας κωδικός Reed-Muller με r=1.

Κεφάλαιο 5. Εφαρμογή κωδικού Hadamard και ορίων του Plotkin

Ένας (n, M, d; q) κωδικός αναφέρεται σε ένα σύνολο από M κωδικές λέξεις με μήκος n, αλφάβητο q και απόσταση Hamming d. Ένας κωδικός θεωρείται βέλτιστος εάν ο αριθμός των κωδικών λέξεων M είναι ο μέγιστος δυνατός για τις δεδομένες τιμές των n, d και q. Το θεώρημα του Plotkin(1960) όρισε τα παρακάτω όρια για δυαδικούς κωδικούς:

(i) $M \leq 2\left[\frac{d}{2d-n}\right]$ αν d είναι άρτιος και $d \leq n < 2d$.

(ii) $M \leq 2n$ αν d είναι άρτιος και n=2d.

(iii) $M \leq 2\left[\frac{d+1}{2d+1-n}\right]$ αν d είναι περιττός και $d \leq n < 2d+1$.

(iv) $M \leq 2n+2$ αν d είναι περιττός και n=2d+1.

Ο Levenshtein απέδειξε ότι όρια Plotkin είναι "στενά", δηλαδή υπάρχει διάδικος κωδικός που ικανοποιεί αυτά τα όρια, εφόσον υπάρχουν αρκετοί πίνακες Hadamard. Επίσης, είναι γνωστό ότι εάν υπάρχουν κωδικοί που ισχύουν για τα όρια (i) και (ii), τότε υπάρχει και κωδικός που ισχύει τα όρια (iii) και (iv) μέσω της εφαρμογής το Θεωρήματος 4.1.18. Συνεπώς, μπορούμε να κατασκευάσουμε έναν κώδικα που ικανοποιεί τα όρια του Plotkin χρησιμοποιώντας τον πίνακα Hadamard αλλά και μια κατηγορία πινάκων που ονομάζονται πίνακες quasi-Hadamard.

5.1 Τέλειος κωδικός διόρθωσης σφαλμάτων

Η μέθοδος κατασκευής βέλτιστων κωδικών σφαλμάτων διόρθωσης κωδικών του Levenshtein που χρησιμοποιεί τους πίνακες Hadamard μπορεί να περιγραφή ως εξής. Έστω ότι δίνονται ο κωδικός C_1 με παραμέτρους $(n_1, M_1, d_1; 2)$ και ο κωδικός C_2 με παραμέτρους $(n_2, M_2, d_2; 2)$, όπου $M_2 \geq M_1$. Σύμφωνα με αυτά, κατασκευάζουμε έναν νέο κώδικα C με παραμέτρους $(n, M_1, d, 2)$. Το n και το d του C το ορίζουμε ως $n = a_1 n_1 + a_2 n_2$, και $d \geq a_1 d_1 + a_2 d_2$ με d άρτιο για κάθε τιμή του α_1 και α_2. Οι ακολουθίες α_1 και α_2 αντιπροσωπεύουν τις ακολουθίες από αντίγραφα του C_1 και C_2 αντίστοιχα. Η ακολουθία α_1 αποτελείται από αντίγραφα του C_1 που τοποθετούνται σε σειρά από τη μια άκρη ως την άλλη. Η ακολουθία α_2 αποτελείται από αντίγραφα του C_2. Τελικά, αφαιρούμε τις τελευταίες $(M_2 - M_1)$ γραμμές του C_2 για να λάβουμε τον επιθυμητό κώδικα. Ο κώδικας C ορίζεται ως εξής:

$$\mathrm{C} = \alpha_1 \mathrm{C}_1 \oplus a_2 \mathrm{C}_2.$$

Θεώρημα 5.1.1:

Αν υπάρχει πίνακας Hadamard τάξης 4t, τότε υπάρχουν η παρακάτω τέλειοι κωδικοί:

- (4t,8t,2t;2),
- (4t-1,4t,2t;2),
- (4t-1,8t,2t-1;2),
- (4t-2,2t,2t;2).

Απόδειξη 5.1.2:

Έστω H είναι ένας κανονικός πίνακας Hadamard τάξης $4t$ και J ένας τετραγωνικός πίνακας τάξης $4t$ με όλα τα στοιχεία του ίσα με ένα. Τότε οι $8t$ γραμμές των δύο πινάκων $W_{4t}^{(1)} = \frac{1}{2}(J + H)$ και $W_{4t}^{(2)} = \frac{1}{2}(J - H)$ αποτελούν τον κωδικό $(4t, 8t, 2t; 2)$.

Για να κατασκευάσουμε τους υπόλοιπους κωδικούς, πραγματοποιούμε τις παρακάτω διαγραφές

- Διαγράφουμε την πρώτη στήλη του H και το αποτέλεσμα το αποκαλούμε K.
- Διαγράφουμε όλες τις γραμμές του K που ξεκινούν από 1 και διαγράφουμε την πρώτη στήλη του παραγόμενου πίνακα και το αποτέλεσμα το αποκαλούμε Λ.

Έτσι, έχουμε:

- Για $4t$ γραμμές, ο πίνακας $W_{4t}^{(3)} = \frac{1}{2}(J + K)$ αντιπροσωπεύει τον κωδικό $((4t\text{-}1, 4t, 2t; 2)$.
- Για $8t$ γραμμές τον πίνακα $W_{4t}^{(3)}$ και $W_{4t}^{(4)} = \frac{1}{2}(J - K)$ αντιπροσωπεύουν τον κωδικό $(4t\text{-}1, 8t, 2t\text{-}1; 2)$.
- Για $2t$ γραμμές, ο πίνακας $W_{4t}^{(5)} = \frac{1}{2}(J + L)$ αντιπροσωπεύει τον κωδικό $(4t\text{-}2, 2t, 2t; 2)$.

Παράδειγμα: 5.2.3

Έχουμε τον πίνακα Hadamard H τάξης $4t$=16 από το παράδειγμα και θέλουμε να σχεδιάσουμε:

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
-1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
-1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
-1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1
\end{bmatrix}$$

Παρατηρούμε ότι ο πίνακας δεν είναι κανονικοποιημένος κι έτσι πολλαπλασιάζουμε τις γραμμές 5, 6, 7, 8, 13, 14, 15, 16 με -1 ώστε να έχουμε τον κανονικοποιημένο πίνακα:

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1
\end{bmatrix}$$

Έπειτα κατασκευάζουμε τους κώδικες όπως περιγράφετε στην απόδειξη του Θεωρήματος 5.1.1:

$$W_{16}^{(1)} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1
\end{bmatrix},$$

$$W_{16}^{(2)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Ο κωδικός (16,32,8) είναι $W_{16}^{(1)} + W_{16}^{(2)}$.

$$W_{16}^{(3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$W_{16}^{(4)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Ο κωδικός (15,32,7) είναι $W_{16}^{(3)}+W_{16}^{(4)}$.

$$W_{16}^{(3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Ο κωδικός (15,16,8) είναι $W_{16}^{(3)}$.

$$W_{16}^{(5)} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

Ο κωδικός (14,8,8;2) είναι $W_{16}^{(5)}$.

Αναλύοντας τα όρια του Plotkin (i) και (ii) για άρτιο *d*, μπορούμε να κατασκευάσουμε έναν κωδικό που ικανοποιεί τα όρια χρησιμοποιώντας την τεχνική που περιεγράφηκε προηγούμενος, καθώς και τους κωδικούς που παρέχονται από το Θεωρήματος 5.1.1. Έστω ένας θετικός ακέραιος *d* και ένας ακέραιος *n*, όπου ο d είναι άρτιος και ισχύει $d \leq n \leq 2d$. Μπορούμε να κατασκευάσουμε έναν τέλειο κωδικό (*n*,*M*,*d*;*2*), όπου *M=2*[*d*/(2*d*-*n*)]. Ορίζουμε:

$$r = \left[\frac{d}{2d-n}\right], \quad a_1 = d(2r+1) - n(r+1), \quad a_2 = rn - d(2r-1).$$

Χρησιμοποιώντας τους πίνακες που προέκυψαν την απόδειξη, μπορούμε να δημιουργήσουμε τον παρακάτω κώδικα:

- Αν ο *n* είναι άρτιος, τότε $\mathrm{C} = \frac{a_1}{2} W_{4r}^{(5)} \oplus \frac{a_2}{2} W_{4r+4}^{(5)}$.
- Αν ο *n* είναι περιττός και ο r είναι άρτιος, τότε $\mathrm{C} = a_1 W_{2r}^{(3)} \oplus \frac{a_2}{2} W_{4r+4}^{(5)}$.
- Αν ο *n* είναι περιττός και ο r είναι περιττός, τότε $\mathrm{C} = \frac{a_1}{2} W_{4r}^{(5)} \oplus \alpha_2 W_{2r+2}^{(4)}$.

Για έναν κωδικό, για να είναι τέλειος και να ισχύει το όριο, είναι απαραίτητη η ύπαρξη του πίνακα Hadamard τάξης 2*r* (αν *r* άρτιος), τάξης 2*r*+2(αν *r* περιττός), τάξης 4*r*, τάξης 4*r*+4. Αυτή η ύπαρξη είναι επαρκής για την ύπαρξη του τέλειου κωδικού που ικανοποιεί τα όρια.

Εφαρμογή: 5.1.4

Θέλουμε να κατασκευάσουμε έναν τέλειο κωδικό με μήκος κωδικών λέξεων 35 και ελάχιστη απόσταση Hamming 20.

Αρχικά θέτουμε *n*=35 και *d*=20 και υπολογίζουμε τον *M* για τον τέλειο κωδικό χρησιμοποιώντας το όριο του Plotkin για άρτιο *d*: $M \leq 2\left[\frac{d}{2d-n}\right]$, αφού ο d είναι άρτιος και $d \leq n < 2d$. Έχουμε $M \leq 2\left[\frac{20}{2*20-35}\right] = 2\left[\frac{20}{5}\right] = 2 * 4 = 8$. Οπότε ο τέλειος κωδικός θα είναι ο κωδικός (35,8,20;2).
Για να βρούμε των τέλειο κωδικό, εφαρμόζουμε τη μέθοδο Levenshtein. Υπολογίζουμε τις τιμές των $r,\ a_1$ και a_2 για *n*=35 και *d*=20:

$$r = \left[\frac{d}{2d-n}\right] = \left[\frac{20}{40-35}\right] = 4,$$

$$a_1 = d(2r+1) - n(r+1) = 20(8+1) - 35(4+1) = 20(9) - 35(5) = 180 - 175 = 5,$$

$$a_2 = rn - d(2r-1) = 4 * 35 - 20(8-1) = 140 - 140 = 0.$$

Σύμφωνα με το θεώρημα, ο τέλειος κωδικός για περιττό *n* και άρτιο *d* θα είναι:

$$\mathrm{C} = a_1 W_{2r}^{(3)} \oplus \frac{a_2}{2} W_{4r+4}^{(5)}\ .$$

Έτσι, για $r = 4,\ a_1 = 5,\ a_2 = 0$, ο τέλειος κωδικός είναι:

$$\mathrm{C} = 5W_8^{(3)}.$$

Για να υπολογίσουμε των $W_8^{(3)}$ χρειαζόμαστε έναν κανονικοποιμένο πίνακα Hadamard τάξης 8, όπως αναφέρεται στο προηγούμενο παράδειγμα έχουμε:

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{bmatrix},$$

$$W_8^3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix},$$

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{vmatrix}$$

Είναι ο τέλειος κωδικός μήκους 35 και ελάχιστης απόστασης Hamming 20.

5.2 Βέλτιστος κωδικός διόρθωσης σφαλμάτων

Ορισμός 5.2.1:

Ένας πίνακας quasi-Hadamard είναι ένας τετραγωνικός πίνακας τάξης *n*, με στοιχεία 1 και -1 και οι q γραμμές του είναι ορθογώνιες μεταξύ του, όπου $q \leq n$.

Ο πίνακας quasi-Hadamard πλησιάζει τον πραγματικό πίνακα Hadamard όσο περισσότερο αυξάνετε το πλήθος των ορθογώνιων γραμμών q σε σχέση με το *n*.

Τώρα θα επεκτείνουμε τη μέθοδο του Levenshtein's για την κατασκευή ενός βέλτιστου κωδικού για την περίπτωση του πίνακα quasi-Hadamard. Ο κωδικός που θα κατασκευάσουμε ονομάζεται κώδικας quasi-Hadamard.

Αρχικά, θεωρούμε έναν κανονικοποιμένο πίνακα quasi-Hadamard M_{4t} της τάξης $4t$ και βάθους q. Ορίζουμε τον πίνακα A'_{4t}, ο οποίος προκύπτει από τον πίνακα M_{4t} επιλέγοντας q γραμμές και αντικαθιστώντας 1 με 0 και -1 με 1.

Θεώρημα 5.2.2:

Έστω ότι έχουμε έναν κώδικα quasi-Hadamard. Τότε υπάρχουν οι παρακάτω κώδικες:

- ($4t$,q,$2t$),
- ($4t$-1,$2q$,$2t$-1),
- ($4t$,$2q$,$2t$),
- ($4t$-2,h,$2t$).

Απόδειξη 5.2.3:

Θεωρούμε έναν κανονικοποιμένο πίνακα quasi-Hadamard M_{4t} της τάξης $4t$ και βάθους q. Ορίζουμε τον πίνακα K'_{4t} όπου διαλέγουμε q γραμμές από τον πίνακα M_{4t} και αντικαθιστούμε 1 με 0 και -1 με 1. Τότε για τον κωδικό ($4t$-1,q,$2t$), ορίζουμε τον πίνακα A'_{4t}, ο οποίος είναι ίσος με τον πίνακα K'_{4t}, αλλά με την πρώτη στήλη διαγραμμένη. Για τον κωδικό ($4t$-1,$2q$,$2t$-1), ορίζουμε τον πίνακα B'_{4t}, ο οποίος είναι ίσος με τον πίνακα A'_{4t} και -A'_{4t}. Επίσης, για τον κωδικό ($4t$,$2q$,$2t$) ορίζουμε τον πίνακα C'_{4t}, ο οποίος είναι ίσος με των πίνακα K'_{4t} και -K'_{4t}. Τέλος, για τον κωδικό ($4t$-2,h,$2t$), ορίζουμε τον πίνακα D'_{4t}, ο οποίος αποτελείται από τις γραμμές του πίνακα A'_{4t} που ξεκινάνε από 0 και διαγεγραμμένη τη στήλη με τα μηδενικά.

Από τη στιγμή που είναι επέκταση του κώδικα Hadamard που έρχονται από τους πίνακες Hadamard, αφού K'_{4t} περιέχει q γραμμές και για οποιεσδήποτε δυο γραμμές είναι ορθογώνιες μεταξύ τους, έχουν $2t$ θέσεις που συμφωνούν και $2t$ που διαφέρουν, οπότε η απόσταση Hamming είναι $2t$.

Όσο πιο κοντά είναι το q στο $4t$, τόσο "καλύτεροι" είναι οι κωδικοί A'_{4t},B'_{4t}, C'_{4t} και D'_{4t}. Αυτό σημαίνει ότι ο αριθμός των κωδικών λέξεων που παράγεται είναι πολύ κοντά στην βέλτιστη μορφή που ορίζεται από τα όρια του Plotkin.

Θεώρημα 5.2.4:

Για d άρτιο για $2d > n \geq d$, ορίζουμε $k = \left[\frac{d}{2d-n}\right]$ και $a_1 = d(2k+1) - n(k+1)$, $a_2 = kn - d(2k-1)$.

Ένας καλός κώδικας διόρθωσης σφαλμάτων C' μήκους n και ελάχιστη απόσταση Hamming d προκύπτει από έναν κατάλληλο πίνακα quasi-Hadamard. Ο κώδικας θα έχει την ακόλουθη μορφή:

- $C' = \frac{a_1}{2} D'_{4r} \oplus \frac{a_2}{2} D'_{4r+4}$, εάν n είναι άρτιος.
- $C' = a_1 A'_{2r} \oplus \frac{a_2}{2} D'_{4r+4}$, εάν n είναι περιττός και r είναι άρτιος.
- $C' = \frac{a_1}{2} D'_{4r} \oplus \alpha_2 A'_{2r+2}$, εάν n είναι περιττός και r είναι περιττός.

Απόδειξη 5.2.5:

Με βάση τη μέθοδο του Levenshtein που περιγράψαμε προηγουμένως, ο κωδικός C′ περιέχει κωδικές λέξεις μεγέθους n όπως και ο κώδικάς C. Συνεχίζοντας, εάν ο n είναι περιττός, επιλέγουμε έναν κανονικό πίνακα quasi-Hadamard $M^1_{4\kappa}$ τάξης $4k$ και βάθος q_1, καθώς και έναν κανονικό πίνακα quasi-Hadamard $M^2_{4\kappa+4}$ τάξης 4 k +4 και βάθος q_2. Ορίζουμε τους πίνακες A^i για q_i γραμμές, που είναι κατά ζεύγη ορθογώνιες γραμμές από των πίνακα M^i με την πρώτη στήλη διαγεγραμμένη και όπου 1 αντικαθιστούμε με 0 και όπου -1 αντικαθιστούμε με 1. Ορίζουμε τον πίνακα D^i ως το h_i-σετ γραμμών του πίνακα A^i που ξεκινάνε με 0 με $0 \leq h_i \leq q_i$. Επομένως, ο κωδικός $C' = \frac{a_1}{2} D^1_{4r} \oplus \frac{a_2}{2} D^2_{4r+4}$ περιέχει τον κωδικό $(n, \min\{h_1, h_2\}, d)$.

Αν ο n είναι άρτιος, επιλέγουμε έναν κανονικό πίνακα quasi-Hadamard $M^1_{2\kappa}$ τάξης $2k$ και βάθος q_1, καθώς και έναν κανονικό πίνακα quasi-Hadamard $M^2_{4\kappa+4}$ τάξης $4k$ +4 και βάθους q_2. Ορίζουμε τους A^i για q_i γραμμές, που είναι ορθογώνιες μεταξύ τους από τον M^i με πρώτη στήλη διαγεγραμμένη και όπου 1 αντικαθιστούμε με 0 και όπου -1 αντικαθιστούμε με 1. Ορίζουμε D^2 με h_2-σετ γραμμών A^2 που ξεκινούν με 0 με $0 \leq h_2 \leq q_2$. Έτσι, ο κώδικας $C' = \alpha_1 A^1_{4r} \oplus \frac{a_2}{2} D^2_{4r+4}$ περιέχει τον κωδικό $(n, \min\{q_1, h_2\}, d)$.

Αν τα n και d είναι άρτια, επιλέγουμε έναν κανονικό πίνακα quasi-Hadamard $M^1_{4\kappa}$ τάξης $4k$ και βάθους q_1, και κανονικό πίνακα quasi-Hadamard M^2_{2k+2} τάξης $2k$+2 και βάθους q_2. Ορίζουμε τους A^i για q_i γραμμές, κατά ζεύγη ορθογώνιες από τον πίνακα M^i με την πρώτη στήλη διαγεγραμμένη και όπου 1 αντικαθιστούμε με 0 και όπου -1 αντικαθιστούμε με 1. Ορίζουμε D^1 με h_1-σετ γραμμών A^1 που ξεκινάνε με 0 με $0 \leq h_1 \leq q_1$. Επομένως, ο κωδικός C′ $= \frac{a_1}{2} D'_{4k} \oplus \frac{a_2}{2} A'_{2k+2}$ περιέχει τον κωδικό $(n, \min\{h_1, q_2\}, d)$.

Η απόσταση του κώδικα C′ από τα όρια του Plotkin εξαρτάται από τις τιμές των q_i και h_i.

Εφαρμογή 5.2.6:

Έστω ότι πρέπει να βρούμε έναν αριθμό από το διάστημα [1,20] και έχουμε στη διάθεσή μας 16 ερωτήσεις, όπου η απάντηση είναι ναι ή όχι, αλλά υπάρχει η περίπτωση να μας πουν μέχρι τρία ψέματα. Εμείς πρέπει να βρούμε τον σωστό αριθμό και ποια είναι αυτά τα ψέματα.

Για να κερδίσουμε, πρέπει να κατασκευάσουμε έναν κωδικά διόρθωσης σφαλμάτων που θα μπορεί να διορθώνει μέχρι τρία σφάλματα και θα έχει 20 κωδικές λέξεις. Γράφουμε έναν για κάθε ναι και μηδέν για κάθε όχι. Έπειτα, επιλέγουμε ερωτήσεις έτσι ώστε η δυαδική ακολουθία που προκύπτει

σε κάθε περίπτωση να συμπίπτει με την αντίστοιχη κωδική λέξη. Αυτό απαιτεί ότι το μήκος της κωδικής λέξης θα πρέπει να είναι ίσο με τον αριθμό των ερωτήσεων. Συνολικά, χρειαζόμαστε έναν (*n*,*M*,*d*;*2*) κωδικό, με τουλάχιστον 20 λέξης οπότε $M \geq 20$, το μήκος τους να είναι 16 και κατάλληλο d ώστε να διορθώνει τουλάχιστον τρία σφάλματα. Από προηγούμενο θεώρημα, γνωρίζουμε ότι για να διορθώσουμε e σφάλματα χρειαζόμαστε ένα κωδικό με ελάχιστη απόσταση d τέτοια ώστε $\left[\frac{d-1}{2}\right] \geq e$. Οπότε αφού θέλουμε να διορθώσουμε 3 σφάλματα το e=3, οπότε λύνουμε την ανισότητα και έχουμε το αποτέλεσμα $d \geq 7$.

Υποθέτουμε ότι d=8. Χρησιμοποιώντας το δεύτερο όριο του Plotkin, με n=2d=16 και M οι κωδικές λέξεις είναι πάντα M≤2n=32. Χρησιμοποιώντας τη μέθοδο του Levenshtein's, ο κωδικός $C_{16}=\begin{bmatrix} W_{16}^{(2)} \\ W_{16}^{(1)} \end{bmatrix}$ όπου $W_{16}^{(2)}$ και $W_{16}^{(1)}$ είναι οι πίνακες από το Παράδειγμα 5.1.4. Έτσι, ο κώδικας C_{16} δημιουργήθηκε από τον πίνακα Hadamard τάξης 16 και είναι ένας βέλτιστος κώδικας μεγέθους 16 με ελάχιστη απόσταση 8. Αφού ο C_{16} περιέχει 32 κωδικές λέξεις ο C_{16} μπορεί να χρησιμοποιηθεί για να λύσει το παιχνίδι, αλλά θα προτιμούσαμε έναν μικρότερο κώδικα με 20 κωδικές λέξεις. Για να δημιουργήσουμε έναν τέτοιο κώδικα, θα χρησιμοποιήσουμε τον πίνακα quasi-Hadamard τάξης 16 και βάθους 10. Θεωρούμε έναν πίνακα quasi-Hadamard M_{16} ο οποίος προκύπτει από έναν πίνακα Hadamard τάξης 16 όπως στο παράδειγμα και τυχαία αλλάζουμε τα στοιχεία στις γραμμές ένα, δώδεκα, δεκατρία, δεκατέσσερα, δεκαπέντε, δεκαέξι.

$$\begin{bmatrix}
* & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
* & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
* & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
* & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
* & * & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\
* & * & * & * & * & * & * & * & * & * & * & * & * & * & * & *
\end{bmatrix}$$

Οπότε από το θεώρημα, κατασκευάζουμε (16,20,8) κωδικό C_{16}'.

0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0
0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1
1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1
1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0
1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	1

Τώρα χαρτογραφούμε κάθε ακέραιο i στο εύρος [1,20] για κάθε i υπάρχει η κωδική λέξη στο c_i στον C'_{16}. Τώρα ρωτάμε τις παρακάτω ερωτήσεις:

(1)>10

(2){1,3,5,7,9,12,14,16,18,20}

(3)2,3mod(4)

(4)1,2mod(4)

(5){4,5,6,7,11,12,13,18,19,20}

(6){1,3,4,6,9,12,15,17,18,20}

(7){2,3,4,5,10,11,16,17,18,19}

(8){1,2,4,7,9,10,13,15,16,18}

(9)[8,17]

(10){1,2,5,7,8,10,11,14,15,20}

(11){2,3,6,7,8,9,11,14,15,20}

(12){1,2,5,6,8,13,14,17,19,20}

(13)[4,13]

(14){1,3,4,6,8,10,12,15,17,19}

(15){2,3,4,5,8,9,11,16,17,20}

(16){1,2,4,7,8,13,15,16,19,20}

Υποθέτουμε ένα διάνυσμα απάντησης $\alpha = (\alpha_1, \dots, \alpha_{16})$. Επιλέγουμε μια μοναδική κωδική λέξη c_i από τον C'_{16}, όπου το άθροισμα α modulo 2 παράγει ένα διάνυσμα με το πολύ τρία μη μηδενικές στοιχεία. Στη συνέχεια, διορθώνουμε τα στοιχεία που δεν είναι μηδέν, καθιστώντας σαφές πότε ο

αντίπαλος παίχτης ψεύδεται. Συνεπώς, όταν μας ρωτήσει ποια είναι η σωστή απάντηση, επιλέγουμε τη γραμμή που είναι ίδια με τη δική μας που οδηγεί στην λύση.

Σημείωση: Θα μπορούσαμε να χρησιμοποιήσουμε οποιονδήποτε πίνακα quasi-Hadamard τάξης 16 και βάθους 10 για να λύσει το παιχνίδι. Το μόνο που αλλάζει είναι οι ερωτήσεις για να αντιστοιχούν στης καινούριες κωδικές λέξεις.

ΚΕΦΑΛΑΙΟ 3. ΒΙΒΛΙΟΓΡΑΦΙΑ

1. K. Fender, (2016), Recursively, «*CONSTRUCTED UNIT HADAMARD MATRICES: THEIR EXCESS AND A RESULTING FAMILY OF BIBDS*», University of Lethbridge.
2. A. Hedayat and W.D. Wallis, (1978), «*HADAMARD MATRICES AND THEIR APPLICATION*», University of Illinois at Chicago Circle and University of Newcastle.
3. Jennifer Wallis, (1968), «*CONFIGURATIONS AND HADAMARD MATRICES*».
4. A.M. Leghwel, «*ON SOME METHODS OF CONSTRUCTING HADAMARD MATRICES*», Alasmarya Islamic University.
5. J. Seberry, M. Yamada, (1992), «*HADAMARD MATRICES, SEQUENCES, AND BLOCK DESIGNS*»,431-559, University of Wollongong, Hoboken, New Jersey, USA JOHN WILEY & SON.
6. J. Seberry, M. Yamada, (2020), «*HADAMARD MATRICES: CONSTRUCTIONS USING NYMBER THEORY AND LINEAR ALGEBRA*»,1-48, Hoboken, New Jersey, USA JOHN WILEY & SON.
7. A.J. Laub, (2005), «*MATRIX FOR SCIENTISTS AND ENGINEERS*»,137-150, University of California.
8. V. Alvarez, J.A. Armario, M.D. Frau, E. Martin, and A. Osuma, (2007) «*ERROR CORRECTING CODES FROM QUASI-HADAMARD MATRICES*», University of Sevilla.
9. K. Brown, (1994), «*LINEAR CODES AND ERROR-CORRECTION*», University of Northern Iowa.
10. Χ. Κουκουβίνος, Α. Παπαϊωάνου (2003), «*ΘΕΩΡΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΚΩΔΙΚΩΝ*», Αθήνα.
11. J.B. Fraleigh, (2016), «*ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΛΓΕΒΡΑ*», Ηράκλειο.
12. Α.Γ. Φελλούρης, (2005), «*ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ ΚΑΙ ΑΝΑΛΥΤΙΚΗ ΓΕΩΜΕΤΡΙΑ*», Αθήνα.
13. Ν. Καδιανάκης, Σ. Καρανάσιος, (2016), «*ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ ΑΝΑΛΥΤΙΚΗ ΓΕΩΜΕΤΡΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ*», Αθήνα.
14. Γ. Παντελίδης, Δ. Κραββαρίτης, Β. Νασόπουλος, Τσεκρέκος Π., (2016), «*ΓΡΑΜΜΙΚΗ ΑΛΓΕΒΡΑ*», Αθήνα.