Unbiased Hadamard Matrices and Bent Sequences

by

Vlad Zaitsev

MATH 4995 - Undergraduate Thesis in Mathematics

Department of Mathematics and Computer Science
University of Lethbridge

Abstract

A *Hadamard* matrix is a ± 1 matrix such that any two distinct rows are mutually orthogonal. A bent sequence is a row vector x, attached to a Hadamard matrix of square order, say H, such that the inner product of every row of H and x is constant in absolute value.

Recently, an application of bent sequences related to Hadamard matrices was motivated by a security application relating to Physically Unclonable Functions (Solé, et al., 2021). In the paper, the authors work with rows of Hadamard matrices, referred to as *Hadamard codes*. The authors conjecture that to maximize entropy when adding an additional codeword, the codeword should minimize total deviation. Codewords coming from bent sequences minimize total deviation.

Bush-type, as well as Regular Hadamard matrices, are known to be useful in providing bent sequences. In this thesis, we will generalize the notion of bent sequences to complex Hadamard matrices. We will proceed to show several constructions giving rise to an abundant set of bent sequences using Latin squares. Finally, we will generalize bent sequences to weighing matrices, by allowing zero entries and generalizing constructions to include zero entries.

Acknowledgements

There are many individuals who deserve to be recognized. First is my supervisor, Dr. Hadi Kharaghani, whose contributions cannot be overstated. I am grateful to Dr. Kharaghani for introducing me to research and guiding me throughout my degree. Dr. Kharaghani has exhibited incredible patience, provided excellent insights and has provided countless opportunities for me to further enhance my undergraduate education.

Committee member Dr. Amir Akbary also deserves special recognition for providing feedback, greatly improving the quality of this work. Moreover, Dr. Akbary is an excellent professor, and I am grateful I have had the privilege to be taught by such an exceptional teacher.

Lastly, I would also like to extend my gratitude to the numerous individuals within the Department of Mathematics and Computer Science who have helped me secure a most rewarding undergraduate student career. The incredible individuals within this department continue to inspire me, fueling my passion for learning and pushing me to achieve my highest potential.

Table of Contents

List of Symbols

0_n	Denotes the $n \times n$ all zero matrix
1_n	Denotes the all ones column vector of length n
$\bar{z}$	Denotes the complex conjugate of $z \in \mathbb{C}$
$\mathbb{F}_q$	Denotes the finite field of order q
$\mathbb{Z}_m$	Denotes the ring of residue classes modulo n
A^*	Denotes the conjugate-transpose of the matrix A
A^T	Denotes the transpose of the matrix A
I_n	Denotes the standard identity matrix of order n
J_n	Denotes an $n \times n$ all ones matrix

Chapter 1

Introduction

The evolution of modern computers has been an instrumental force driving various areas of mathematics research. Computing has revolutionized the way we process, store, and transmit data. However, at the center of this digital revolution lie elaborate algorithms and cryptographic techniques aimed at safeguarding sensitive information and ensuring secure communication channels. Among these cryptographic constructs, developments in boolean algebra led to the discovery of bent functions, which are indispensable tools, intricately woven into the fabric of modern encryption protocols. However, as is often the case in research, the utility of many abstract concepts is only realized after many years of research and development.

1.1 Motivation

In [24], an application of bent sequences, objects synonymous to bent functions, was motivated by a security application relating to Physically Unclonable Functions. This discovery widened research interest, fueling many discoveries and further generalizations of bent sequences. Even during the short duration of the writing of this thesis, there have been various developments and generalizations relating to bent sequences. This thesis aims to discuss, examine and provide further insights into recent developments.

1.2 Thesis Outline

As our exploration of bent sequences is linked to a number of combinatorial objects, our discussion will begin with necessary preliminaries. These preliminaries will be discussed in Chapters 2-4.

Following the introduction, Chapter 2 will introduce Hadamard matrices, acting as the groundwork for future generalizations. In this chapter, we will discuss properties, and showcase several useful constructions and existence results relating to Hadamard matrices. Finally, we end the chapter by exploring different classifications of Hadamard matrices

In Chapter 3, we generalize Hadamard matrices. In the first generalization, we extend the entries of Hadamard matrices to include zero, sparking our discussion of weighing matrices. Section 3.1, dedicated to weighing matrices, will include several useful constructions as well as present some existence results. In Section 3.2, we allow the entries of weighing matrices to take form as complex roots of unity, providing the definitions for complex weighing matrices.

Chapter 4 shifts our focus away from generalizations of Hadamard matrices, to that of Latin squares. In this chapter, we introduce and explore general constructions and existence results for orthogonal Latin squares. The chapter ends with a brief introduction to suitable Latin squares and connects these objects to orthogonal Latin squares.

In Chapter 5 we shift our focus to that of bent functions. The chapter will begin with an overview of Boolean functions, providing the necessary groundwork to fuel our discussion of bent functions. Lastly, we will introduce and explore the recently discovered applications of bent sequences.

Many of the results contained in Chapters 2-5 are found in Stinson's book of Combinatorial Designs [25]. However, changes to some proofs are presented throughout these four chapters. Notably, Corollaries 3.19, 3.20, Propositions 3.29, 5.30, 5.31,

Theorems 4.14, 4.16, 4.20 and Lemma 3.12 all show known results which have been proven using modified techniques not found in the referenced literature.

Chapter 6 contains many of the constructions discovered throughout the duration of the writing of this thesis. The general construction using Latin squares and auxiliary matrices is based on our paper [23] in collaboration with Shi, Lu, Kharaghani, and Solé. The chapter begins by introducing the last necessary preliminary objects, namely unbiased Hadamard matrices. We will demonstrate several constructions of complex bent sequences using unbiased Hadamard matrices and Latin squares. Lastly, we generalize bent sequences to include zero, enabling us to further generalize previous results. New results in this chapter include Theorems 6.7, 6.13, 6.16 and Lemma 6.9, not included in [23].

1.3 Notation

When writing matrices, we denote -1 as $-$ and $-i$ as j. For example, we denote the matrix

$$\begin{pmatrix} 1 & -1 \\ i & -i \end{pmatrix}$$

as

$$\begin{pmatrix} 1 & - \\ i & j \end{pmatrix}.$$

Finally, a note on indexing matrices. If we let M be any $n \times m$ matrix, unless explicitly stated the rows and columns are naturally indexed by $1, 2, \ldots, n$ and $1, 2, \ldots, m$, respectively.

Chapter 2

Hadamard Matrices

Hadamard matrices possess remarkable properties that have found applications in various fields, ranging from mathematics and computer science to telecommunications and quantum computing. Due to their elegant structure and diverse applications, these matrices have enthralled researchers for over a century.

In modern telecommunications, Hadamard matrices have found many applications in digital signal processing, stemming from their error-correcting capabilities [28]. The error-correcting capabilities of Hadamard matrices ensure reliable data transmission over noisy telecommunication channels. Furthermore, Hadamard matrices play a vital role in designing spreading sequences which allow multiple users to share the same frequency bands without interference [12].

In quantum computing, Hadamard Matrices are fundamental components in quantum circuits [16]. Specifically, Hadamard matrices are used to form Hadamard gates, which are used to perform quantum operations.

Closely tied to the work behind this thesis, Hadamard matrices find applications in combinatorial mathematics. In particular, Hadamard matrices are related to many combinatorial objects including balanced incomplete block designs, orthogonal arrays, difference sets and association schemes [25].

Mathematicians have also presented generalized forms of Hadamard matrices and applied these generalized properties to various combinatorial objects. Throughout

the thesis, we will encounter many generalizations of Hadamard matrices, explore some important properties, and eventually relate these generalizations to the subject of focus, bent sequences.

2.1 Properties

We now state the formal definition of a Hadamard matrix.

Definition 2.1. *A Hadamard matrix of order n is a square matrix H with entries in $\{-1, 1\}$ such that*

$$HH^T = nI_n$$

where I_n denotes the identity matrix of order n.

By way of explanation, given a Hadamard matrix of order n, say H, the condition $HH^T = nI_n$ is equivalent to stating that the row vectors of H are pairwise orthogonal. Below we give some examples of Hadamard matrices.

Example 2.2. *The following are Hadamard matrices of order 1, 2 and 4.*

$$H_1 = \begin{pmatrix} 1 \end{pmatrix}, \; H_2 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}, \; H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}$$

The condition that $HH^T = nI_n$ is also equivalent to stating that the column vectors of H are also pairwise orthogonal. This statement is proven in the following proposition.

Proposition 2.3. *If H is a Hadamard matrix of order n, then H^T is a Hadamard matrix of order n.*

Proof. Since H is Hadamard, we have $HH^T = nI_n$. Then multiplying on the left by H^{-1} we see $H^T = nH^{-1}$. Therefore, using the fact that $(H^T)^T = H$, it follows that

$$H^T(H^T)^T = H^T H = nH^{-1}H = nI_n.$$

□

A natural question to ask when learning about Hadamard matrices is for which n does there exist a Hadamard matrix of order n? To answer this question, we must build the necessary framework to prove an important necessary existence condition for Hadamard matrices.

2.1.1 Equivalenence of Hadamard Matrices

Looking at the examples of Hadamard matrices, one notices that by multiplying any row or column of a Hadamard matrix by -1, or permuting the order of rows and columns, the matrix remains a Hadamard matrix. In general, since the rows and columns of a Hadamard matrix H are pairwise orthogonal, it is not hard to see that negating a row or column of H, the resulting matrix retains the pairwise row and pairwise column orthogonality. Similarly, we can also permute the rows and columns of a Hadamard matrix, with the resulting matrix retaining the orthogonality of both rows and columns. We summarize these observations in the following proposition.

Proposition 2.4. *If H is a Hadamard matrix of order n and P and Q are $n \times n$ signed permutation matrices, then PHQ is a Hadamard matrix of order n.*

Proof. As P and Q are signed permutation matrices, we have $PP^T = I_n$ and $QQ^T = I_n$. It follows that

$$(PHQ)(PHQ)^T = PHQQ^TH^TP^T = PHH^TP^T = nPP^T = nI_n.$$

□

The observation that negating any row or column of a Hadamard matrix H gives us another Hadamard matrix naturally gives rise to the following definition of Hadamard equivalence.

Definition 2.5. *Let H and K be two Hadamard matrices of order n. The matrices H and K are said to be equivalent if there exist two $n \times n$ signed permutation matrices P and Q such that $H = PKQ$.*

Put differently, two Hadamard matrices of order n, say H and K, are equivalent if K can be obtained by performing a series of row and column permutations and negations. Hadamard equivalence is also symmetric, reflexive and transitive. Thus we can define an *equivalence class* of a Hadamard matrix to be the set of all Hadamard matrices to which it is equivalent. The following definition provides us with a standard presentation of Hadamard matrices.

Definition 2.6. *A normalized Hadamard matrix is a Hadamard matrix in which every entry in the first row and the first column is* 1.

In the previous example, the matrices H_1, H_2 and H_4 are all normalized Hadamard matrices. It is straightforward to see that given any Hadamard matrix H, we can multiply rows and columns whose first entries are -1 by -1 to normalize the matrix. This observation is summarized in the following proposition.

Proposition 2.7. *Any Hadamard matrix is equivalent to a normalized Hadamard matrix.*

2.1.2 Existence of Hadamard Matrices

We have now established the necessary framework to prove the following result, which gives us a well-known existence condition for a Hadamard matrix of order n.

Proposition 2.8. *If H is a Hadamard matrix of order $n > 2$, then $n \equiv 0 \pmod 4$.*

Proof. From Proposition 2.8, we know H is equivalent to a normalized Hadamard matrix. Thus, without loss of generality, we can assume H is normalized. Then, it is clear that the first entry of every column of H will be 1. As the entries of H are ± 1, the possible second and third entries of any column of H will be $1, 1$, or $1, -1$, or

$-1, 1$, or $-1, -1$. Suppose that there are a columns whose second and third entries are $1, 1$, b columns whose second and third entries are $1, -1$, c columns whose second and third entries are $-1, 1$ and d columns whose second and third entries are $-1, -1$. By permitting columns we have the following visual presentation of the normalized Hadamard matrix.

$$\left(\begin{array}{cccccccccccccccccccc}
1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\
1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & - & - & \cdots & - & - & - & - & \cdots & - & - \\
1 & 1 & \cdots & 1 & 1 & - & - & \cdots & - & - & 1 & 1 & \cdots & 1 & 1 & - & - & \cdots & - & - \\
 & \vdots & & & & & \vdots & & & & & \vdots & & & & & \vdots & & &
\end{array}\right)$$

$$\underbrace{\qquad\qquad}_{a \text{ columns}} \quad \underbrace{\qquad\qquad\qquad}_{b \text{ columns}} \quad \underbrace{\qquad\qquad\qquad}_{c \text{ columns}} \quad \underbrace{\qquad\qquad\qquad}_{d \text{ columns}}$$

Then, as H is a Hadamard matrix of order n, we know the rows of H are orthogonal, giving us the following system of equations.

$$\begin{aligned}
a + b + c + d &= n \quad \text{since the order of } H \text{ is } n, \\
a + b - c - d &= 0 \quad \text{as rows one and two are orthogonal,} \\
a - b + c - d &= 0 \quad \text{as rows one and three are orthogonal,} \\
a - b - c + d &= 0 \quad \text{as rows two and three are orthogonal.}
\end{aligned}$$

A straightforward calculation verifies that the above system has the unique solution

$$a = b = c = d = \frac{n}{4}.$$

As each of the variables a, b, c, d represents some number of columns, a, b, c and d must be divisible by 4. Therefore, we have that $a + b + c + d = n \equiv 0 \pmod 4$.

□

We have already seen Hadamard matrices of order 1, 2, and 4. Table 1 shows the number of known equivalence classes of Hadamard matrices of order n for $n \leq 40$. Aside from the number of equivalence classes dropping from 5 to 3 as we move from

Hadamard matrices of order 16 to order 20, the data indicates a rapidly growing number of equivalence classes for larger orders. The largest order completely classified is 32, which was done by Kharaghani and Tayfey-Rezaie in [10]. The lower bounds of inequivalent Hadamard matrices of order 36 and 40 are found in [5]. A natural question to ask now is whether n being a multiple of 4 is not just an existence condition, but instead a sufficient condition for the existence of a Hadamard matrix of order n. This condition is known as the Hadamard Conjecture and is believed to be true.

Conjecture 2.9. *There exists a Hadamard matrix of order n if and only if $n = 1, 2$ or $n \equiv 0 \pmod 4$.*

order	inequivalent matrices
1	1
2	1
4	1
8	1
12	1
16	5
20	3
24	60
28	487
32	13710027
36	> 15000000
40	> 366000000000

Table 2.1: Number of equivalence classes of Hadamard matrices of order $n \leq 40$.

Currently, there are 3 possible multiples of 4 less than 1000 for which no Hadamard matrix of that order is known. These orders are 668, 716 and 892. Previously, the smallest order which was not known was 428, which was discovered by Kharaghani

and Tayfey-Rezaie in 2004 [9], making 668 the smallest order for which the Hadamard Conjecture remains open.

In the upcoming section, we present some ways to construct infinite classes of Hadamard matrices.

2.2 Constructions

Although Hadamard matrices are named after the French mathematician Jacques Hadamard, the first constructions were a result of Sylvester in 1867 [27], approximately 26 years before Hadamard published his results in 1893. Sylvester was curious about the combinatorial properties of these matrices and began his work on Hadamard matrices as a way to solve a tessellation problem. We now showcase Sylvester's result, which gives the first discovered infinite class of Hadamard matrices.

Theorem 2.10 (Sylvester, [27])**.** *If H is a Hadamard matrix of order n, then the block matrix*

$$\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$$

is a Hadamard matrix of order $2n$.

Proof. Since H is a Hadamard matrix of order n, we use the fact that $HH^T = nI_n$ to simplify the following matrix multiplication.

$$\begin{aligned} \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \begin{pmatrix} H & H \\ H & -H \end{pmatrix}^T &= \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \begin{pmatrix} H^T & H^T \\ H^T & -H^T \end{pmatrix} \\ &= \begin{pmatrix} HH^T + HH^T & HH^T - HH^T \\ HH^T - HH^T & HH^T + HH^T \end{pmatrix} \\ &= \begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} \\ &= 2nI_{2n}. \end{aligned}$$

□

Using Theorem 2.10, Sylvester was able to prove the existence of the Hadamard matrices of order 2^n. The Hadamard matrices of order 2^n obtained from Sylvester's construction are called the *Sylvester Hadamard matrices*.

Corollary 2.11 (Sylvester, [27])**.** *Let $n \in \mathbb{N}$. Then there exists a Hadamard matrix of order 2^n.*

Proof. The proof follows by induction on n. When $n = 0$, H_1 is the corresponding Hadamard matrix of order 1. When $n = 1$, H_2 is the corresponding Hadamard matrix of order 2. Suppose that H_{2^n} exists for some $n \geq 1$. Then applying Theorem 2.10 we see

$$H_{2^{n+1}} = \begin{pmatrix} H_{2^n} & H_{2^n} \\ H_{2^n} & -H_{2^n} \end{pmatrix}$$

is a Hadamard matrix of order 2^{n+1}. Therefore, there exists a Hadamard matrix of order 2^n for all $n \in \mathbb{N}$. □

Jacques Hadamard would then generalize Sylvester's result in 1893, whose study of Hadamard matrices was motivated by trying to answer the maximal determinant problem. The maximal determinant problem commonly refers to finding the largest determinant of a matrix with elements in $\{1, -1\}$. However, Hadamard was not only intrigued by the determinants of ± 1-matrices but also interested in the determinants of matrices with complex entries. In his 1893 paper [6], Hadamard presented his determinant bound, commonly referred to as Hadamard's inequality. This result was presented without reference to matrices, instead, Hadamard used determinant to refer to the homogeneous polynomial of degree n having n^2 variables, which comes from calculating the determinant of a matrix of order n whose entries are commuting indeterminates. The result using modern terminology is shown below.

Theorem 2.12 (Hadamard's inequality)**.** *Let M be the matrix having rows r_i, then*

$$|\det(M)| \leq \prod_{i=1}^{n} \|r_i\| .$$

Equality in Hadamard's inequality is achieved if and only if the rows are orthogonal. We now showcase an immediate consequence of Hadamard's inequality.

Corollary 2.13. *Let M be a matrix having entries ± 1. Then*

$$|\det(M)| \leq n^{n/2}.$$

Hadamard realized that the Sylvester Hadamard matrices attained this bound. Hence, the matrices that attain the determinant bound of $n^{n/2}$ are now called Hadamard matrices. In this thesis, Hadamard also produced Hadamard matrices of order 12 and 20 and extended Sylvester's construction. However, to show Hadamard's generalized construction, we must first define the Kronecker product. We begin by giving the definition.

Definition 2.14. *Let $A = (a_{ij})$ be an $n \times m$ matrix, and let $B = (b_{ij})$ be a $p \times q$ matrix. The Kronecker product $A \otimes B$ of the matrices A and B is the $np \times mq$ block matrix*

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{pmatrix}.$$

The Kronecker product is interesting for various reasons. For instance, the Kronecker product is bilinear and associative. Furthermore, for matrices of the appropriate dimension, the Kronecker product satisfies the mixed-product property (property 2). Let A, B, C and D be matrices over a commutative ring of appropriate dimension (meaning that AC and BD exist), then the Kronecker product satisfies the usual properties of bilinearity and associativity, as well as the following properties:

1. $(A + B) \otimes (C + D) = A \otimes C + A \otimes D + B \otimes C + B \otimes D$,

2. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$,

3. $(rA) \otimes B = A \otimes (rB) = r(A \otimes B)$ for any scalar r,

Example 2.15. *Among the list of properties of the Kronecker product, commutativity is not listed. Aside from specific examples, $A \otimes B$ and $B \otimes A$ are different matrices. However, as shown in [21] these matrices are still permutationally equivalent. For example, if $A = I_2$ and $B = J_2$, then*

$$A \otimes B = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \text{ and}$$

$$B \otimes A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Hadamard did not present his generalized construction in terms of Kronecker products. However, using the Kronecker product and some of its properties, we can more easily demonstrate Hadamard's results, while also introducing an important tool which will be used in future constructions.

Theorem 2.16 (Hadamard, [6])**.** *If H is a Hadamarmd matrix of order n and K is a Hadamard matrix of order k, then $H \otimes K$ is a Hadamard matrix of order nk.*

Proof. Using Property 2 of the Kronecker product we simplify

$$(H \otimes K)(H \otimes K)^T = (HH^T) \otimes (KK^T) = (nI_n) \otimes (kI_k) = nkI_{nk}.$$

□

Example 2.17. *We have already seen Sylvester Hadamard matrices of order* 2 *and* 4*. Using the Kronecker product we create a Sylvester Hadamard matrix of order* 8*:*

$$H_2 \otimes H_4 = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{pmatrix}$$

2.3 Classifications

In this section, we introduce and give examples of some special types of Hadamard matrices.

Definition 2.18. *Let H be a Hadamard matrix of order n. Then H is a skew-type Hadamard matrix if $H + H^T = 2I_n$.*

Example 2.19. *The following is a skew-type Hadamard matrix of order* 8*:*

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

Another formulation of the definition states that H is a skew-type Hadamard matrix of order n, if $H = A + I_n$, where $A^T = -A$. We now state the following fact about skew-type Hadamard matrices.

Remark 2.20. *If $H = A + I_n$, then H is a skew-type Hadamard matrix of order n if and only if A is a skew-symmetric conference matrix of order n.*

Recently, there has been a significant effort put towards classifying skew-type Hadamard matrices of order 36. In the 2024 [1], it was shown that there are at least 157132 SH-inequivalent skew-type Hadamard matrices of order 36 (Note that SH-inequivalent means there does not exist a signed permutation matrix P such that $H = PKP^T$). To understand the magnitude of the task that is the classification of Hadamard matrices of order 36, it is shown in [7] that there are only 7227 SH-inequivalent skew-type Hadamard matrices of order 32. A straightforward computation shows that there are approximately 1900 times more Hadamard matrices than skew-type Hadamard matrices of order 32. Using this value, we can use the 157132 known SH-inequivalent skew-type Hadamard matrices to estimate that if this pattern holds, there are likely over 300 million inequivalent Hadamard matrices of order 36.

The next two special types of Hadamard matrices are closely related.

Definition 2.21. *A Hadamard matrix H is regular if all row sums are equal.*

We present a well-known property of regular Hadamard matrices.

Lemma 2.22. *Let H be a regular Hadamard matrix of order n. Then the absolute value of the row and column sums must be $\sqrt{n}$.*

Proof. Let r_i denote the row sums of H and let j be the column vector of all ones of length n. First, we will calculate the row sums of H. Observe that

$$(Hj)^T(Hj) = j^T H^T H j = j^T n I_n j = n j^T j = n^2.$$

Thus

$$\sum_{i=1}^{n} \|r_i\|^2 = n^2$$

and since H is regular, each $\|r_i\|^2 = n$, and so $\|r_i\| = \sqrt{n}$ as desired. To see that the column sums of H are also $\sqrt{n}$ restate the argument above by using H^T in place of H. □

As the row sum of a Hadamard matrix must be an integer, the above result also proves that a regular Hadamard matrix of order n can only exist if n is a square.

Definition 2.23. *Let H be a Hadamard matrix of order n^2. Then H is a Bush-type Hadamard matrix if it is partitioned into n^2 square blocks of size n, all row and column sums of nondiagonal blocks are 0, and all row and column sums of diagonal blocks are n.*

Since the row and column sums of all off-diagonal blocks of a Bush-type are zero, and the row and column sums of diagonal blocks are n, the row and column sums of a Bush-type Hadamard matrix of order n^2 will be n. Thus a Bush-type Hadamard matrix is always a regular Hadamard matrix.

Example 2.24. *The following is a (regular) Bush-type Hadamard matrix of order 16.*

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

In Section 6.1 we will show how to use Latin squares, which are objects described in Chapter 4, to construct Bush-type Hadamard matrices. We introduce one last special type of Hadamard matrix. We begin with a preliminary definition.

Definition 2.25. *A circulant matrix (or equivalently array) is the matrix where each row is rotated one element to the right relative to the row directly above. A circulant matrix can be written only using its first row as shown below.*

$$circ\begin{pmatrix} 1 & 2 & \cdots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & 1 & \cdots & n-1 \\ \vdots & \vdots & \ddots & \vdots \\ 2 & 3 & \cdots & 1 \end{pmatrix}.$$

Furthermore, we define the back-circulant matrix as the matrix where each row is rotated one element to the left relative to the row directly above and is denoted as bcirc(r) where r is the first row of a matrix.

This definition can also be generalized. Suppose that the entries $1, 2, \ldots, n$ are $k \times k$ matrices. In this case, the resulting $nk \times nk$ matrix is made up of $k \times k$ blocks. Such a matrix is said to be *block-circulant* or *block-back-circulant.*

Definition 2.26. *A circulant Hadamard matrix is a Hadamard matrix such that each row is rotated one element to the right relative to the row directly above.*

However, circulant Hadamard matrices are very rare. There exist only two known examples of circulant Hadamard matrices, which are given below.

$$\text{circ}(1) = (1),\ \text{circ}\begin{pmatrix} - & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \end{pmatrix}.$$

Apart from the circulant Hadamard matrices of order 1 and 4, it is believed that no other circulant Hadamard matrices exist. In [20], Bernhard Schmidt verified that no circulant Hadamard matrices exist for all but 26 orders less than 10^4.

Although there are very few circulant Hadamard matrices, circulant matrices are highly useful and will be referred back to in upcoming sections.

Chapter 3

Generalizations

Due to their remarkable properties, Hadamard matrices have led researchers to generalize away from the stringent requirements placed on the entries which can appear within these matrices. In particular, retaining their orthogonality property, Hadamard matrices can be generalized to include the 0 entry, leading to weighing matrices. Alternatively, they can be generalized to include the complex roots of unity, leading to Butson Hadamard matrices. Furthermore, these matrices can even be generalized to include both complex roots of unity and the 0 entry, which leads to complex weighing matrices. Throughout this chapter, we will focus our discussion on the three mentioned generalizations. However, Hadamard matrices can be generalized to other types of orthogonal designs. For further insights on the various possible types of orthogonal designs, we refer the reader to [22].

3.1 Weighing Matrices

The applications of weighing matrices range from error corrections to experimental design and coding theory. The name weighing matrix comes from their use in optimally measuring individual weights of multiple objects. For example, if you consider a balance scale used for weighing objects, we can add weight to the measurement of an object by adding a weight on one side, and subtract weight by adding a weight on the opposite side. Consider each row of a weighing matrix as representing a specific

measurement, and each column as representing a specific predetermined reference weight. Adding a weight on one side will correspond to a 1 in the corresponding column of the matrix while adding a weight on the opposite side will correspond to a -1 in the corresponding column. Not adding a specific weight will correspond to a 0. Thus, the ij-th entry is 1 if the j-th reference weight was placed on the opposite side of the object in the i-th trial, -1 if the j-th weight was placed on the same side as the object in the i-th trial, and 0 if the j-th weight was not used in the i-th trial. Doing this with smaller and smaller weights each time in turn reduces the statistical variance of the measurement. In summary, weighing matrices are highly versatile mathematical objects with many uses. We now state a formal definition.

Definition 3.1. *A weighing matrix of order n and weight k, denoted $W(n,k)$ is an $n \times n$ square matrix W with entries in $\{0, 1, -1\}$, such that $WW^T = kI_n$.*

From the definition of a weighing matrix, we know that rows of a $W(n,k)$ will be pairwise orthogonal. If W is a $W(n,k)$ then from straightforward matrix multiplication we can verify the following properties hold:

- $W^T W = kI_n$,
- $W^{-1} = k^{-1}W^T$,
- There are k non-zero entries in every row and column.

As mentioned, weighing matrices are also a generalization of Hadamard matrices. If W is a $W(n,n)$ (i.e., $k = n$), then $WW^T = nI_n$, and so W is a Hadamard matrix.

Another special case of weighing matrices is when $k = n - 1$. A weighing matrix $W(n, n-1)$ is called a *conference matrix*.

Example 3.2. *Consider the matrices*

$$W_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{pmatrix}, \; W_2 = \begin{pmatrix} - & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & - & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & - & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & - & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & - & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & - & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & - \end{pmatrix}.$$

W_1 is a symmetric $W(6,5)$ and W_2 is a circulant $W(7,4)$. Since the weight of W_1 is one less the order, W_1 is a conference matrix.

3.1.1 Existence

Naturally, when learning about a new object questions relating to the object's existence often arise. To help answer this question, we will now show some simple non-existence conditions for weighing matrices. The following proposition and its proof are found in [22].

Proposition 3.3. *Suppose n is odd. If there exists a $W(n,k)$, then*

1. *k is a square*
2. *$n - 1 \leq (n-k)^2 - (n-k)$*

Proof. Suppose there exists a $W(n,k)$. Part 1 follows by computing $\det(W)$. Notice that

$$\det(W)^2 = \det(WW^T) = \det(kI_n) = k^n.$$

Hence, $\det(W) = k^{n/2}$ and as n is odd, it follows that k must be a square.
To prove Part 2, square all the entries of W, and let A be the resulting $(0,1)$-matrix. The matrix A will have k ones in every row and column. Then $AJ_n = A^T J_n = kJ_n$

and so $AA^TJ_n = kA^TJ_n = k^2J_n$. Denoting the rows of A by $r_1, r_2, \ldots, r_n$, we can see

$$\sum_{i=1}^{n} r_i \cdot r_j = k^2.$$

If we now fix a row r_j. Then we have

$$\sum_{i \neq j} r_i \cdot r_j = k^2 - k.$$

As the rows of W are pairwise orthogonal, the inner product between distinct rows of A must be even. Define $B = J - A$ to be the $(0,1)$-matrix which has $n-k$ ones in every row and column. Then as n is odd, the inner product between distinct rows of B is odd and so must be at least 1. Applying the same result as we saw for A to the matrix B we have

$$\sum_{i \neq j} r_i \cdot r_j = (n-k)^2 - (n-k).$$

Therefore

$$n - 1 \leq (n-k)^2 - (n-k)$$

as each inner product of distinct rows must be at least 1. □

Before proving our next non-existence result, we state a few preliminary lemmas. We begin by stating two well-known theorems from number theory. The first is an elementary result of Fermat.

Lemma 3.4. *If $n \in \mathbb{Z}^+$, then n is the sum of two squares if and only if every prime of the form $4k+3$ in the prime factorization of n appears as an even power.*

Lemma 3.5. *For any non-negative integer n, there exist integers $k_1, k_2, k_3, k_4 \in \mathbb{Z}^+$ such that $n = k_1^2 + k_2^2 + k_3^2 + k_4^2$.*

Lemma 3.6. *Define $n = k_1^2 + k_2^2 + k_3^2 + k_4^2$ and let*

$$C = \begin{pmatrix} k_1 & k_2 & k_3 & k_4 \\ -k_2 & k_1 & -k_4 & k_3 \\ -k_3 & k_4 & k_1 & -k_2 \\ -k_4 & -k_3 & k_2 & k_1 \end{pmatrix}.$$

Then $C^{-1} = \frac{1}{n}C^T$.

Proof. Simple matrix multiplication shows that

$$\begin{aligned} C\big(\frac{1}{n}C^T\big) &= \frac{1}{n}\begin{pmatrix} k_1 & k_2 & k_3 & k_4 \\ -k_2 & k_1 & -k_4 & k_3 \\ -k_3 & k_4 & k_1 & -k_2 \\ -k_4 & -k_3 & k_2 & k_1 \end{pmatrix}\begin{pmatrix} k_1 & -k_2 & -k_3 & -k_4 \\ k_2 & k_1 & k_4 & k_3 \\ k_3 & -k_4 & k_1 & k_2 \\ k_4 & k_3 & -k_2 & k_1 \end{pmatrix} \\ &= \frac{1}{n}\begin{pmatrix} n & 0 & 0 & 0 \\ 0 & n & 0 & 0 \\ 0 & 0 & n & 0 \\ 0 & 0 & 0 & n \end{pmatrix} \\ &= I_4. \end{aligned}$$

□

We now prove the final non-existence result for weighing matrices included in this section. For more existence and non-existence results see [22].

Proposition 3.7. *Let* $n \equiv 2 \pmod 4$. *A* $W(n,k)$ *exists only if* k *is the sum of two squares.*

Proof. Let $W = (w_{ij})$ be a $W(n,k)$. For the case of $n = 2$, a $W(2,k)$ exists for both $k = 1 = 1^2 + 0^2$ and $k = 2 = 1^2 + 1^2$. Namely, I_2 is a $W(2,1)$ and the Hadamard matrix H_2 is a $W(2,2)$. Thus we can assume $n = 4m + 2$ for some positive integer m. For $1 \leq i \leq v$ define

$$L_j = \sum_{i=1}^{n} m_{ij}x_i,$$

for some indeterminates $x_1, \ldots, x_n$. Then careful algebraic simplifications give us

$$L_j^2 = \left(\sum_{i=1}^{n} m_{ij}x_i\right)^2 = \sum_{i=1}^{n}\sum_{h=1}^{n} m_{ij}m_{hj}x_ix_h$$

and so

$$\begin{aligned}\sum_{j=1}^{n} L_j^2 &= \sum_{j=1}^{n}\sum_{i=1}^{n}\sum_{h=1}^{n} m_{ij}m_{hj}x_ix_h \\ &= \sum_{i=1}^{n}\sum_{h=1}^{n}\left(\sum_{j=1}^{n} m_{ij}m_{hj}\right)x_ix_h \\ &= \sum_{i=1}^{n}\sum_{h=1}^{n} kx_ix_h \\ &= k\left(\sum_{j=1}^{n} x_i\right)^2.\end{aligned}$$

We now transform the variables $x_1, \ldots, x_n$ into new indeterminates $y_1, \ldots, y_n$, which will be made up of linear combinations of $x_i's$. First, let $k = k_1^2 + k_2^2 + k_3^2 + k_4^2$ for $k_1, k_2, k_3, k_4 \in \mathbb{Z}^+$ and let C be the matrix defined in Lemma 3.6. For $1 \leq h \leq m$ let

$$(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h}) = (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C.$$

Additionally let $y_{n-1} = x_{n-1}$ and $y_{n-2} = x_{n-2}$. From Lemma 3.6 we have $CC^T = nI_4$ and so for $1 \leq h \leq m$ it follows that

$$\begin{aligned}&y_{4h-3}^2 + y_{4h-2}^2 + y_{4h-1}^2 + y_{4h}^2 \\ &= (y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h})(y_{4h-3}, y_{4h-2}, y_{4h-1}, y_{4h})^T \\ &= (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C((x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})C)^T \\ &= (x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})CC^T(x_{4h-3}, x_{4h-2}, x_{4h-1}, x_{4h})^T \\ &= k(x_{4h-3}^2 + x_{4h-2}^2 + x_{4h-1}^2 + x_{4h}^2).\end{aligned}$$

Thus

$$\sum_{j=1}^{n} L_j^2 = ky_n^2 + ky_{n-1}^2 + \sum_{i=1}^{n-2} y_i^2.$$

Recall that each L_i is defined as an integral sum of x_i's. As $C^{-1} = C^T$ we can express each x_i as some rational combination of the y_i's. First,

$$L_1 = \sum_{i=1}^{n} e_i y_i$$

for some rational e_i. If $e_1 \neq 1$ let $y_1 = L_1$, and if $e_1 = 1$, then let $y_1 = -L_1$. By doing this, we have expressed y_1 as a rational linear combination of $y_2, \ldots, y_n$, such that $L_1^2 = y_1^2$. Thus

$$\sum_{j=2}^{n} L_j^2 = ky_n^2 + ky_{n-1}^2 + \sum_{i=2}^{n-2} y_i^2.$$

Continuing this process, we can eliminate the variables $y_2, \ldots, y_{n-1}$, which simplifies to

$$L_{n-1}^2 + L_n^2 = ky_n^2 + ky_{n-1}^2.$$

If we let $y_n = 1$ and $y_{n-1} = 0$, we can see that $k = L_{n-1}^2 + L_n^2$ is a sum of two rational squares. Then without loss of generality, assume $k = (a/c)^2 + (b/c)^2$ for $a, b, c \in \mathbb{Z}$ where each fraction is reduced. Thus, $kc^2 = a^2 + b^2$ and since c shares no prime factors with a or b, every prime of the form $4l + 3$ will appear as an even power. Therefore, by Lemma 3.4, k is the sum of two squares as desired. □

In the next section, we showcase a construction for conference matrices and relate conference matrices to Hadamard matrices

3.1.2 Paley's Construction

In Chapter 2, we showcased Sylvester's construction for Hadamard matrices of order 2^n, $n \in \mathbb{N}$. Sylvester's construction was the first infinite class of Hadamard matrices. However, this construction did not deal with Hadamard matrices whose orders were not powers of two. This left open questions relating to the existence of Hadamard matrices of order 12 and 20. As we have seen, in his 1893 paper, Hadamard extended Sylvester's construction and presented Hadamard matrices of order 12 and 20. However, these Hadamard matrices were not claimed to be found by using any form of a replicable construction. It would not be until 1933, that Paley would discover a connection between Field theory and Hadamard matrices, which would culminate in a general construction for Hadamard matrices, including those of order 12 and 20. In this section, we will work towards demonstrating Paley's construction for Hadamard

matrices of order $2q+2$ whenever $q \equiv 1 \pmod 4$ and $q+1$ whenever $q \equiv -1 \pmod 4$ for a prime power q. We begin with a necessary definition.

Definition 3.8. *Suppose q is an odd prime power. Let $\mathbb{F}_q$ denote the finite field of order q, and suppose $x \in \mathbb{F}_q \setminus \{0\}$. We say that x is a quadrtatic residue if it is a square in $\mathbb{F}_q$, and x is a quadratic non-residue if it is not a square in $\mathbb{F}_q$. The element 0 is neither a quadratic residue nor a quadratic non-residue. Finally, define $QR(q)$ to be the set containing the quadratic residues of $\mathbb{F}_q$ and $QN(q)$ to be the set containing quadratic non-residues of $\mathbb{F}_q$.*

In other words, $x \in \mathbb{F}_q \setminus \{0\}$ is a quadratic residue if $x = y^2$ for some $y \in \mathbb{F}_q$, and a quadratic non-residue of no such y exists. The next proposition unveils the cardinalities of $QR(q)$ and $QN(q)$.

Proposition 3.9. *Let q be an odd prime power. Then there are $(q-1)/2$ quadratic residues and $(q-1)/2$ quadratic non-residues in $\mathbb{F}_q$ (i.e., $|QR(q)| = |QN(q)| = (q-1)/2$).*

Proof. First, notice that $(x)^2 = (-x)^2$ for any $x \in \mathbb{F}_q$. Using this fact, note that the map $\phi : \mathbb{F}_q \setminus \{0\} \mapsto \mathbb{F}_q \setminus \{0\}$ defined by $\phi(x) = x^2$ for $x \in \mathbb{F}_q \setminus \{0\}$ is a two-to-one mapping. Thus, ϕ is a group homomorphism and $|\ker \phi| = 2$. By the first isomorphism theorem we have

$$\phi(\mathbb{F}_q \setminus \{0\}) \cong (\mathbb{F}_q \setminus \{0\})/\ker \phi.$$

Then as $\phi(\mathbb{F}_q \setminus \{0\})$ is a subgroup of $\mathbb{F}_q \setminus \{0\}$ we can apply Lagrange's theorem to obtain

$$|\phi(\mathbb{F}_q \setminus \{0\})| = \frac{|\mathbb{F}_q \setminus \{0\}}{|\ker \phi|} = \frac{q-1}{2}.$$

As $\phi(\mathbb{F}_q \setminus \{0\}) = QR(q)$, we have shown that $|QR(q)| = (q-1)/2$. Since there are $q-1$ elements in $\mathbb{F}_q \setminus \{0\}$, and every element is either a quadratic residue or a quadratic non-residue, it follows that $|QN(q)| = (q-1)/2$. □

Next, we introduce a new characterization for quadratic residues and non-residues. Both during and in the sections following this characterization, we will make use of the well-known fact from field theory that establishes the fact that multiplicative group $(\mathbb{F}_q \setminus \{0\}, \times)$ is a cyclic group. A generator of this group is said to be a *primitive element* of the field $\mathbb{F}_q$.

Proposition 3.10. *Let q be an odd prime power and let $\omega \in \mathbb{F}_q$ be a primitive element of $\mathbb{F}_q$. Then the set*

$$S = \left\{ \omega^{2i} : 0 \leq i \leq \frac{q-3}{2} \right\}$$

is the set of all quadratic residues in $\mathbb{F}_q$ (i.e., $QR(q) = S$).

Proof. First, notice that $|S| = (q-1)/2$. Next, for any $x_i = \omega^{2i} \in S$ we have $x_i = (\omega^i)^2 \in QR(q)$. Thus $S \subseteq QR(q)$, and $|S| = |QR(q)|$. It follows that $QR(q) = S$ as desired. □

Definition 3.11. *Let q be an odd prime power, and let $\mathbb{F}_q$ denote the finite field of order q. The quadratic character is a function $\chi_q : \mathbb{F}_q \to \{-1, 0, 1\}$ defined by*

$$\chi_q(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \in QR(q) \\ -1 & \text{if } x \in QN(q) \end{cases}$$

for $x \in \mathbb{F}_q$.

The following lemmas show two useful properties of the quadratic character.

Lemma 3.12. *Let q be an odd prime power. Then*

$$\sum_{x \in \mathbb{F}_q} \chi_q(x) = 0.$$

Proof. Define the set

$$R = \{x^2 : x \in \mathbb{F}_q, x \neq 0\}.$$

We can prove that R is a multiplicative subgroup of $\mathbb{F}_q$ having index 2. As R is the set of all quadratic residues of $\mathbb{F}_q \setminus \{0\}$, the coset of R, say N, will be the set of all

quadratic non-residues of $\mathbb{F}_q \setminus \{0\}$. As $\chi_q(0) = 0$ and R and its coset N have the same cardinality, it follows that

$$\sum_{x \in \mathbb{F}_q} \chi_q(x) = |R| - |N| + \chi_q(0) = 0.$$

□

Lemma 3.13. *Let q be an odd prime power. If $y \neq 0$ then*

$$\sum_{x \in \mathbb{F}_q} \chi_q(x)\chi_q(x+y) = -1.$$

Proof. Since $\chi_q(0) = 0$, then $\chi_q(0)\chi_q(0+y) = 0$. If $x \neq 0$, then using the fact that $\mathbb{F}_q$ is a field, there exists a unique $z \in \mathbb{F}_q$ such that $x + y = xz$. Note that since $y \neq 0$ it is easily seen that $z \neq 1$. As x takes on all values in $\mathbb{F}_q$ except for 0, then z will take on all values in $\mathbb{F}_q$ except for the value 1. Thus

$$\begin{aligned}
\sum_{x \in \mathbb{F}_q} \chi_q(x)\chi_q(x+y) &= \sum_{x \in \mathbb{F}_q} \chi_q(x)^2\chi_q(z) \\
&= \sum_{z \in \mathbb{F}_q \setminus \{1\}} \chi_q(z) \\
&= 0 - \chi_q(1) \\
&= -1
\end{aligned}$$

since $\sum_{z \in \mathbb{F}_q} \chi_q(z) = 0$. □

We now define a matrix construction first described in 1933 by English mathematician Raymond Paley.

Definition 3.14. *Working in $\mathbb{F}_q$, we define the Paley matrix $P = [p_{ij}]$ to be the $q \times q$ matrix in which the rows and columns are indexed by $\mathbb{F}_q$, where the ij-th entry of P is given by $p_{ij} = \chi_q(i-j)$ for $i, j \in \mathbb{F}_q$.*

As $\chi_q(i-j) = \chi_q(-1)\chi_q(j-i)$, P will be symmetric if $q \equiv 1 \pmod 4$ as this implies $\chi_q(-1) = 1$. Similarly, if $q \equiv -1 \pmod 4$, $\chi_q(-1) = -1$ and so P will be skew-symmetric. The following is an immediate consequence of the previous two lemmas.

Lemma 3.15. *Let P be a Paley matrix. Then*

- $PJ_q = JP_q = 0$ *(by Lemma 3.12),*
- $PP^T = qI_q - J_q$ *(by Lemma 3.13).*

We now present an important construction of conference matrices used by Paley to construct Hadamard matrices.

Theorem 3.16. *Let q be an odd prime power. If $q \equiv 1 \pmod 4$, then there exists a symmetric conference matrix of order $q+1$. If $q \equiv -1 \pmod 4$, then there exists a skew-symmetric conference matrix of order $q+1$.*

Proof. Case 1: If $q \equiv 1 \pmod 4$, define

$$W_1 = \begin{pmatrix} 0 & 1_q^T \\ 1_q & P \end{pmatrix}.$$

Case 2: If $q \equiv -1 \pmod 4$, define

$$W_2 = \begin{pmatrix} 0 & 1_q^T \\ -1_q & P \end{pmatrix}.$$

Using Lemma 3.15, it we can verify that W_1 is symmetric and $W_1 W_1^T = qI_{q+1}$. Similarly W_2 is skew-symmetric and $W_2 W_2^T = qI_{q+1}$. □

Theorem 3.17. *Let W be a symmetric conference matrix of order n. Then the matrix*

$$H = \begin{pmatrix} W + I_n & W - I_n \\ W - I_n & -W - I_n \end{pmatrix}$$

is a Hadamard matrix of order $2n$.

Proof. As C is symmetric, H will also be symmetric. To simplify the multiplication of HH^T we make some simplifications. First, observe that

$$\begin{aligned} (W + I_n)^2 + (W - I_n)^2 &= 2W^2 + 2I_n^2 \\ &= 2(n-1)I_n + 2I_n \\ &= 2nI_n \end{aligned}$$

Similarly, since $(W + I_n)^2 = (-W - I_n)^2$ we have $(-W - I_n)^2 + (W - I_n)^2 = 2nI_n$. Next, observe that

$$(W + I_n)(W - I_n) + (W - I_n)(-W - I_n) = W^2 - I_n^2 - W^2 + I_n^2 = 0$$

and

$$(W - I_n)(W + I_n) + (-W - I_n)(W - I_n) = W^2 - I_n^2 - W^2 + I_n^2 = 0.$$

Using these identities we have

$$\begin{aligned} HH^T &= \begin{pmatrix} W + I_n & W - I_n \\ W - I_n & -W - I_n \end{pmatrix} \begin{pmatrix} W + I_n & W - I_n \\ W - I_n & -W - I_n \end{pmatrix} \\ &= \begin{pmatrix} (2n)I_n & 0 \\ 0 & (2n)I_n \end{pmatrix} \\ &= 2nI_{2n}, \end{aligned}$$

which completes the proof. □

Example 3.18. *The following is a* $W(6, 5)$ *(i.e., a conference matrix of order* 6*).*

$$W_1 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & - & - & 1 \\ 1 & 1 & 0 & 1 & - & - \\ 1 & - & 1 & 0 & 1 & - \\ 1 & - & - & 1 & 0 & 1 \\ 1 & 1 & - & - & 1 & 0 \end{pmatrix}.$$

Using Theorem 3.17 we form the following Hadamard matrix of order 12.

$$\begin{pmatrix} W_1 + I_6 & W_1 - I_6 \\ W_1 - I_6 & -W_1 - I_6 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - \\ 1 & - & 1 & 1 & 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - \\ - & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & - & - & 1 & 1 & - \\ 1 & 1 & - & 1 & - & - & - & - & - & - & 1 & 1 \\ 1 & - & 1 & - & 1 & - & - & 1 & - & - & - & 1 \\ 1 & - & - & 1 & - & 1 & - & 1 & 1 & - & - & - \\ 1 & 1 & - & - & 1 & - & - & - & 1 & 1 & - & - \end{pmatrix}.$$

It is also possible to use a skew-symmetric conference matrix of order 12 *constructed using Theorem 3.16 to construct a Hadamard matrix of order* 12*. Using the following skew-symmetric conference matrix of order* 12

$$W_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ - & 0 & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 \\ - & 1 & 0 & - & 1 & - & - & - & 1 & 1 & 1 & - \\ - & - & 1 & 0 & - & 1 & - & - & - & 1 & 1 & 1 \\ - & 1 & - & 1 & 0 & - & 1 & - & - & - & 1 & 1 \\ - & 1 & 1 & - & 1 & 0 & - & 1 & - & - & - & 1 \\ - & 1 & 1 & 1 & - & 1 & 0 & - & 1 & - & - & - \\ - & - & 1 & 1 & 1 & - & 1 & 0 & - & 1 & - & - \\ - & - & - & 1 & 1 & 1 & - & 1 & 0 & - & 1 & - \\ - & - & - & - & 1 & 1 & 1 & - & 1 & 0 & - & 1 \\ - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 0 & - \\ - & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 0 \end{pmatrix},$$

we can construct a skew-symmetric Hadamard matrix of order 12*.*

$$W_2 + I_{12} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ - & 1 & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 \\ - & 1 & 1 & - & 1 & - & - & - & 1 & 1 & 1 & - \\ - & - & 1 & 1 & - & 1 & - & - & - & 1 & 1 & 1 \\ - & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 & 1 \\ - & 1 & 1 & - & 1 & 1 & - & 1 & - & - & - & 1 \\ - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - & - & - \\ - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - & - \\ - & - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 & - \\ - & - & - & - & 1 & 1 & 1 & - & 1 & 1 & - & 1 \\ - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 1 & - \\ - & - & 1 & - & - & - & 1 & 1 & 1 & - & 1 & 1 \end{pmatrix}.$$

The following corollary generalizes the constructions seen in the previous example.

Corollary 3.19. *Let* q *be a prime power. If* $q \equiv 1 \pmod 4$ *then there is a Hadamard matrix of order* $2q+2$*. If* $q \equiv -1 \pmod 4$*, then there is a skew-symmetric Hadamard matrix of order* $q+1$*.*

Proof. If $q \equiv 1 \pmod 4$ then there exists a symmetric conference matrix of order $q+1$, say W_1. Then by Theorem 3.17, there exists a Hadamard matrix of order $2q+2$

given by

$$H = \begin{pmatrix} W_1 + I_n & W_1 - I_n \\ W_1 - I_n & -W_1 - I_n \end{pmatrix}.$$

If $q \equiv -1 \pmod 4$ then there exists a skew-symmetric conference matrix of order $q+1$, say W_2. We know $W_2 W_2^T = qI_{q+1}$. As W_2 is skew-symmetric, it follows that $W_2 + I_{q+1}$ is the desired Hadamard matrix of order $q+1$. □

Applying Theorem 2.16 to Corollary 3.19 presents the following result.

Corollary 3.20. *Let q be a prime power and let n be the order of a Hadamard matrix. If $q \equiv 1 \pmod 4$ then there is a Hadamard matrix of order $2n(q+1)$. If $q \equiv -1 \pmod 4$, then there is a Hadamard matrix of order $n(q+1)$.*

Remark. Another way to state Paley's result found in Theorem 3.17 is by using Kronecker products. For a prime power $q \equiv 1 \pmod 4$, a straightforward calculation shows that if W_1 is a conference matrix of order $q+1$

$$H = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes W_1 + \begin{pmatrix} 1 & - \\ - & - \end{pmatrix} \otimes I_{q+1}$$

is the same Hadamard matrix of order $2q+2$. However, it is possible to extend this result even further.

Lemma 3.21. *Let W be a matrix of order m such that $W^T = \sigma W$, $\sigma = \pm 1$ and $WW^T = (m-1)I_m$. Let A and B be matrices of order n such that $AA^T = BB^T = nI_n$ and $AB^T = -\sigma BA^T$. Define $K = A \otimes I_m + B \otimes W$. Then $KK^T = nmI_{nm}$.*

Proof. Notice that $\sigma^2 = 1$. Straight-forward computation shows that

$$\begin{aligned}
KK^T &= (A \otimes I_m + B \otimes W)(A \otimes I_m + B \otimes W)^T \\
&= (A \otimes I_m + B \otimes W)(A^T \otimes I_m + B^T \otimes W^T) \\
&= (AA^T \otimes I_m) + (AB^T \otimes W^T) + (BA^T \otimes W) + (BB^T \otimes WW^T) \\
&= (nI_n \otimes I_m) + (-\sigma BA^T \otimes \sigma W) + (BA^T \otimes W) + (nI_n \otimes (m-1)I_m) \\
&= (nI_n \otimes I_m) - \sigma^2(BA^T \otimes W) + (BA^T \otimes W) + (nI_n \otimes (m-1)I_m) \\
&= nI_{nm} + n(m-1)I_{nm} \\
&= nmI_{nm}.
\end{aligned}$$

□

Corollary 3.22. *If q be a prime power $q \equiv 1 \pmod 4$, and H is a Hadamard matrix of order n, then there exists a Hadamard matrix of order $n(q+1)$.*

Proof. Let W be a symmetric conference matrix of order $q+1$ coming from Theorem 3.16. Define

$$M = I_{n/2} \otimes \begin{pmatrix} 0 & 1 \\ - & 0 \end{pmatrix},$$

and let $B = MH$. Notice that $M^T = -M$ and $MM^T = I_n$. Then, note that

$$BB^T = (MH)(MH)^T = MHH^TM^T = nMM^T = nI_n.$$

Next, observe that

$$HB^T = H(MH)^T = HH^TM^T = -nM.$$

Since $W = \sigma W^T$, with $\sigma = 1$ the matrices W, H and B satisfy the required conditions of Lemma 3.21. Therefore $K = H \otimes I_{q+1} + B \otimes W$ is the desired Hadamard matrix of order $n(q+1)$. □

3.2 Complex Case

Throughout this section, we will use $*$ to denote the conjugate transpose of a matrix. Refer to the list of symbols and Section 1.3 for further information on notation. To begin our discussion of this section, we define the following notation.

Definition 3.23. *Let $\xi_q = e^{\frac{2\pi i}{q}}$ be a primitive complex q-th root of unity. Then define the set $\langle \xi_q \rangle = \{\xi_q^j : 0 \leq j \leq q-1\}$.*

We can now extend the definition of weighing matrices by giving a general definition of weighing matrices over $\langle \xi_q \rangle$.

Definition 3.24. *A complex weighing matrix of order n and weight k is an $n \times n$ square matrix W with entries in $\Omega_q = \{0\} \cup \langle \xi_q \rangle$ such that $WW^* = kI_n$. We denote a complex weighing matrix with the given parameters by $CW(n, k; q)$.*

Example 3.25. *Let ξ be a primitive third root of unity. Denoting $\xi^3 = 1$, the following is a block-back-circulant $CW(15, 9; 3)$.*

$$\left[\begin{array}{ccccccccccccccc}
0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
\xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
\xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & \xi^2 & \xi & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi & \xi^2 \\
\xi^2 & \xi & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \xi & \xi^2 & 1 \\
\xi & 1 & \xi^2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & 1 & \xi \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2
\end{array}\right].$$

As for the case of real weighing matrices, we know that the rows of a $CW(n, k; q)$ will be pairwise orthogonal. It is straightforward to verify that such a matrix will have k non-zero entries in every row and column. In the special case where $k = n$, a $CW(n, n; k)$ provides another natural generalization of Hadamard matrices. This

generalization is named after A.T. Butson for his research developments in generalized Hadamard matrices [4].

Definition 3.26. *A Butson Hadamard matrix of order n is an $n \times n$ square matrix H, with entries in $\langle \xi_q \rangle$ such that $HH^* = nI_n$. Such a matrix is denoted $BH(n;q)$.*

Note a BH$(n;2)$ is just a real Hadamard matrix of order n. Naturally, a $BH(n;q)$ is said to be *normalized* if the first entry in every row and column is 1.

Example 3.27. *As before, let ξ be a primitive third root of unity and denote $\xi^3 = 1$, the following is a block-circulant $BH(9;3)$.*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 \\ 1 & 1 & 1 & \xi & 1 & \xi^2 & \xi^2 & 1 & \xi \\ 1 & 1 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 \\ 1 & \xi & \xi^2 & 1 & 1 & 1 & 1 & \xi^2 & \xi \\ \xi^2 & 1 & \xi & 1 & 1 & 1 & \xi & 1 & \xi^2 \\ \xi & \xi^2 & 1 & 1 & 1 & 1 & \xi^2 & \xi & 1 \\ 1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 \\ \xi & 1 & \xi^2 & \xi^2 & 1 & \xi & 1 & 1 & 1 \\ \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Example 3.28. *Let ζ be a primitive 9th root of unity and denote $\zeta^9 = 1$. The following is a $BH(9;9)$.*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 & \zeta^7 & \zeta^8 \\ 1 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^8 & \zeta & \zeta^3 & \zeta^5 & \zeta^7 \\ 1 & \zeta^3 & \zeta^6 & 1 & \zeta^3 & \zeta^6 & 1 & \zeta^3 & \zeta^6 \\ 1 & \zeta^4 & \zeta^8 & \zeta^3 & \zeta^7 & \zeta^2 & \zeta^6 & \zeta & \zeta^5 \\ 1 & \zeta^5 & \zeta & \zeta^6 & \zeta^2 & \zeta^7 & \zeta^3 & \zeta^8 & \zeta^4 \\ 1 & \zeta^6 & \zeta^3 & 1 & \zeta^6 & \zeta^3 & 1 & \zeta^6 & \zeta^3 \\ 1 & \zeta^7 & \zeta^5 & \zeta^3 & \zeta & \zeta^8 & \zeta^6 & \zeta^4 & \zeta^2 \\ 1 & \zeta^8 & \zeta^7 & \zeta^6 & \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{bmatrix}$$

The construction in Example 3.28 can be extended to every positive integer n by using the Discrete Fourier Transform. We showcase the result in the following proposition, but first, we define the function

$$\delta_{x,y} = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

Proposition 3.29. *There exists a $BH(n;n)$ for any positive integer n.*

Proof. Let ξ be a primitive n-th root of unity. Define $H = (h_{ij})$ to be the $n \times n$ matrix whose rows and columns are indexed by $0, 1, \ldots, n-1$, given by $h_{ij} = \xi^{(i \cdot j)}$. The matrix is given below.

$$H = \begin{pmatrix} \xi^{0\cdot 0} & \xi^{0\cdot 1} & \cdots & \xi^{0\cdot(n-1)} \\ \xi^{1\cdot 0} & \xi^{1\cdot 1} & \cdots & \xi^{1\cdot(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \xi^{(n-1)\cdot 0} & \xi^{(n-1)\cdot 1} & \cdots & \xi^{(n-1)\cdot(n-1)} \end{pmatrix}.$$

We now show that H is a $BH(n; n)$. Let $r_0, r_1, \ldots, r_{n-1}$ be the rows of H. It suffices to show that for any $0 \leq i, j \leq n-1$

$$r_i \cdot r_j^* = n\delta_{i,j}.$$

Using the definition of h_{ij}, observe that

$$\begin{aligned} r_i \cdot r_j^* &= \sum_{k=0}^{n-1} h_{ik} \cdot \overline{h_{jk}} \\ &= \sum_{k=0}^{n-1} \xi^{i\cdot k} \overline{\xi^{j\cdot k}} \\ &= \sum_{k=0}^{n-1} \xi^{i\cdot k} \xi^{j\cdot(n-k)} \\ &= \sum_{k=0}^{n-1} \xi^{k\cdot(i-j)}. \end{aligned}$$

Clearly, if $i = j$ then we have

$$\sum_{k=0}^{n-1} \xi^{k\cdot 0} = n.$$

In the case that $i \neq j$ let $m = i - j$. To see that

$$\sum_{k=0}^{n-1} \xi^{km} = 0$$

note that if m and n are coprime, the summation is adding up all the n-th roots of unity. If $\gcd(m, n) = p > 1$, then let $q = n/p$. The above sum is then equivalent to adding up all the q-th roots of unity p times. Therefore

$$r_i \cdot r_j^* = \sum_{k=0}^{n-1} \xi^{k\cdot(i-j)} = n\delta_{i,j}$$

as desired. □

In general, if we restrict ourselves to the fourth root of unity, a $CW(n, k; 4)$ is called a *quaternary weighing matrix*, and similarly a $BH(n, 4)$ is called a *quaternary complex Hadamard matrix*.

Chapter 4

Latin Squares

In this section, we showcase a new combinatorial object which will play an important role in Chapter 6. We begin by defining Latin squares.

Definition 4.1. *A Latin square of order n is an $n \times n$ array L, with entries from a set X where $|X| = n$, and every entry of L contains an element of X, such that every row and every column of L is a permutation of X.*

It is not hard to show that there exists a Latin square of order $n \geq 1$. Taking the first row to be

$$\begin{bmatrix} 1 & 2 & \cdots & n \end{bmatrix}$$

we can form an $n \times n$ circulant array, where each row is rotated one element to the right relative to the row directly above, which is easily verified to be a Latin square. Similarly, we can form a back-circulant array, where each row is rotated one element to the left relative to the row directly above, also resulting in a Latin square. For the remainder of this section, unless explicitly stated otherwise we will take the symbol set $X = \{1, 2, \ldots, n\}$.

Example 4.2. *The following are Latin squares of order n for $1 \leq n \leq 4$:*

$$L_1 = \begin{bmatrix} 1 \end{bmatrix}, \; L_2 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \; L_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \; L_4 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix}.$$

We now define the notion of equivalence in relation to Latin squares. Performing any combination of the following operations transforms one Latin square to another equivalent (or isomorphic) Latin square.

- Swapping any two rows.
- Swapping any two columns.
- Changing all the rows to columns and columns to rows (i.e., taking the transpose).
- Permuting the symbols in X.

Next, we expand the possible functionality of Latin squares by delving into the notion of orthogonality.

4.1 Orthogonal Latin Squares

In 1782, Leonhard Euler proposed the problem of arranging 36 military officers into a 6×6 square array. Each of the officers had to come from one of 6 different regiments and must hold one of 6 possible ranks. Placing the condition that no two officers from the same regiment hold the same rank, Euler attempted to ask the question of whether it was possible to organize the officers into a square such that in each row and column, there is exactly one officer from each regiment and one precisely one officer of each rank. For the first step, Euler arranged the regiments, by setting aside 6 positions in the square to be filled by officers from that regiment. He would then try to assign ranks to the officers in these 6 positions. In other words, Euler was trying to find two Latin squares of order 6, such that when superimposed, there would be precisely one officer from each regiment who holds each of the 6 possible ranks. In other words, the superimposition of the two Latin squares would contain every possible pair of regiment and rank. Using Latin characters to denote regiment, Euler called the first square a "Latin square", and the square containing both rank and regiment

was called a "Graeco-Latin square" since he used Greek letters to denote rank. In other words, the square containing rank, when superimposed on the Latin square containing regiments should form the desired "Graeco-Latin square" which contains one officer from each regiment who holds each of the 6 possible ranks. However, Euler was unable to find such a square. On the other hand, Euler was able to easily produce Graeco-Latin squares of order n for any $n \not\equiv 2 \pmod 4$. It was also not hard for Euler to see that there was no Graeco-Latin square of order 2. Thus, Euler conjectured that Graeco-Latin squares of order n do not exist for any $n \equiv 2 \pmod 4$. Equivalently, this conjecture can be stated in reference to orthogonal Latin squares, which we now define.

Definition 4.3. *Two Latin squares L_1 and L_2 of order n with entries from X and Y respectively are orthogonal if the superposition of L_1 and L_2 given by $\{(L_1(i,j), L_2(i,j)) : 1 \leq i, j \leq n\}$ contains every ordered pair in $X \times Y$.*

An equivalent definition for orthogonality states that L_1 and L_2 are orthogonal if for every $x \in X$ and $y \in Y$, there is a unique cell (i,j) such that $L_1(i,j) = x$ and $L_2(i,j) = y$. In the context of Euler's problem, Euler created the Latin square and then attempted to fill this square with the 6 possible ranks. In other words, Euler skipped the step of creating the second Latin square and instead worked exclusively with the superposition of the two squares. Euler's conjecture using the above definition states that there do not exist orthogonal Latin squares of order n for any $n \equiv 2 \pmod 4$. Although this conjecture was shown to be correct for $n = 6$, in 1959 Ernest Parker published [15], which showcased a construction for orthogonal Latin squares of order 10. Soon after, a general construction that produced pairs of orthogonal Latin squares of order $n \equiv 2 \pmod 4$, $n > 6$ was published by Raj Chandra Bose and Sharadchandra Shankar Shrikhande in [2].

Example 4.4. *There are no orthogonal Latin squares of order 2. Consider L_3, which was the Latin square of order 3 shown in Example 4.2. As shown below, the Latin*

square L_3' together with L_3 form a pair of orthogonal Latin squares of order 3.

$$L_3 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \; L_3' = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

The superposition of L_3 and L_3' is as follows.

$$\begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (3,2) & (1,3) & (2,1) \\ (2,3) & (3,1) & (1,2) \end{bmatrix}.$$

However, it is possible to show that there does not exist a Latin square orthogonal to L_4, which was the Latin square of order 4 from Example 4.2. Nevertheless, orthogonal Latin squares of order 4 exist, as shown below.

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}.$$

We give one more example which will be utilized in an upcoming construction.

Example 4.5. *The following are orthogonal Latin squares of order 8.*

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 8 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \\ 5 & 6 & 7 & 9 & 1 & 2 & 3 & 4 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{bmatrix}.$$

4.1.1 Constructions

Orthogonal Latin squares of order 1 exist, however, these objects are unsurprisingly uninteresting. We now examine several constructions for orthogonal Latin squares for larger orders.

Theorem 4.6. *Let $n > 1$ be odd. Then there exists orthogonal Latin squares of order n.*

Proof. Let $X = \mathbb{Z}_n$ and define

$$L_1(i, j) = (i + j) \pmod{n},$$
$$L_2(i, j) = (i - j) \pmod{n}.$$

Holding i constant we can see each row of L_1 and L_2 will contain all elements of $\mathbb{Z}_n$. Similarly, holding j constant note that each column of L_1 and L_2 will also contain all elements of $\mathbb{Z}_n$. Thus L_1 and L_2 are Latin squares. To prove that L_1 and L_2 are orthogonal we must show that the superposition of L_1 and L_2 contains every ordered pair $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$. If we let $L_1(i, j) = x$ and $L_2(i, j) = y$, we must solve the system

$$x \equiv i + j \pmod{n},$$
$$y = i - j \pmod{n}.$$

Adding the two equations gives

$$i + j + i - j = 2i \equiv (x + y) \pmod{n},$$

and subtracting gives

$$i + j - (i - j) = 2j \equiv (x - y) \pmod{n}.$$

Since $n > 1$ is odd, $2^{-1} = (n + 1)/2$. Therefore, the system has a unique solution given by

$$i \equiv (x + y)(n + 1)/2 \pmod{n},$$
$$j \equiv (x - y)(n + 1)/2 \pmod{n}.$$

As $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n$ was arbitrary, we have shown that the superposition of L_1 and L_2 contains every ordered element in $\mathbb{Z}_n \times \mathbb{Z}_n$, completing the proof. □

Example 4.7. *Suppose $n = 5$. Using Theorem 4.6, we are able to construct the following orthogonal Latin squares.*

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}, \quad \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{bmatrix}.$$

Note that

$$L_1 = bcirc \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \end{bmatrix},$$

and

$$L_2 = circ \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \end{bmatrix}.$$

Next, we showcase an operation very similar to the Kronecker product, which will allow us to construct a new Latin square from two smaller Latin squares. Let L_1 and L_2 be Latin squares of order n_1 and n_2 defined on the sets X and Y respectively. The *direct product* of L_1 and L_2 is denoted as $L_1 \times L_2$, and is the $n_1 n_2 \times n_1 n_2$ array defined by

$$(L_1 \times L_2)((i_1, i_2), (j_1, j_2)) = (L_1(i_1, j_1), L_2(i_2, j_2)).$$

Note that $L_1 \times L_2$ is defined on the symbol set $X \times Y$. To see why $L_1 \times L_2$ is a Latin square, consider the row (i_1, i_2). To find the element (x, y) for $x \in X$ and $y \in Y$, note that since L_1 is a Latin square there is a unique column indexed by j_1 such that $L_1(i_1, j_1) = x$. Similarly, since L_2 is a Latin square there is a unique column indexed by j_2 such that $L_2(i_2, j_2) = y$. Thus $(L_1 \times L_2)((i_1, i_2), (j_1, j_2)) = (x, y)$ as desired. Similarly, we find the element (x, y) in the column (j_1, j_2) as follows. Note that since L_1 is a Latin square there is a unique row indexed by i_1 such that $L_1(i_1, j_1) = x$.

Similarly, since L_2 is a Latin square there is a unique row indexed by i_2 such that $L_2(i_2, j_2) = y$. Thus $(L_1 \times L_2)((i_1, i_2), (j_1, j_2)) = (x, y)$. This discussion establishes the following lemma.

Lemma 4.8. *Let L_1 and L_2 be Latin squares of order n_1 and n_2 defined on the symbol sets X and Y respectively. Then $L_1 \times L_2$ is a Latin square of order $n_1 n_2$ over the symbol set $X \times Y$.*

Example 4.9. *Let*

$$L_1 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \; L_2 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Then $L_1 \times L_2$ is given by

$$L_2 = \begin{bmatrix} (1,2) & (1,1) & (2,2) & (2,1) \\ (1,1) & (1,2) & (2,1) & (2,2) \\ (2,2) & (2,1) & (1,2) & (1,1) \\ (2,1) & (2,2) & (1,1) & (1,2) \end{bmatrix}.$$

We now prove that the direct product preserves orthogonality.

Theorem 4.10. *Let L_1 and L_2 be orthogonal Latin squares of order n_1 on the symbol set X and let M_1 and M_2 be orthogonal Latin squares of order n_2 on the symbol set Y. Then $L_1 \times M_1$ and $L_2 \times M_2$ are orthogonal Latin squares of order $n_1 n_2$.*

Proof. By Lemma 4.8 we know $L_1 \times M_1$ and $L_2 \times M_2$ are both Latin squares of order $n_1 n_2$. We want to show that the superposition of $L_1 \times M_1$ and $L_2 \times M_2$ contains every ordered pair in $(X \times Y) \times (X \times Y)$. Consider the ordered pair of symbols $((x_1, y_1), (x_2, y_2))$. To find the cell $((i_1, i_2), (j_1, j_2))$ containing the symbol, we must have

$$(L_1 \times M_1)((i_1, i_2), (j_1, j_2)) = (x_1, y_1),$$
$$(L_2 \times M_2)((i_1, i_2), (j_1, j_2)) = (x_2, y_2).$$

By the definition of direct product, the first equation means that

$$L_1(i_1, j_1) = x_1,$$
$$M_1(i_2, j_2) = y_1,$$

and the second means that

$$L_2(i_1, j_1) = x_2,$$
$$M_2(i_2, j_2) = y_2.$$

Since L_1 and L_2 are orthogonal, there must be a unique cell (i_1, j_1) such that the superposition of L_1 and L_2 contains (x_1, x_2). Similarly, since M_1 and M_2 are orthogonal, there must be a unique cell (i_2, j_2) such that the superposition of M_1 and M_2 contains (y_1, y_2). Therefore, the cell $((i_1, i_2), (j_1, j_2))$ is the unique cell containing the symbol $((x_1, y_1), (x_2, y_2))$. □

Utilizing all of our results, we are now able to match Euler's findings to produce Latin squares of order $n \not\equiv 2 \pmod 4$.

Theorem 4.11. *If $n \not\equiv 2 \pmod 4$ then there exist orthogonal Latin squares of order n.*

Proof. If $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$ then n is odd, and so we can apply Theorem 4.6 to obtain orthogonal Latin squares of order n.

Then suppose $n \geq 4$. If $n = 2^k$ for $k \geq 2$. In Example 4.4 we have seen orthogonal Latin squares of order 4, which correspond to $k = 2$ and in Example 4.5 we showcased orthogonal Latin squares of order 8, corresponding to $k = 3$. To show that orthogonal Latin squares of order 2^k exist for all k we use a proof by induction. Using Theorem 4.10 we know that since there exists a pair of orthogonal Latin squares of order 4, the direct product of these Latin squares with themselves generate a pair of orthogonal Latin squares of order $16 = 2^4$. Then assume orthogonal Latin squares of order 2^k and 2^{k-1} exist for some $k \geq 4$. To form a pair of orthogonal Latin squares of order

2^{k+1} employ Theorem 4.10 to the orthogonal Latin squares of order 2^{k-1} and 4. This gives us a pair of orthogonal Latin squares of order $2^{k-1}2^2 = 2^{k+1}$, completing the induction. Hence, there exist orthogonal Latin squares of order 2^k for all integers $k \geq 2$.

If $n \neq 2^k$ then write $n = 2^k m$ for some odd integer m. Since $n \equiv 0 \pmod 4$, we must have $k \geq 2$. Since m is odd, by Theorem 4.6 there exist orthogonal Latin squares of order m. As shown above, there also exist orthogonal Latin squares of order 2^k for all $k \geq 2$. Applying Theorem 4.10 to the orthogonal Latin squares of order 2^k and m, we can form a pair of orthogonal Latin squares of order $2^k m$ as desired. □

Another interesting property of orthogonal Latin squares is that permuting symbols will not disrupt orthogonality. To see why, suppose L_1 and L_2 are two orthogonal Latin squares over the symbol set X. As L_1 and L_2 are orthogonal, the superposition of the Latin squares will contain each ordered pair (x_1, y_1) precisely once. If we apply a permutation to L_1 which maps x_1 to x_2 and a permutation to L_2 mapping y_1 to y_2, the ordered pair (x_2, y_2) will also appear precisely once, as (x_1, y_1) appeared once. As this is true for any permutation of entries of X, every pair (x_2, y_2) will appear precisely once, and so L_1 and L_2 will retain orthogonality through applying a permutation to the symbol set X.

4.1.2 Existence

An inferential question to ask after learning about orthogonal Latin squares is can orthogonal Latin squares exist in more than just pairs? To answer this question, we first define this concept and then present an example to answer this question.

Definition 4.12. *A set of k Latin squares, say $\{L_1, L_2, \ldots, L_k\}$ is mutually orthogonal if every pair L_i and L_j, $1 \leq i < j \leq k$ are orthogonal. We call such a set a set of mutually orthogonal Latin squares, abbreviated as MOLS. A set of k MOLS of order n will be denoted as k MOLS(n).*

Example 4.13. *The following is a set of* 3 *MOLS*(4).

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \; L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \; L_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

The above example answers the question of whether orthogonal Latin squares can exist in groups larger than 2. A much more interesting question to ask now is what is how many mutually orthogonal Latin squares of order n can we find for each n? To partially answer this question, we present the following Theorem.

Theorem 4.14. *If S is a set of MOLS(n), then $|S| \leq n - 1$.*

Proof. Let S be a set of MOLS(n) over the symbol set $X = \{1, 2, \ldots, n\}$. According to our previous discussion, we can permute the symbols of each Latin square, and retain the property of orthogonality. Thus, we may assume that the first row of each Latin square contains the symbols, $1, 2, \ldots, n$, written in this particular order.

Then consider the entry in the first column of the second row of some Latin square in the set of MOLS(n), say L. Since the first column of every Latin square in this set of MOLS already contains 1 in the first row, this entry cannot be 1. Then suppose this entry is some $i \in X$, where $i \neq 1$. As the pair (i, i) appears in the first row of the superposition of any two Latin squares, any Latin square orthogonal L must have the entry in its first column and second row be a symbol $j \in X$, such that $j \neq 1$, and $j \neq i$. Therefore, there can be a maximum of $n - 2$ Latin squares orthogonal to L, and so in total, there can be no more than $n - 1$ Latin squares in S, completing the proof. □

In the case that $|S|$ meets the bound of Theorem 4.14 with equality, we say S is a *complete set* of MOLS(n). A complete set of MOLS is interesting because it is equivalent to a projective plane. In 1938, Bose [3] showed that there does not exist a

projective plane of order 6 by relating the existence of a projective plane of order n to a complete set of MOLS(n). We state Bose's result without proof.

Theorem 4.15 (Bose, [19])**.** *Let $n \geq 3$. There exists a projective plane of order n if and only if there exists a complete set of $n-1$ MOLS(n).*

In Example 4.13 the set of 3 MOLS(4) forms a complete set. Naturally, the next question to ask is when is it possible to form a complete set of MOLS(n). In other words, for what n can we find $n-1$ MOLS(n)? We can partially answer this question with the following result.

Theorem 4.16. *If $q \geq 3$ is a prime power, then there exists $q-1$ MOLS(q).*

Proof. Consider the case when q is prime. We will construct q MOLS(q) over the symbol set $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. Note that since q is prime $\mathbb{Z}_q$ is a finite field of order q. We construct the $q-1$ Latin squares L_k for $k \in \{1, 2, \ldots, q-1\}$ as follows. Define

$$L_k = \begin{bmatrix} 0 & 1 & \cdots & q-1 \\ k & k+1 & \cdots & k+(q-1) \\ 2k & 2k+1 & \cdots & 2k+(q-1) \\ \vdots & \vdots & \ddots & \vdots \\ (q-1)k & (q-1)k+1 & \cdots & (q-1)k+(q-1) \end{bmatrix},$$

where we index the rows and columns by elements $\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$. We first show that each L_k is a Latin square. It is readily verified that the entries in each row are permutations of $\mathbb{Z}_q$. Then consider the j-th column of L_k. If $i_1 k + j \equiv i_2 k + j \pmod{q}$, where i_1, i_2 are the indices of two rows of L_k, it follows that $i_1 k \equiv i_2 k \pmod{q}$. Since $\mathbb{Z}_q$ is a field, there exists $l = k^{-1}$. Multiplying both sides of this equivalence by l we see $i_1 \equiv i_2 \pmod{q}$, meaning that the entries in the j-th column of L_k are all distinct. As j was arbitrary, every L_k is a Latin square.

Next, we must verify that each pair of Latin squares is orthogonal. Suppose that $k_1, k_2 \in \{1, 2, \ldots, q-1\}$, $k_1 \neq k_2$. Then suppose that when we superimpose L_{k_1} and

L_{k_2}, the ordered pair in the position indexed by (i_1, j_1) is the same as the ordered pair in the position indexed by (i_2, j_2), for some $i_1, i_2, j_1, j_2 \in \mathbb{Z}_q$. Then using the definition of L_{k_1} we have

$$i_1 k_1 + j_1 \equiv i_2 k_1 + j_2 \pmod{q}, \tag{$\star$}$$

and using the definition of L_{k_2} we have

$$i_1 k_2 + j_1 \equiv i_2 k_2 + j_2 \pmod{q}. \tag{$\star\star$}$$

Subtracting the two equations above we see

$$\begin{aligned} i_1 k_1 + j_1 - (i_1 k_2 + j_1) &\equiv i_2 k_1 + j_2 - (i_2 k_2 + j_2) \pmod{q} \\ i_1 k_1 - i_1 k_2 &\equiv i_2 k_1 - i_2 k_2 \pmod{q} \\ i_1 (k_1 - k_2) &\equiv i_2 (k_1 - k_2) \pmod{q}. \end{aligned}$$

Then as $k_1 \neq k_2$, we must have $k_1 - k_2 \neq 0$. Since $\mathbb{Z}_q$ is a field, there exists some $l = (k_1 - k_2)^{-1} \in \mathbb{Z}$. Multiplying both sides by l we see $i_1 \equiv i_2 \pmod{q}$. Then using $(\star)$ or $(\star\star)$ we can verify that $j_1 \equiv j_2 \pmod{q}$. Thus, we have shown that the position indexed by (i_1, j_1) and the position indexed by (i_2, j_2) are the same. Therefore, the superposition of L_{k_1} and L_{k_2} contains each ordered pair precisely once, meaning that L_{k_1} and L_{k_2} are orthogonal. As k_1, k_2 were arbitrary, we see that $\{L_1, L_2, \ldots, L_{q-1}\}$ is a set of $q - 1$ MOLS(q).

When q is a prime power, the proof is essentially the same, however, instead of working over the $\mathbb{Z}_q$, we work over $\mathbb{F}_q$. In this case, the Latin squares L_k are defined for $k \in \mathbb{F}_q \setminus \{0\}$, and we index the rows and columns of L_k by elements of $\mathbb{F}_q$. □

We have now seen that it is possible to find a complete set of MOLS(n) whenever n is a prime power. However, circling back to our discussion of Euler's original problem, it has been shown that there does not exist a pair of orthogonal Latin squares of order 6. Hence, there does not exist a complete set of MOLS(6).

Moreover, in 1989 [13] Clement Wing Hong Lam, Henry Thiel and Stan Swiercz used a computer search to prove that there does not exist a projective plane of order 10. Equivalently, this showed that there does not exist a complete set of MOLS(10). Currently, the largest known set of MOLS(10) contains only two Latin squares. It is not known if there are sets of MOLS(10) containing more than two Latin squares.

The next open order is 12. The existence of a projective plane of order 12 is unknown. However, the largest known set of MOLS(12) contains five Latin squares. It is also unknown if there are sets of MOLS(12) containing more than five Latin squares.

4.2 Suitable Latin Squares

We can slightly modify the definition of orthogonal Latin squares to help us facilitate future constructions in Chapter 6. Suitable Latin squares were first introduced by Holzmann, Kharaghani and Orrick in [8].

Definition 4.17. *Let L_1 and L_2 be two Latin squares defined over the symbol set X. L_1 and L_2 are called suitable if every superimposition of each row of L_1 on each row of L_2 has only one element in the form (x, x).*

In other words, two Latin squares, L_1 and L_2, are suitable if any row of L_1, when superimposed on a row of L_2, agrees in precisely one position. As we defined sets of mutually orthogonal Latin squares, we can also define sets of mutually suitable Latin squares.

Definition 4.18. *A set of k Latin squares, say $\{L_1, L_2, \ldots, L_k\}$ is mutually suitable if every pair L_i and L_j, $1 \leq i < j \leq k$ are suitable. We call such a set a set of mutually suitable Latin squares, abbreviated as MSLS(n).*

Example 4.19. *The following is a set of* 3 *MSLS*(4).

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \; L_2 = \begin{bmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}, \; L_3 = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \end{bmatrix}.$$

Orthogonal and suitable Latin squares are similar in structure, however, we must be mindful of their differences. For example, as was shown in Theorem 4.16 and Theorem 4.14, we usually write sets of mutually orthogonal Latin squares all having the same first row. But mutually suitable Latin squares cannot be written in this form, as a row from one Latin square must agree in precisely one column as a row from another Latin square. Nevertheless, MOLS and MSLS are very closely related. The following theorem demonstrates how given a pair of orthogonal Latin squares, we can construct a pair of suitable Latin squares and vice versa.

Theorem 4.20. *There are* m *MOLS*(n) *if and only if there are* m *MSLS*(n).

Proof. Let S be the set of MOLS(n) over the symbol set $X = \{1, 2, \ldots, n\}$. Let L_x and L_y be a pair of orthogonal Latin squares in S, and index the rows and columns of L_x and L_y by the elements of X. Then suppose that the (i, j) position of L_x is k. Then perform the transformation where i becomes the entry in the position indexed by (k, j). Doing this for all $i, j \in X$ the transformation $((i, j), k) \mapsto ((k, j), i)$ gives L'_x, and doing the same for L_y gives L_y'.

We now show that L'_x and L'_y are Latin squares. First, suppose that the entry k in the position indexed by (i_1, j) is the same as the entry in the position (i_2, j) of L'_x. Then the entry i_1 appears in the position indexed by (k, j) in L_x. Similarly, the entry i_2 must also appear in the position indexed by (k, j). Thus $i_1 = i_2$, and so the columns of L'_x are permutations of X. A similar argument shows that the rows of L'_x are also permutations of X. As the choice of L_x was arbitrary, this is true for any Latin square in S.

Next, we show L'_x and L'_y are suitable. Suppose that when superimposing the row indexed by i_1 of L'_x and the row indexed by i_2 of L'_y, there are two columns, say j_1 and j_2, where the entries agree. Let k_1 be the entry in the position (i_1, j_1) of L'_x and (i_2, j_1) of L'_y, and let k_2 be the entry in the position (i_1, j_2) of L'_x and (i_2, j_2) of L'_y. Reversing the transformation, this tells that the superimposition of L_x and L_y contains the ordered pair (i_1, i_2) in the position (k_1, j_1) and the superimposition also contains the ordered pair (i_1, i_2) in the position (k_2, j_2). However, as L_x and L_y are orthogonal, we must have $k_1 = k_2$ and $j_1 = j_2$. This means that the row i_1 of L'_x agrees with the entries of row i_2 of L'_y in precisely one position, meaning that L'_x and L'_y are suitable. As the choice of L_x and L_y was arbitrary, we have shown we can use a set of m MOLS(n) to form a set of m MSLS(n).

To start with a set of m MSLS(n) and obtain a set of m MOLS(n), the reverse of the transformation described above gives the desired result. □

The following is an immediate consequence of Theorem 4.16 and Theorem 4.20.

Lemma 4.21. *If $q \geq 3$ is a prime power, then there exists $q - 1$ MSLS(q).*

Chapter 5

Bent Functions

Outside of novel quantum computing applications, almost all modern computers created today run on binary, where the value 1 represents true, and 0 false. Therefore, it is not difficult to see both the prevalence and usefulness of Boolean algebra (i.e., an algebra which deals with operations on logical values with binary values). The real-world applications of Boolean algebra have resulted in the rapid expansion of this branch of mathematics, leading to the creation and development of topics closely related to Boolean algebra. One such example is the topic of bent functions, which we will specifically focus on. However, before delving into the notion of bent functions, we must first develop our understanding of Boolean functions.

5.1 Boolean Functions

In this section, we define and state some necessary properties of Boolean functions. The primary reference for the results in Sections 5.1 and 5.2 is [25].

Definition 5.1. *A Boolean function on n variables is a function*

$$f : (\mathbb{Z}_2)^n \to \mathbb{Z}_2.$$

Put simply, a Boolean function takes a string of binary as an input, and outputs either a 1 or a 0. We label $\mathcal{B}_n$ to be the set containing all Boolean functions on n variables. Observing the definition, we can predict that there should be a finite

number of unique Boolean functions on n variables. Naturally, one may ask how many Boolean functions exist on n variables. We answer this question in the following proposition.

Proposition 5.2. *There are 2^{2^n} Boolean functions on n variables, i.e., $|\mathcal{B}_n| = 2^{2^n}$.*

Proof. Let $f \in \mathcal{B}_n$ be arbitrary. For any $x \in (\mathbb{Z}_2)^n$, the Boolean function $f(x)$ gives us precisely one output. As there are 2^n choices for $x \in (\mathbb{Z}_2)^n$, there are 2^n possible outputs for $f(x)$. Thus, all possible output values of $f(x)$ are contained in $(\mathbb{Z}_2)^{2^n}$. As the choice of f was arbitrary, we have $|\mathcal{B}_n| = 2^{2^n}$. □

Boolean functions are highly versatile and have many applications. For example, one of the primary applications of Boolean functions is in analyzing and creating digital circuits. Furthermore, Boolean functions give us a novel way to construct Sylvester Hadamard matrices. First, we outline some preliminary results before showcasing the construction. Let $x, y \in (\mathbb{Z}_2)^n$. The inner product of the vectors x, y is defined as

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \pmod 2.$$

Finally, for all $x \in (\mathbb{Z}_2)^n$ define the matrix $S_n = (s_{x,y})$ where rows and columns of S_n are indexed by $(\mathbb{Z}_2)^n$ in lexicographic order, and $s_{x,y} = (-1)^{x \cdot y}$. The matrix S_n will form a Sylvester Hadamard matrix of order 2^n, as we prove in the following theorem.

Theorem 5.3. *S_n is a Hadamard matrix of order 2^n.*

Proof. It is clear that S_n will be a square matrix of order 2^n as there are 2^n elements in $(\mathbb{Z}_2)^n$. Let $x, y \in (\mathbb{Z}_2)^n$. We show that the rows indexed by x and y have an inner product of 0 when $x \neq y$ and an inner product of 2^n when $x = y$. We have

$$\begin{aligned}
\sum_{z \in (\mathbb{Z}_2)^n} s_{x,z} s_{y,z} &= \sum_{z \in (\mathbb{Z}_2)^n} (-1)^{x \cdot z} (-1)^{y \cdot z} \\
&= \sum_{z \in (\mathbb{Z}_2)^n} (-1)^{x \cdot z + y \cdot z} \\
&= \sum_{z \in (\mathbb{Z}_2)^n} (-1)^{(x+y) \cdot z}.
\end{aligned}$$

If $x = y$, since we are working modulo 2, $x + y = 0$ and the above equation simplifies to

$$\sum_{z\in(\mathbb{Z}_2)^n} (-1)^{0\cdot z} = \sum_{z\in(\mathbb{Z}_2)^n} (-1)^0 = 2^n.$$

If $x \neq y$ then $x + y \neq 0$ and the sum simplifies to 0 as there will be the same number of 1's and -1's. Thus

$$\sum_{z\in(\mathbb{Z}_2)^n} (-1)^{(x+y)\cdot z} = 0,$$

showing the inner product of the rows indexed by x and y is 2^n when $x = y$ and 0 otherwise. □

The above discussion establishes the following.

Corollary 5.4. *Let $y \in (\mathbb{Z}_2)^n$. Then*

$$\sum_{x\in(\mathbb{Z}_2)^n} (-1)^{x\cdot y} = 2^n \delta_{y,(0,\ldots,0)}.$$

Example 5.5. *We list the matrices S_n for $n = 2, 3, 4$ below.*

$$S_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix}, \; S_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - \end{pmatrix},$$

and $S_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & - \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - \\ 1 & - & 1 & - & 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 \\ 1 & 1 & - & - & 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 \\ 1 & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - \\ 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 & 1 & - & 1 & - \\ 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - \\ 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 \end{pmatrix}.$

Next, we define a useful function.

Definition 5.6. *Let F be any real-valued function $F : (\mathbb{Z}_2)^n \to \mathbb{R}$. For any $x \in (\mathbb{Z}_2)^n$, the Fourier transform of F is the real-valued function defined by*

$$\hat{F}(x) = \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} F(y).$$

For an arbitrary set S and any function $f : (\mathbb{Z}_2)^n \to S$ define the row vector $\phi(f)$ to be the vector listing all the values of $f(x)$ for $x \in (\mathbb{Z}_2)^n$ in lexicographic order. It is not hard to see that $\phi(f)$ will be a vector of length 2^n. Following immediately from how we defined the entries of S_n and the definition of $\hat{F}$ we have the following result.

Lemma 5.7. *For any $F : (\mathbb{Z}_2)^n \to \mathbb{R}$, we have $\phi(\hat{F}) = \phi(F)S_n$.*

Note that since S_n is symmetric, the above result also implies that $\phi(\hat{F}) = S_n \phi(F)^T$.

Corollary 5.8. *Let $F : (\mathbb{Z}_2)^n \to \mathbb{R}$. Then $\phi(\hat{\hat{F}}) = 2^n \phi(F)$.*

Proof. As defined previously, let S_n be the Hadamard matrix of order 2^n. By definition S_n is symmetric. Thus $S_n^2 = 2^n I_{2^n}$. By Lemma 5.7 we have $\phi(\hat{F}) = \phi(F)S_n$. Multiplying on the right by S_n and applying Lemma 5.7 to $\phi(\hat{F})$ gives

$$\phi(\hat{\hat{F}}) = \phi(F)S_n^2.$$

Since S_n is a symmetric Hadamard matrix, we have

$$\phi(F)S_n^2 = 2^n \phi(F) I_{2^n} = 2^n \phi(F)$$

and so we have shown $\phi(\hat{\hat{F}}) = 2^n \phi(F)$. □

Example 5.9. *We now summarize the results above with an example. Consider the case of $n = 4$ variables, and the boolean function $f = x_1x_2 + x_3x_4$. Then, we find $\phi(f)$ by computing all possible inputs in lexicographic order. For example, the first entry of $\phi(f)$ is the output of $f((0,0,0,0))$, the second entry is the output of $f((0,0,0,1))$ and so on. Doing this, we obtain*

$$\phi(f) = (\,0\;0\;0\;1\;0\;0\;0\;1\;0\;0\;0\;1\;1\;1\;1\;0\,).$$

Next, define the real valued function $F(x) = (-1)^{f(x)}$ *for all* $x \in (\mathbb{Z}_2)^4$. *Then,*

$$\phi(F) = (\,1\;1\;1\;-\;1\;1\;1\;-\;1\;1\;1\;-\;-\;-\;-\;1\,).$$

Next, consider the matrix S_4 *from Example 5.5. Observe that*

$$S_4\phi(F)^T = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - & 1 & - \\ 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - \\ 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 & 1 & - & - & 1 \\ 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - \\ 1 & - & 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 \\ 1 & 1 & - & - & - & - & 1 & 1 & 1 & 1 & - & - & - & - & 1 & 1 \\ 1 & - & - & 1 & - & 1 & 1 & - & 1 & - & - & 1 & - & 1 & 1 & - \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - \\ 1 & - & 1 & - & 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 \\ 1 & 1 & - & - & 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 \\ 1 & - & - & 1 & 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - \\ 1 & 1 & 1 & 1 & - & - & - & - & - & - & - & - & 1 & 1 & 1 & 1 \\ 1 & - & 1 & - & - & 1 & - & 1 & - & 1 & - & 1 & 1 & - & 1 & - \\ 1 & 1 & - & - & - & - & 1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - \\ 1 & - & - & 1 & - & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ - \\ 1 \\ 1 \\ 1 \\ - \\ 1 \\ 1 \\ 1 \\ - \\ - \\ - \\ - \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ 4 \\ 4 \\ \bar{4} \\ 4 \\ 4 \\ 4 \\ \bar{4} \\ 4 \\ 4 \\ 4 \\ \bar{4} \\ \bar{4} \\ \bar{4} \\ \bar{4} \\ 4 \end{pmatrix} = \phi(\hat{F})^T$$

where $\bar{4}$ *denotes* -4. *Finally, since* $(S_4)^2 = 16I_{16}$ *we have*

$$\phi(\hat{\hat{F}}) = \begin{pmatrix} 16 & 16 & 16 & \bar{16} & 16 & 16 & 16 & \bar{16} & 16 & 16 & 16 & \bar{16} & \bar{16} & \bar{16} & \bar{16} & 16 \end{pmatrix} = 16\phi(F),$$

where $\bar{16}$ *denotes* -16.

5.2 Bent Functions

So far, we have introduced and proved some useful properties of Boolean functions. However, with the extensive prevalence of binary within modern technology, the functionality of Boolean functions is not limited to just analyzing and creating digital circuits and constructing Hadamard matrices. Boolean functions are also used extensively in cryptography for their security applications. Specifically, a special subset of Boolean functions which are particularly useful are those which are *maximally non-linear*. These Boolean functions which are maximally non-linear are called *bent functions*. However, before stating a formal definition for bent functions, we must explore the notion of non-linearity and how it relates to Boolean functions.

The measure of non-linearity, as the name suggests, is a measure of how far from the notion of linearity a given function is. In other words, it is a measure of how hard it is to approximate the function by a linear function. However, to understand non-linearity, we must understand what it means for a boolean function to be linear. Undoubtedly, anyone following along will already possess an understanding of linear functions. Logically, we can extend the notion of linear functions to Boolean functions.

Definition 5.10. *Let $f \in \mathcal{B}_n$. Then f is a linear function if for all $x \in (\mathbb{Z}_2)^n$*

$$f(x) = a \cdot x,$$

for some $a \in (\mathbb{Z}_2)^n$.

To extend this definition, a function $f \in \mathcal{B}_n$ which is in the form of

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

for some $a \in (\mathbb{Z}_2)^n$ and $b \in \mathbb{Z}_2$ is called an *affine function*. Notice that when $b = 0$ in an affine function f, the function fits the definition of a linear function. Thus all linear functions are affine functions. Observing the definition of linear functions, we can see that as there are 2^n choices for $a \in (\mathbb{Z}_2)^n$, there are 2^n linear functions in $\mathcal{B}_n$. Similarly, as $b = 0$ or $b = 1$, there are 2^{n+1} affine functions in $\mathcal{B}_n$.

Next, to help objectively measure non-linearity, we define the *distance* between two functions $f, g \in \mathcal{B}_n$ to be equal to the Hamming distance between the vectors $\phi(f)$ and $\phi(g)$, and we denote this value by $d(f, g)$. In other words, the distance between f and g is given by

$$d(f, g) = |\{x \in (\mathbb{Z}_2)^n : f(x) \neq g(x)\}|.$$

One way of measuring nonlinearity comes from the use of Fourier coefficients. The following result relates the Fourier transform of a function $f \in \mathcal{B}_n$ to the distance between f and an affine function.

Theorem 5.11. *Let $f \in \mathcal{B}_n$, and define $F(x) = (-1)^{f(x)}$. Then for any $a \in (\mathbb{Z}_2)^n$ we have*

$$d(f, a \cdot x) = 2^{n-1} - \frac{1}{2}\hat{F}(a)$$

and

$$d(f, a \cdot x + 1) = 2^{n-1} + \frac{1}{2}\hat{F}(a).$$

Proof. From the definition of $\hat{F}$, observe

$$\begin{aligned}
\hat{F}(a) &= \sum_{x \in (\mathbb{Z}_2)^n} (-1)^{a \cdot x}(-1)^{f(x)} \\
&= \sum_{x \in (\mathbb{Z}_2)^n} (-1)^{a \cdot x + f(x)} \\
&= |\{x \in (\mathbb{Z}_2)^n : a \cdot x = f(x)\}| - |\{x \in (\mathbb{Z}_2)^n : a \cdot x \neq f(x)\}| \\
&= 2^n - 2d(f, a \cdot x),
\end{aligned}$$

where we use the definition of $d(f, g)$ to simplify the equation in the last step. Solving for $d(f, a \cdot x)$

$$d(f, a \cdot x) = 2^{n-1} - \frac{1}{2}\hat{F}(a).$$

Finally, note that $f(x) = a \cdot x$ if and only if $f(x) \neq a \cdot x + 1$. Thus

$$d(f, a \cdot x) + d(f, a \cdot x + 1) = 2^n.$$

Solving for $d(f, a \cdot x + 1)$ gives

$$d(f, a \cdot x + 1) = 2^n - d(f, a \cdot x) = 2^{n-1} + \frac{1}{2}\hat{F}(a).$$

□

Finally, we define the *nonlinearity* of $f \in \mathcal{B}_n$ as

$$N_f = \min\{d(f, a \cdot x), d(f, a \cdot x + 1) : a \in (\mathbb{Z}_2)^n\}.$$

In other words, the nonlinearity of f is equal to the minimum number of different outputs between f and an affine function in the form of $a \cdot x + b$ for $a \in (\mathbb{Z}_2)^n$ and

$b \in \mathbb{Z}_2$. Equivalently, it is equal to the value of the minimum Hamming distance between $\phi(f)$ and $\phi(a \cdot x + b)$ for $a \in (\mathbb{Z}_2)^n$ and $b \in \mathbb{Z}_2$.

Applying Theorem 5.11, observe that

$$N_f = 2^{n-1} - \frac{1}{2}\hat{F}_m,$$

where $\hat{F}_m = \max\{|\hat{F}(x)| : x \in (\mathbb{Z}_2)^n\}$. We are now able to define bent functions formally.

Definition 5.12. *A bent function is a function $f \in \mathcal{B}_n$ such that $|\hat{F}(x)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$.*

Since $|\hat{F}(x)|$ must be an integer, a bent function can only exist when $f \in \mathcal{B}_n$ for an even n.

Example 5.13. *In Example 5.9, we saw for $n = 4$ variables, and the boolean function $f = x_1x_2 + x_3x_4$ and the real-valued function $F(x) = (-1)^{f(x)}$ we have*

$$\phi(f) = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

To find the nonlinearity of f we find the minimum Hamming distance between $\phi(f)$ and $\phi(a \cdot x + b)$ for $a \in (\mathbb{Z}_2)^4$ and $b \in \mathbb{Z}_2$. For $a = \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}$ note that

$$\phi(a \cdot x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and $d(f, a \cdot x) = 6$. Similarly,

$$\phi(a \cdot x + 1) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix},$$

and correspondingly $d(f, a \cdot x + 1) = 10$. To avoid tedious computations for the remaining choices of a, refer to Example 5.9, where we saw

$$\phi(\hat{F}) = \begin{pmatrix} 4 & 4 & 4 & \bar{4} & 4 & 4 & 4 & \bar{4} & 4 & 4 & 4 & \bar{4} & \bar{4} & \bar{4} & \bar{4} & 4 \end{pmatrix},$$

where -4 is written as $\bar{4}$. As $|\hat{F}(x)| = 4$ for all $x \in (\mathbb{Z}_2)^4$, f is a bent function on four variables. Furthermore, observe that

$$N_f = 2^{4-1} - \frac{1}{2}\hat{F}_m(x) = 8 - \frac{4}{2} = 6.$$

The next theorem shows that this is the maximum nonlinearity for a boolean function on four variables.

Bent functions are boolean functions that are maximally non-linear. In other words, a bent function maximizes N_f. The following theorem proves this statement.

Theorem 5.14. *Let $f \in \mathcal{B}_n$ and $F(x) = (-1)^{f(x)}$. Then $N_f \leq 2^{n-1} - 2^{n/2-1}$ and equality holds if and only if f is a bent function.*

Proof. First, suppose f is a bent function. Then $|\hat{F}(x)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$. Hence $\hat{F}_m(x) = 2^{n/2}$ and so

$$N_f = 2^{n-1} - \frac{1}{2}\hat{F}_m(x) = 2^{n/2} - 2^{n/2-1}.$$

Conversely, suppose $N_f = 2^{n-1} - 2^{n/2-1}$. Observe that

$$\begin{aligned}
\sum_{x\in(\mathbb{Z}_2)^n} (\hat{F}(x))^2 &= \sum_{x\in(\mathbb{Z}_2)^n} \left(\sum_{y\in(\mathbb{Z}_2)^n} (-1)^{x\cdot y} F(y) \right)^2 \\
&= \sum_{x\in(\mathbb{Z}_2)^n} \left[\left(\sum_{y\in(\mathbb{Z}_2)^n} (-1)^{x\cdot y} F(y) \right) \left(\sum_{z\in(\mathbb{Z}_2)^n} (-1)^{x\cdot z} F(z) \right) \right] \\
&= \sum_{x\in(\mathbb{Z}_2)^n} \sum_{y\in(\mathbb{Z}_2)^n} \sum_{z\in(\mathbb{Z}_2)^n} (-1)^{x\cdot y} F(y) (-1)^{x\cdot z} F(z) \\
&= \sum_{x\in(\mathbb{Z}_2)^n} \sum_{y\in(\mathbb{Z}_2)^n} \sum_{z\in(\mathbb{Z}_2)^n} (-1)^{x\cdot y + x\cdot z} F(y) F(z) \\
&= \sum_{x\in(\mathbb{Z}_2)^n} \sum_{y\in(\mathbb{Z}_2)^n} \sum_{z\in(\mathbb{Z}_2)^n} (-1)^{x\cdot (y+z)} F(y) F(z) \\
&= \sum_{y\in(\mathbb{Z}_2)^n} \sum_{z\in(\mathbb{Z}_2)^n} F(y) F(z) \sum_{x\in(\mathbb{Z}_2)^n} (-1)^{x\cdot (y+z)} \\
&= \sum_{y\in(\mathbb{Z}_2)^n} \sum_{z\in(\mathbb{Z}_2)^n} F(y) F(z) 2^n \delta_{y,z} \\
&= 2^n \sum_{y\in(\mathbb{Z}_2)^n} (F(y))^2 \\
&= 2^n 2^n \\
&= 2^{2n}.
\end{aligned}$$

Note that since $\hat{F}(x) \leq \hat{F}_m$ for all $x \in (\mathbb{Z}_2)^n$, and there are precisely 2^n possible choices for x, using the identity found above we have

$$2^{2n} = \sum_{x\in(\mathbb{Z}_2)^n} (\hat{F}(x))^2 \leq 2^n (\hat{F}_m)^2.$$

Thus $2^{n/2} \leq \hat{F}_m$ and so

$$N_f = 2^{n-1} - 2^{n/2-1} \geq 2^{n-1} - \frac{1}{2}\hat{F}_m = N_f,$$

implying that $\hat{F}_m = |\hat{F}(x)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$. □

The following lemma will further generalize the sum which was carefully proven above.

Lemma 5.15. *Suppose $f \in \mathcal{B}_n$ and $F = (-1)^f$. Then for $y \in (\mathbb{Z}_2)^n$ it holds that*

$$\sum_{x\in(\mathbb{Z}_2)^n} \hat{F}(x)\hat{F}(x+y) = \begin{cases} 2^{2n} & \text{if } y = (0,\ldots,0), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The proof for $y = (0, \ldots, 0)$ is shown in Theorem 5.14. The proof for $y \neq (0, \ldots, 0)$ follows closely as shown

$$\begin{aligned}
&\sum_{x \in (\mathbb{Z}_2)^n} \hat{F}(x)\hat{F}(x+y) \\
&= \sum_{x \in (\mathbb{Z}_2)^n} \sum_{a \in (\mathbb{Z}_2)^n} \sum_{b \in (\mathbb{Z}_2)^n} (-1)^{x \cdot a} F(a) (-1)^{(x+y) \cdot b} F(b) \\
&= \sum_{a \in (\mathbb{Z}_2)^n} \sum_{b \in (\mathbb{Z}_2)^n} (-1)^{y \cdot b} F(a) F(b) \sum_{x \in (\mathbb{Z}_2)^n} (-1)^{x \cdot (a+b)} \\
&= \sum_{a \in (\mathbb{Z}_2)^n} \sum_{b \in (\mathbb{Z}_2)^n} (-1)^{y \cdot b} F(a) F(b) 2^n \delta_{a,b} \\
&= 2^n \sum_{a \in (\mathbb{Z}_2)^n} (-1)^{y \cdot a} (F(a))^2 \\
&= 2^{2n} \delta_{y,(0,\ldots,0)}
\end{aligned}$$

where we use the fact that $F(a) = \pm 1$ and Corollary 5.4 to simplify the final summation. □

Therefore, it is straightforward to see that on $n = 2$ variables the function $f = x_1 x_2$ is also a bent function. Taking $F = (-1)^f$ the Fourier coefficients of F are $\phi(\hat{F}) = \begin{pmatrix} 2 & 2 & 2 & -2 \end{pmatrix}$ with the nonlinearity given by $N_f = 2^{2-1} - 2^{2/2}/2 = 1$. We have also just shown that on $n = 4$ variables, the function $f = x_1 x_2 + x_3 x_4$ is also bent. It is possible to generalize these results to all even $n \geq 2$. We first prove a useful preliminary result.

Lemma 5.16. *Let $f_1 \in \mathcal{B}_n$ and $f_2 \in \mathcal{B}_k$ both be bent functions. Then $f \in \mathcal{B}_{n+k}$ defined by*

$$f = f_1 \oplus f_2 = f_1(x_1, \ldots, x_n) + f_2(x_{n+1}, \ldots, x_{n+k})$$

is a bent function.

Proof. First, define $F = (-1)^f$, $F_1 = (-1)^{f_1}$ and $F_2 = (-1)^{f_2}$. Then let $x = (x_1, \ldots, x_{n+k})$, $x_1 = (x_1, \ldots, x_n)$ and $x_2 = (x_{n+1}, \ldots, x_{n+k})$ where

$$x = x_1 \oplus x_2 = (x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+k}).$$

Observe that for any $y \in (\mathbb{Z}_2)^{n+k}$

$$\begin{aligned}
\hat{F}(y) &= \sum_{x \in (\mathbb{Z}_2)^{n+k}} (-1)^{x \cdot y} F(x) \\
&= \sum_{x_1 \in (\mathbb{Z}_2)^n,\ x_2 \in (\mathbb{Z}_2)^k} (-1)^{(x_1 \oplus x_2) \cdot (y_1 \oplus y_2)} F_1(x_1) F_2(x_2) \\
&= \sum_{x_1 \in (\mathbb{Z}_2)^n} \sum_{x_2 \in (\mathbb{Z}_2)^k} (-1)^{x_1 \cdot y_1 + x_2 \cdot y_2} F_1(x_1) F_2(x_2) \\
&= \sum_{x_1 \in (\mathbb{Z}_2)^n} \sum_{x_2 \in (\mathbb{Z}_2)^k} (-1)^{x_1 \cdot y_1} (-1)^{x_2 \cdot y_2} F_1(x_1) F_2(x_2) \\
&= \left(\sum_{x_1 \in (\mathbb{Z}_2)^n} (-1)^{x_1 \cdot y_1} F_1(x_1) \right) \left(\sum_{x_2 \in (\mathbb{Z}_2)^k} (-1)^{x_2 \cdot y_2} F_2(x_2) \right) \\
&= \hat{F}_1(y_1) \hat{F}_2(y_2).
\end{aligned}$$

Since f_1 is a bent function we have $|\hat{F}_n(x_1)| = 2^{n/2}$ for all $x_1 \in (\mathbb{Z}_2)^n$. Similarly, as f_2 is a bent function we have $|\hat{F}_k(x_2)| = 2^{k/2}$ for all $x_2 \in (\mathbb{Z}_2)^k$. Thus

$$|\hat{F}(x)| = 2^{n/2} 2^{k/2} = 2^{(n+k)/2}$$

for all $x \in (\mathbb{Z}_2)^{n+k}$. Thus

$$N_f = 2^{n+k-1} - \frac{1}{2} 2^{(n+k)/2} = 2^{n+k-1} - 2^{(n+k)/2-1}$$

meeting the upper bound of Theorem 5.14. Therefore f is a bent function as desired.

□

We are now able to inductively prove the following result.

Corollary 5.17. *Let n be an even integer. Suppose $f \in \mathcal{B}_n$ is defined by $f_n = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$. Then f is a bent function.*

Proof. We have already seen that $f_2 = x_1x_2$ is a bent function. Then suppose

$$f_m = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$$

is a bent function for some even integer $m \geq 2$. Since $f_2 = x_{m+1}x_{m+2}$ is bent, we apply Lemma 5.16 to see that

$$f_m = f_m \oplus f_2 = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m + x_{m+1}x_{m+2}$$

is also a bent function. As $m \geq 2$ was an arbitrary even integer, by the principle of mathematical induction, f_m being a bent function implies f_{m+2} is a bent function. Therefore, for all even integers n, the function f_n is a bent function. □

Theorem 5.18. *Let $f \in \mathcal{B}_n$ and $F = (-1)^f$. Define the $2^n \times 2^n$ matrix $H_f = (h_{x,y})$ whose elements are indexed by $x, y \in (\mathbb{Z}_2)^n$ in lexicographic order and $h_{x,y} = F(x+y)$. Then f is a bent function if and only if H_f is a Hadamard matrix.*

Proof. First, suppose H_f is a Hadamard matrix. We must show that $|\hat{F}(x)| = 2^{n/2}$. By our assumption of H_f

$$\sum_{z \in (\mathbb{Z}_2)^n} h_{x,z} h_{y,z} = 2^n \delta_{x,y}.$$

Next, let $G : (\mathbb{Z}_2)^n \to \mathbb{R}$ be defined by

$$G(x) = \frac{1}{2^{n/2}} \hat{F}(x).$$

By Corollary 5.8 note that for any $x \in (\mathbb{Z}_2)^n$

$$\begin{aligned} 2^n F(x) = \hat{\hat{F}}(x) &= \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} \hat{F}(y) \\ &= 2^{n/2} \sum_{y \in (\mathbb{Z}_2)^n} (-1)^{x \cdot y} G(y) \\ &= 2^{n/2} \hat{G}(x), \end{aligned}$$

and so $\hat{G}(x) = 2^{n/2} F(x)$. Then observe that if $y = (0, \ldots, 0)$ we have

$$2^n \delta_{x,(0,\ldots,0)} = \sum_{z \in (\mathbb{Z}_2)^n} h_{x,z} h_{(0,\ldots,0),z},$$

and by definition of H_f observe that

$$\begin{aligned} \sum_{z \in (\mathbb{Z}_2)^n} h_{x,z} h_{(0,\ldots,0),z} &= \sum_{z \in (\mathbb{Z}_2)^n} F(x+z) F(z) \\ &= \sum_{z \in (\mathbb{Z}_2)^n} \left(\frac{1}{2^{n/2}} \hat{G}(x+z) \right) \left(\frac{1}{2^{n/2}} \hat{G}(z) \right) \\ &= \frac{1}{2^n} \sum_{z \in (\mathbb{Z}_2)^n} \hat{G}(x+z) \hat{G}(z). \end{aligned}$$

Following from Corollary 5.15 we have that

$$\begin{aligned}\frac{1}{2^n}\sum_{z\in(\mathbb{Z}_2)^n}\hat{G}(x+z)\hat{G}(z) &= \sum_{z\in(\mathbb{Z}_2)^n}(-1)^{x\cdot z}(G(z))^2\\ &= \sum_{z\in(\mathbb{Z}_2)^n}(-1)^{x\cdot z}\left(\frac{1}{2^{n/2}}\hat{F}\right)^2\\ &= \frac{1}{2^n}\sum_{z\in(\mathbb{Z}_2)^n}(-1)^{x\cdot z}(\hat{F}(z))^2.\end{aligned}$$

Thus for a fixed $x \in (\mathbb{Z}_2)^n$ we see that

$$2^{2n}\delta_{x,(0,\ldots,0)} = \sum_{z\in(\mathbb{Z}_2)^n}(-1)^{x\cdot z}(\hat{F}(z))^2.$$

As x is arbitrary, we can apply the definition of S_n to generalize our simplification in the previous equation to obtain

$$2^{2n}(1,0,\ldots,0) = \phi((\hat{F}(z))^2)S_n.$$

Then multiplying on the right by S_n and simplifying gives

$$\begin{aligned}2^{2n}(1,0,\ldots,0)S_n &= 2^n\phi((\hat{F}(z))^2)\\ 2^n(1,1,\ldots,1) &= \phi((\hat{F}(z))^2)\end{aligned}$$

which shows that $|\hat{F}(z)| = 2^{n/2}$ for all $z \in (\mathbb{Z}_2)^n$, and since $F = (-1)^f$, we have shown that $f \in \mathcal{B}_n$ is a bent function as desired.

Conversely, suppose f is a bent function. As f is bent $|\hat{F}(X)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$. Using the same G as defined above, note that

$$|G(x)| = \left|\frac{1}{2^{n/2}}\hat{F}(x)\right| = 1$$

meaning that $G(x) = (-1)^{g(x)}$ for some $g \in \mathcal{B}_n$. To show H_f is a Hadamard matrix, we show

$$\sum_{z\in(\mathbb{Z}_2)^n} h_{x,z}h_{y,z} = 2^n\delta_{x,y}$$

for all $x, y \in (\mathbb{Z}_2)^n$. Observe that

$$\begin{aligned}\sum_{z\in(\mathbb{Z}_2)^n} h_{x,z}h_{y,z} &= \sum_{z\in(\mathbb{Z}_2)^n} F(x+z)F(y+z)\\ &= \sum_{z\in(\mathbb{Z}_2)^n} \left(\frac{1}{2^{n/2}}\hat{G}(x+z)\right)\left(\frac{1}{2^{n/2}}\hat{G}(y+z)\right)\\ &= \frac{1}{2^n}\sum_{z\in(\mathbb{Z}_2)^n} \hat{G}(x+z)\hat{G}(y+z).\end{aligned}$$

Then define $w = x + z$. Since we are working mod 2, it is straightforward to verify that $x = -x$, so note that this implies $z = w + x$. As $z \in (\mathbb{Z}_2)^n$ and x is fixed w will take all values in $(\mathbb{Z}_2)^n$. Rewriting the variables in terms of w and applying Corollary 5.15 we obtain

$$\begin{aligned}\frac{1}{2^n}\sum_{z\in(\mathbb{Z}_2)^n} \hat{G}(x+z)\hat{G}(y+z) &= \frac{1}{2^n}\sum_{w\in(\mathbb{Z}_2)^n} \hat{G}(w)\hat{G}(x+y+w)\\ &= \frac{1}{2^n}\times 2^{2n}\delta_{x+y,(0,\ldots,0)}\\ &= 2^n\delta_{x,y}\end{aligned}$$

as desired. □

5.3 Bent Sequences

Computer chips are used everywhere. These chips are created in various places around the world by large semiconductor manufacturing companies such as Intel, NVIDIA and TSMC. However, semiconductor manufacturing is an extremely intricate process. Since the creation of the first semiconductors in the mid-1900s, advances in semiconductor manufacturing have led to many notable improvements in size, computational power and efficiency. For example, modern semiconductor wafers are over 2000 times more dense compared to semiconductors manufactured in the 1970s, with the transistor sizes decreasing from 10 micrometres to under 5 nanometers (i.e., Apple M2 chip uses a new 5nm technology). In 1965, Gordon Moore, co-founder of Intel observed that the number of transistors on a microchip doubles nearly annually. However, in

1975, Moore revised his statement to say that the number of transistors would double every two years. This famous observation is referred to as "Moore's Law". This observation gives a great, historically accurate indication of the increasing complexity of semiconductors. The image below showcases the exponential growth of transistor counts since the early 1970s.

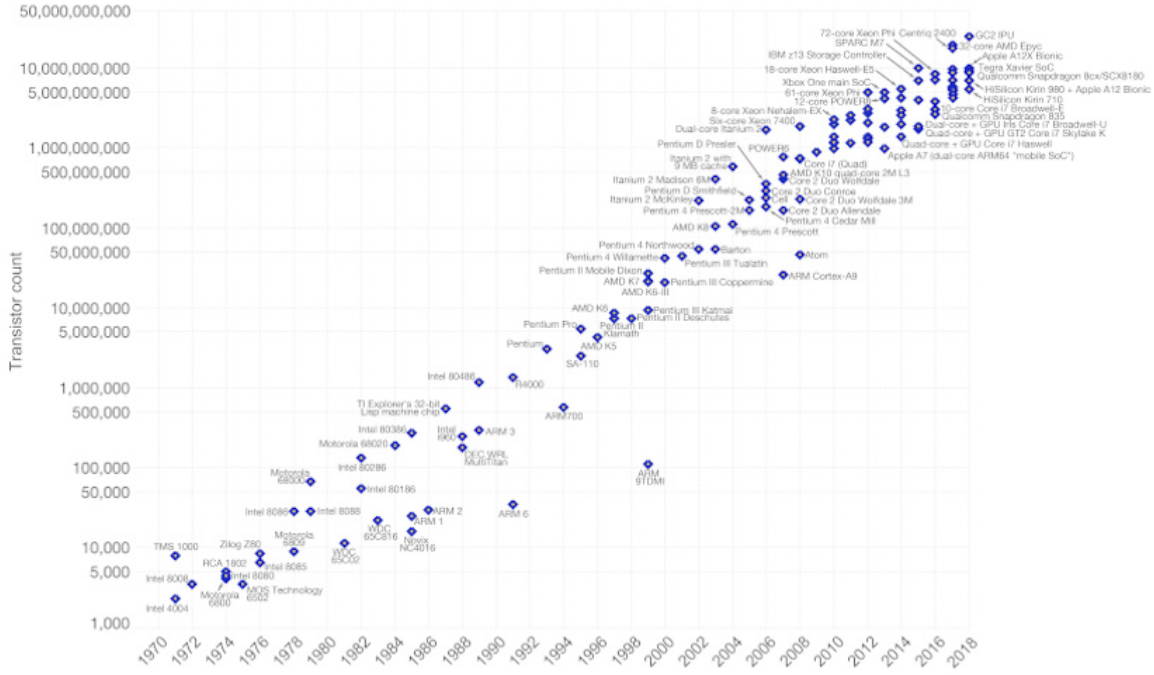

Figure 5.1: Graph of increasing transistor counts found in Our World in Data [18]

However, as chips become smaller and smaller, the process becomes increasingly delicate. To give some reference for how small chip sizes are, consider that a silicon atom measures 0.2nm, and when working with sub-5 nm transistor technology, dealing with imperfections in the manufacturing process becomes unavoidable. Therefore, this has led semiconductor manufacturers to seek out practical solutions to both identifying and authenticating semiconductors. This is possible, because semiconductors manufactured in the same facility, at the same time, and even coming from the same silicone wafer have inherent manufacturing variations. This allows for the differentiation and identification of two devices which may appear to be identical. However, these inherent variations are intrinsically random, and cannot be replicated by the

manufacturer.

One practical solution for both authenticating and identifying devices which manufacturers currently rely on are *physically unclonable functions* (PUFs). The primary references for the applications of PUFs are [14] and [26]. To summarize, these functions allow manufacturers to authenticate semiconductors by generating a unique cryptographic key, leading to greater security, even when the semiconductors have inherent imperfections. These keys can then be recorded to a whitelist, which can later be referenced to verify that a device is not a counterfeit or has been overproduced during the manufacturing process. Furthermore, PUFs can be used in cryptographic algorithms to provide further security. Specifically, PUFs re-generate their static random values at every startup, providing a significant improvement in security against tampering attacks. To measure the security of a PUF, we examine the quality of randomness of the responses as the PUF responds to different challenges. This measure of the randomness of the responses of the PUF is commonly referred to as *entropy* [17]. The challenges come in the form of cryptographic keys. A large number of challenges (i.e., a large code) will of course result in a greater entropy. However, it is of interest to maximize the bits of entropy given a fixed number of challenges.

The primary reference for many of the results found in this Section is [24]. We begin by stating some preliminary definitions which will lay the groundwork for our discussion of bent sequences.

Definition 5.19. *Let C be a binary code of length n over the alphabet $A = \{\pm 1\}$. The deviation of a vector $x \in C$ is given by*

$$\theta(C, x) = \max_{y \in C} |\langle x, y \rangle|.$$

As C is a binary code, it can also be shown that $\langle x, y \rangle = n - 2d(x, y)$, where $d(x, y)$ denotes the Hamming distance of the two codewords x and y.

Definition 5.20. *The total deviation of the code C is defined as*

$$\theta(C) = \min_{x \in A^n} \theta(C, x) = \min_{x \in A^n} \max_{y \in C} |\langle x, y \rangle|.$$

Recall that our goal is to maximize entropy for a fixed number of codewords. One possible approach is to minimize total deviation. Hence, the optimal choices for the first $M = n$ challenges (i.e., codewords) are given by the n rows of a Hadamard matrix of order n. Next, consider that the entropy for a given codeword depends on the joint probabilities of the signs of the Gaussian variables (previously labelled Δ_i). Thus the entropy depends on the identifier vector B, which itself is dependent on the joint probabilities for each codeword. The following results summarize the above discussion.

Lemma 5.21. *The entropy of a PUF with challenge code C is determined by the Gram matrix CC^T whose entries represent the inner products of the codewords $\{\langle x, y\rangle : x, y \in C\}$.*

Lemma 5.22. *Equivalent challenge codes give the same entropy and permuting the order of codewords gives the same entropy.*

Proof. The proof that equivalent challenge codes give the same entropy follows from the fact that permuting coordinates and multiplying coordinates by -1 does not change the inner products of codewords. The proof of the second permuting the order of the codewords does not change entry follows from the fact that permuting the order of the codewords simply permutes the components of the identifier B, which also does not change the entropy. □

Lemma 5.23. *Replacing codewords with their binary complements does not change the entropy.*

Proof. By replacing a codeword $c \in C$, we replace B_c with $-B_c$ in the identifier B. This does not change the entropy. □

Previously, we have mentioned the possibility that minimizing the total deviation for a code maximizes entropy. For the case of $M = n$, this result has been proven true, and it has been shown that the optimal choices for the first $M = n$ challenge

codewords are given by *Hadamard codes*. Hadamard codes are binary codes whose codewords are pairwise orthogonal. In other words, we can think of the $M = n$ codewords of a Hadamard code as the n rows of a Hadamard matrix of order n. However, when adding an additional codeword to the n codewords already present in the Hadamard code, the question of whether minimizing the total deviation of the $M+1$ codewords maximizes entropy has not yet been answered. In [24], it is conjectured that choosing the next codeword can be constructively done by minimizing the total deviation $\theta(C)$. The conjecture is as follows.

Conjecture 5.24. *For the $(n+1)$-th codeword, minimizing the total deviation maximizes the entropy of the PUF responses.*

We now move forward by examining some bounds for total deviation.

Theorem 5.25. *If $\mathcal{H}$ is a Hadamard code of length n then by adding an additional codeword, its total deviation is bounded below by $\sqrt{n} \leq \theta(\mathcal{H})$. Furthermore, $\sqrt{n} = \theta(\mathcal{H})$ occurs if and only if $|\langle x, y\rangle| = \sqrt{n}$ for all codewords $y \in \mathcal{H}$.*

Proof. The codewords of $\mathcal{H}$ form an orthogonal basis for $\mathbb{R}^n$. Then any $x \in \{\pm 1\}^n$ can be decomposed. We have

$$x = \sum_{y \in \mathcal{H}} \frac{\langle x, y\rangle}{\|y\|^2} y,$$

where $\|x\|^2 = \|y\|^2 = n$. Thus,

$$n = \|x\|^2 = \sum_{y \in \mathcal{H}} \left(\frac{\langle x, y\rangle}{n} \right)^2 \|y\|^2 = \sum_{y \in \mathcal{H}} \frac{(\langle x, y\rangle)^2}{n} \leq \theta(\mathcal{H})^2$$

where equality occurs if and only if $|\langle x, y\rangle| = \sqrt{n}$ for all $y \in \mathcal{H}$, which can only occur if n is a perfect square. □

We define a special name for a codeword which achieves equality in Theorem 5.25.

Definition 5.26. *Let $\mathcal{H}$ be a Hadamard code of length n. In the case that the vector x attains the equality $|\langle x, y\rangle| = \sqrt{n}$ for all $y \in \mathcal{H}$, then x is called a bent sequence with respect to the Hadamard code $\mathcal{H}$.*

Example 5.27. *A column vector x, attached to a Hadamard matrix, H, of order 4:*

$$Hx = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ - \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \\ \bar{2} \end{pmatrix}.$$

Indexing the rows of H by r_i for $1 \leq i \leq 4$, notice that $|\langle r_i, x\rangle| = 2$ for all r_i. Hence, x is a bent sequence with respect to H. As the total deviation is bounded below by $\sqrt{4} = 2$, the vector x minimizes total deviation. Additionally, notice that in this example the resulting vector is a multiple of the vector we started with. Namely $Hx = 2x$.

In general, whenever a bent sequence results in a multiple of itself, the sequence is said to be *self-dual* bent sequence. We now give a formal definition.

Definition 5.28. *Let x be a bent sequence with respect to a Hadamard matrix H of order n. Then as $\langle x, y\rangle = \pm\sqrt{n}$ for any row y of H, then the sequence*

$$y = \frac{Hx}{\sqrt{n}} \in \{\pm 1\}^n.$$

The sequence y is called the dual sequence of x. In the case that $y = x$, we say that x is a self-dual bent sequence.

In the previous example, the vector x is a self-dual bent sequence. Throughout Section 5.2 which dealt with bent functions, we have already caught glimpses of some other examples of bent sequences. The following proposition shows the equivalence of bent functions and bent sequences.

Proposition 5.29. *Let $f \in \mathcal{B}_n$ and $F = (-1)^f$. Then f is a bent function if and only if $\phi(F)^T$ is a bent sequence attached to S_n.*

Proof. Suppose f is a bent function. Then we know $|\hat{F}(x)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$. By Lemma 5.7 we also know $\phi(\hat{F})^T = S_n\phi(F)^T$. Since S_n is a Hadamard matrix of

order 2^n, and $|\hat{F}(x)| = 2^{n/2}$ then $|\langle \phi(F), y \rangle| = 2^{n/2}$ for all rows $y \in S_n$. Hence $\phi(F)^T$ is a bent sequence with respect to S_n.

Conversely, suppose $\phi(F)^T$ is a bent sequence attached to S_n. By definition $|\langle \phi(F), y \rangle| = 2^{n/2}$ for all rows $y \in S_n$. This means $|\hat{F}(x)| = 2^{n/2}$ for all $x \in (\mathbb{Z}_2)^n$, which proves that f is a bent function. □

Proposition 5.30. *Let H be a Hadamard matrix of order n. If x is a bent sequence with respect to H, then its dual sequence is bent with respect to H^T, and the dual sequence of y is x.*

Proof. We know $HH^T = H^T H = nI_n$. Then observe

$$\begin{aligned} y &= \frac{xH^T}{\sqrt{n}} \\ yH &= \frac{xH^T H}{\sqrt{n}} \\ yH &= x\sqrt{n} \end{aligned}$$

and so $x = yH/\sqrt{n} \in \{\pm 1\}^n$ as desired. □

Theorem 2.16 showed a method of combining two Hadamard matrices into a larger Hadamard matrix using the Kronecker product. Building off of this result, we prove that if there exist bent sequences attached to the two Hadamard matrices, then the Kronecker product of the two bent sequences gives a new, larger bent sequence.

Proposition 5.31. *Suppose h and k are bent sequences with respect to the Hadamard matrices H and K. Then $h \otimes k$ is a bent sequence with respect to the Hadamard matrix $H \otimes K$.*

Proof. Suppose H is a Hadamard matrix of order n and K is a Hadamard matrix of order m. Then using the fact that $\sqrt{n}\sqrt{m} = \sqrt{nm}$ we have

$$\frac{(h \otimes k)(H \otimes K)^T}{\sqrt{nm}} = \frac{hH^T}{\sqrt{n}} \otimes \frac{kK^T}{\sqrt{m}} \in \{\pm 1\}^{nm},$$

completing the proof. □

5.3.1 Computational Results

We now summarize and expand on some computational found in [24].

- For $n = 16$ there are 5 inequivalent Hadamard matrices. These matrices can be found in the Hadamard matrix database in Magma.

    1. One corresponds to the Sylvester type, where any vector v at a distance of 6 is a bent sequence. This matrix corresponds to the Magma index of 1.
    2. Two of the Hadamard matrices do not meet the total deviation condition required for the existence of bent sequences. These matrices correspond to a Magma index of 2 and 3.
    3. The other two Hadamard matrices met the total deviation lower bound, meaning that there were bent sequences attached to these matrices. These matrices correspond to the Magma index of 4 and 5.

- The bent sequences, labelled v, attached to the Hadamard matrices met the minimum deviation bound with equality, namely $\theta(C, v) = \sqrt{16} = 4$.

- For the two non-equivalent Hadamard matrices with Magma index 4 and 5, there were a total of 384 and 128 bent sequences, respectively.

- Not reported in [24], the Sylvester type corresponding to a Magma index of 1 has a total of 896 bent sequences. None of the bent sequences found are self-dual.

In all of these cases, the bent sequences gave maximal entropy. In these cases, the next codeword which maximized entropy was the one where $\theta(C, v)$ was as small as possible.

Chapter 6

Constructions

In this chapter, we will first delve into the notion of unbiased Hadamard matrices. We will then employ our knowledge of Latin squares from Chapter 4 to construct these matrices as well as show how bent sequences arise from the outlined constructions. Most of the results in this chapter are similar to those included in our paper [23].

6.1 Unbiased Hadamard Matrices

The constructions of real unbiased Hadamard matrices showcased in this section were first published in [8]. We begin by giving a definition.

Definition 6.1. *Two Hadamard matrices H and K of order n are said to be unbiased if*

$$HK^T = \sqrt{n}L,$$

where L is a Hadamard matrix of order n.

The definition of an unbiased Hadamard matrix can also be extended to the complex case. Two BH$(n;q)$ matrices H and K are said to be unbiased if

$$HK^* = \sqrt{n}L,$$

where L is a BH$(n;q)$.

We now present an essential theorem which we will use to construct both Bush-type and mutually unbiased Hadamard matrices. The theorem, originating from [11]

is stated in reference to real Hadamard matrices. We generalize this theorem to the case of Butson Hadamard matrices, starting with the following definition.

Definition 6.2. *Let H be a BH$(n;q)$. Define r_i to be the i-th row of H for $i \in \{1,2,\ldots,n\}$. Then the n auxiliary matrices associated to H are the matrices $c_i = r_i^* r_i$.*

Theorem 6.3. *The auxiliary matrices c_i associated to a normalized BH$(n;q)$ satisfy the following properties:*

1. $c_1 = J_n$,
2. $c_i c_j = \delta_{i,j}(nc_i)$,
3. $c_i^* = c_i$, *and*
4. $\sum_i^n c_i = nI_n$.

Proof. Let H be a normalized BH$(n;q)$. Property 1 follows from the fact that H is normalized. To verify Property 2, note that

$$c_i c_j = (r_i^* r_i)(r_j^* r_j) = r_i^*(r_i r_j^*) r_j.$$

Since H is a Butson Hadamard matrix, if $i \neq j$ then $(r_i r_j^*) = 0$. Otherwise if $i = j$ then $r_i r_j^* = n$ and $n r_i^* r_i = n c_i$ as desired.

Property 3 follows from the properties of the conjugate transpose. We have

$$c_i^* = (r_i^* r_i)^* = r_i^*(r_i^*)^* = r_i^* r_i = c_i.$$

Finally, since H^* is a Hadamard matrix

$$\sum_i^n c_i = \sum_i^n r_i^* r_i = nI_n,$$

as these are the entries on the diagonal of $H^*H = nI_n$, proving Property 4. □

We are now able to present a general construction, allowing us to create the Bush-type Hadamard matrix presented in Example 2.24.

Theorem 6.4. *Suppose $c_1, c_2, \ldots, c_n$ are the auxiliary matrices associated with a normalized BH$(n;q)$. Then there exists a regular BH$(n^2;q)$.*

Proof. Let L be a Latin square of size n on the symbols $X = \{1, 2, \ldots, n\}$. Replace the symbol i in L with c_i to form a matrix H. First, we show that H is a BH$(n^2;q)$. Since L is a Latin square, no columns contain repeated elements. Thus the block rows of H are orthogonal by Part 2 of Theorem 6.3. To see that the rows within a given block row of H are orthogonal we refer to Part 4 of Theorem 6.3. Consider two rows within a block row of H, say a and b. Let $r_{i,j}$ denote the j-th entry in the row i of the BH$(n;q)$. The inner product of these rows simplifies is simplified using the fact that distinct rows and columns of the BH$(n;q)$ are orthogonal, giving us

$$a \cdot b = \sum_{i=1}^{n} \sum_{j=1}^{n} (r_{i,a}^* r_{i,j})(r_{i,b}^* r_{i,j}) = \sum_{i=1}^{n} r_{i,a}^* r_{i,b}^* \sum_{j=1}^{n} r_{i,j} r_{i,j} = n \sum_{i=1}^{n} r_{i,a}^* r_{i,b}^* = 0.$$

Thus, the rows within a given block of H are also orthogonal, so H is a BH$(n^2;q)$. Finally, by Part 4 of Theorem 6.3 it easily follows that H is a regular BH$(n^2;q)$ as desired. □

Remark 6.5. *In Theorem 6.4, if a Latin square is chosen such that it has an all-ones diagonal, then the resulting BH$(n^2;q)$ will be a Bush-type Hadamard matrix. Since Latin squares retain orthogonality with permutation, given a BH$(n;q)$ it will always be possible to form a Bush-type BH$(n^2;q)$ by permitting L to have an all-ones diagonal.*

Theorem 6.6. *Let $c_1, c_2, \ldots, c_n$ be the auxiliary matrices associated with a normalized Butson Hadamard matrix BH$(n;q)$ and suppose there exists k MSLS(n). Then there exists a set of k mutually unbiased BH$(n^2;q)$.*

Proof. Suppose each Latin square L_i in the set of MSLS(n) is written over the symbol set $X = \{1, 2, \ldots, n\}$. For each Latin square L_i for $i \in \{1, 2, \ldots, k\}$, create the BH$(n^2;q)$ following Theorem 6.4 and label the resulting matrices $H_1, H_2, \ldots, H_k$. Then choose two arbitrary matrices from this collection, say H_i and H_j for $i, j \in$

$\{1, 2, \ldots, k\}$, $i \neq j$. Let H_i and H_j come from the Latin squares L_i and L_j, respectively. Since L_i and L_j are suitable, any row of L_i will agree in precisely one position with any row of L_j. Thus, performing the matrix multiplication $H_i H_j^*$, any block row of H_i will have exactly one common auxiliary matrix in the same position as any block column of H_j^*. By Part 3 of Theorem 6.3 the conjugate transpose does not change the auxiliary matrices. Label $K = H_i H_j^*$. Then, by Part 2 of Theorem 6.3, for the fixed auxiliary matrix, say c_m, between any block row of H_i and any block column of H_j^* we have $c_m c_m^* = c_m c_m = n c_m$. For the remaining auxiliary matrices which are not fixed, the resulting matrix multiplications will be zero by Part 2 of Theorem 6.3. So far we have shown that any block row of H_i multiplied by a block column of H_j will look like $n c_m$ for some auxiliary matrix c_m. Thus, K is a matrix made up of n^2 blocks of size $n \times n$, with absolute value n.

To see that K is a multiple of a BH$(n^2; q)$, let $L = K/n$. Consider a block row of L, say r_b. If r_b contains two copies of an auxiliary matrix, say c_m, this means that a given row of L_i contains a common entry m in the same position as two rows of L_j. However, this is a contradiction as L_j is a Latin square. Thus, r_b contains only one copy of each auxiliary matrix, and by Part 4 of Theorem 6.3, any two rows within r_b are orthogonal.

Now consider two block rows of L, say r_a and r_b. If r_a and r_b both contain a common auxiliary matrix, say c_m in any column, this implies that two rows of L_i have a common entry m in the same position as a row of L_j. However, this cannot occur as L_j is a Latin square. Thus by Part 2 of Theorem 6.3 the two block rows r_a and r_b are orthogonal. Therefore, L is a BH$(n^2; q)$ as desired. □

Refer to Example A.1 found in Appendix A for an application of the previous theorem.

6.2 Bent Sequences and Unbiased Hadamard Matrices

There is a direct connection between unbiased Hadamard matrices and bent sequences as defined in Definition 5.26. In fact, given two real unbiased Hadamard matrices of order n, say H and K, by definition, we know $HK^T = \sqrt{n}L$. This shows that each row of K is a bent sequence attached to H. We summarize this discussion in the following theorem.

Theorem 6.7. *Let H_n be a normalized Hadamard matrix of order $n > 2$. Then there exists a Hadamard matrix of order n^2 with at least n^2 attached bent sequences.*

Proof. As $n \equiv 0 \pmod 4$, using Theorem 4.11 we know there exists a pair of orthogonal Latin squares of order n. Applying Theorem 6.6 we can construct two unbiased regular Hadamard matrices of order n^2. Call these matrices H and K. Then by definition, $HK^T = \sqrt{n}L$ for some Hadamard matrix L. As L is Hadamard each row of K is a bent sequence attached to H. Therefore, H is a Hadamard matrix with n^2 attached bent sequences. □

Using Theorem 6.7, we can construct a Bush-type Hadamard matrix H of order $16n^2$ along with $16n^2$ unique bent sequences attached to H for any n, provided the existence of Hadamard matrix of order $4n$. However, the utility of Theorem 6.6 can be further extended. First, we generalize bent sequences to contain complex entries.

Definition 6.8. *Let H be a BH$(n; q)$. Then x is a bent sequence attached to H if*

$$Hx = \sqrt{n} \cdot y,$$

where the entries of y are in $\langle \xi_q \rangle$. If $x = y$ then the sequence is said to be self-dual.

We now state a generalization of Theorem 6.7. We use Theorems 4.11 and 4.6, along with the fact that there exist orthogonal Latin squares of order $n \equiv 2 \pmod 4$, $n > 6$. For the general construction of Latin squares of order $n \equiv 2 \pmod 4$, we refer

to the results of Raj Chandra Bose and Sharadchandra Shankar Shrikhande found in [2].

Lemma 6.9. *Let H_n be a normalized normalized BH$(n;q)$, $n>2$, $n\neq 6$. Then there exists a BH$(n^2;q)$ with at least n^2 attached bent sequences.*

Proof. By the discussion above we know there exists orthogonal Latin squares of order n. Applying Theorem 6.6 we construct two unbiased BH$(n^2;q)$, say H and K. Then as $HK^* = \sqrt{n}L$ where the entries of L are in $\langle \xi_q \rangle$, the complex conjugate of the rows of K provides the n^2 bent sequences. □

Remark 6.10. *Theorem 6.7 and Lemma 6.9 show that there exist at least n^2 bent sequences. In the worst-case scenario for these results, there are a minimum of 2 MSLS(n). However, in many cases, there are much more than 2 MSLS(n). In the case that we have k MSLS(n) it is possible to obtain $(k-1)n^2$ bent sequences. These bent sequences are unique, as the resulting k matrices are mutually unbiased, meaning that no rows can be identical.*

Refer to Example A.2 found in Appendix A for a demonstration of Lemma 6.9. As stated in the appendix, the normalized BH$(4;4)$ comes from Proposition 3.29. By applying this proposition, it is possible to construct an example of a BH$(n^2;n)$ having at least n^2 attached bent sequences for any $n>2, n\neq 6$. We now shift our discussion to that of self-dual bent sequences.

6.3 Self-dual Bent Sequences

In the previous section, we used suitable Latin squares to create unbiased Butson Hadamard matrices resulting in many bent sequences. In this section, we showcase a method of using a single Latin square to construct self-dual bent sequences attached to Butson Hadamard matrices. We begin with an example.

Example 6.11. *Let*

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

and

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & - & j \\ 1 & - & 1 & - \\ 1 & j & - & i \end{pmatrix}.$$

Let c_1, c_2, c_3 and c_4 be the auxiliary matrices corresponding to H. Construct the $BH(16;4)$, labelled K, using Theorem 6.4. Note that K is the second matrix in Example A.2. Then let

$$x = \begin{bmatrix} c_1 & c_3 & c_4 & c_2 \end{bmatrix}.$$

Importantly, notice the auxiliary matrices making up x are the same auxiliary matrices appearing on the diagonal of K, in the same order. Multiplying K by x^* we see

$$Kx^* = \begin{pmatrix} 1&1&1&1&1&i-j&1-1-1&j-i \\ 1&1&1&1&j&1&i--1-1&i&1&j- \\ 1&1&1&1-&j&1&i&1-1--&i&1&j \\ 1&1&1&1&i-&j&1-1-1&j-i&1 \\ 1&j-&i&1-1-1&i-&j&1&1&1&1 \\ i&1&j--1-1&j&1&i-1&1&1&1 \\ -&i&1&j&1-1--&j&1&i&1&1&1&1 \\ j-&i&1-1-1&i-&j&1&1&1&1&1 \\ 1&i-&j&1&1&1&1&1&j-&i&1-1- \\ j&1&i-1&1&1&1&i&1&j--1-1 \\ -&j&1&i&1&1&1&1-&i&1&j&1-1- \\ i-&j&1&1&1&1&1&j-&i&1-1-1 \\ 1-1-1&j-&i&1&1&1&1&1&i-&j \\ -1-1&i&1&j-1&1&1&1&j&1&i- \\ 1-1--&i&1&j&1&1&1&1-&j&1&i \\ -1-1&j-&i&1&1&1&1&1&i-&j&1 \end{pmatrix} \begin{pmatrix} 1&1&1&1 \\ 1&1&1&1 \\ 1&1&1&1 \\ 1&1&1&1 \\ 1-1- \\ -1-1 \\ 1-1- \\ -1-1 \\ 1j-i \\ i1j- \\ -i1j \\ j-i1 \\ 1i-j \\ j1i- \\ -j1i \\ i-j1 \end{pmatrix} = 4 \begin{pmatrix} 1&1&1&1 \\ 1&1&1&1 \\ 1&1&1&1 \\ 1&1&1&1 \\ 1-1- \\ -1-1 \\ 1-1- \\ -1-1 \\ 1j-i \\ i1j- \\ -i1j \\ j-i1 \\ 1i-j \\ j1i- \\ -j1i \\ i-j1 \end{pmatrix}.$$

Note that $Kx^* = 4x^*$. Therefore, the columns of x^* give us four self-dual bent sequences attached to K.

Remark 6.12. *We now give some important context relating to Example 6.11. First, any Latin square L without a constant diagonal works. We used L_2 from Example*

4.13, but L_3 would also work. Notably, all Latin squares constructed without $k = 0$ in Theorem 4.16 will work for the construction given the correct choice of x. In the example, it was noted that x was chosen such that the auxiliary matrices making up x are the same auxiliary matrices appearing on the diagonal of K, in the same order. Therefore, if we chose another Latin square, such as L_3 from Example 4.13 we would have

$$x = \begin{bmatrix} 1 & 4 & 2 & 3 \end{bmatrix},$$

and replace the each symbol i with the corresponding auxiliary matrix c_i. By Theorem 6.3, this particular choice of x ensures that only the diagonal blocks of the matrix constructed from Theorem 6.4 will remain once we multiply on the right by x^*.

The above discussion establishes the following.

Theorem 6.13. *Let H be a $BH(n; q)$ with corresponding auxiliary matrices $c_1, c_2, \ldots, c_n$ and let L be a Latin square of order n over the symbols $X = \{1, 2, \ldots, n\}$ with a non-constant diagonal. Let K be the matrix constructed from Theorem 6.4 using H and L. Suppose the diagonal of L is given by*

$$x = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \end{bmatrix}.$$

Then replacing x_i with c_{x_i}, the columns of x^* provide n self-dual bent sequences attached to K.

6.4 Bent Sequences With Zero Entries

In this section, we allow bent sequences to contain zero entries. Previously, our definition of bent sequences relied on Butson Hadamard matrices. However, in this section, we generalize bent sequences to be attached to a natural generalization of Butson Hadamard matrices, namely, complex weighing matrices.

We begin by broadening the definition of bent sequences to include zero entries.

Let W be a CW$(n, k; q)$. Then x is a *bent sequence* attached to W if

$$Wx = \sqrt{k}y,$$

where the entries of y are in $\langle \xi_q \rangle \cup \{0\}$. As before, if $x = y$ then x is said to be *self-dual*.

First and foremost, we showcase a method of constructing complex weighing matrices analogous to our previous method of constructing Butson Hadmard matrices. Suppose H is a BH$(n; q)$. Then, it is straightforward to verify that adding any number of $n \times n$ zero matrices to the set of auxiliary matrices coming from H does not violate any of the four conditions of Theorem 6.3. This allows us to generalize Theorem 6.4 to create complex weighing matrices.

Theorem 6.14. *Let $c_1, c_2, \ldots, c_n$ be the auxiliary matrices associated with a normalized BH$(n; q)$ and let m be any non-negative integer. Then there exists a CW$(n(n + m), n^2; q)$.*

Proof. Let L be a Latin square of size $n + m$ on the integers $X = \{1, 2, \ldots, n, n + 1, \ldots, n + m\}$. Then, replace the integers $i \leq n$ in L with c_i and $i > n$ with 0_n. Call this new matrix W. From the fact that L is a Latin square, it easily follows that W is an $n(n + m) \times n(n + m)$ matrix with n^2 nonzero entries in every row and column.

To show that W is a CW$(n(n + m), n^2; q)$ recall that in the proof of Theorem 6.4, we showed that distinct block rows and rows within block rows are orthogonal by applying properties of Theorem 6.3, which still holds when adding any number of zero matrices.

To see that two rows within a block row are orthogonal define each zero matrix in the same way as we defined the auxiliary matrices. Namely, note that $0_n = r_0^* r_0$ where r_0 is a row of all zeroes of length n. Then, apply the same process as in the proof of Theorem 6.4 to show that the rows are orthogonal. □

We are now able to generalize Theorem 6.13 to obtain a method constructing

self-dual bent sequences attached to the complex weighing matrices constructed in Theorem 6.14.

Theorem 6.15. *Let H be a BH$(n;q)$ with corresponding auxiliary matrices $c_1, c_2, \ldots, c_n$ and let m be a non-negative integer. Then let $c_{n+1} = \cdots = c_{n+m} = 0_n$. If L is a Latin square of order $n+m$ over the symbols $X = \{1, 2, \ldots, n+m\}$ with all symbols of X appearing on the diagonal. If the diagonal of L is given by*

$$x = \begin{bmatrix} x_1 & x_2 & \cdots & x_{n+m} \end{bmatrix},$$

then replacing the entry x_i with c_{x_i}, the columns of x^* provide n self-dual bent sequences attached the CW$(n(n+m), n^2; q)$ constructed using Theorem 6.14.

Proof. Let K denote the CW$(n(n+m), n^2; q)$ from Theorem 6.14. From our previous discussion, we know that the larger set of auxiliary matrices, now containing m additional zero matrices satisfies all the properties of Theorem 6.3. As a direct consequence of Part 2 of Theorem 6.3, this particular choice of x ensures that only the diagonal blocks of K will remain in the product of Kx^*. Furthermore, as every symbol in X appears on the diagonal of L, x will have precisely m blocks of zeroes, and n blocks of the auxiliary matrices coming from H. □

Refer to Example B.1 found in Appendix B for an example application of Theorem 6.15.

Furthermore, we can generalize Theorem 6.6 to obtain even more bent sequences attached to the complex weighing matrices from Theorem 6.14. First, we extend the definition of unbiased matrices to include weighing matrices. As in the case of Butson Hadamard matrices, two CW$(n, k; q)$, say W and K are said to be *unbiased* if

$$WK^* = \sqrt{k}L,$$

where L is a CW$(n, k; q)$.

Theorem 6.16. *Let $c_1, c_2, \ldots, c_n$ be the auxiliary matrices associated with a normalized Butson Hadamard matrix BH$(n;q)$ and define $c_{n+1} = \cdots = c_{n+m} = 0_n$ where m is some non-negative integer. Suppose there exists k MSLS$(n+m)$. Then there exists a set of k mutually unbiased CW$(n(n+m), n^2; q)$.*

Proof. Suppose each Latin square L_i in the set of MSLS$(n+m)$ is written over the symbol set $X = \{1, 2, \ldots, n+m\}$. For each Latin square L_i for $i \in \{1, 2, \ldots, k\}$, create the CW$(n(n+m), n^2; q)$ following Theorem 6.6 and label the resulting matrices $W_1, W_2, \ldots, W_k$.

We must show that $W_i W_j^* = nW$ where W is a CW$(n(n+m), n^2; q)$. The proof that the rows of W are orthogonal is essentially a restatement of the proof of Theorem 6.6, where we use the fact that the extended set of auxiliary matrices satisfies all four properties of Theorem 6.3 to show that the rows of W are orthogonal.

To complete the proof we must still show that W has a weight of n^2. Let L_i and L_j be the Latin squares from which W_i and W_j were constructed. As a given row of L_i agrees in precisely one position as any row of L_j, each c_i for $i \in \{1, 2, \ldots, n+m\}$ must appear precisely once as each row of L_j is a permutation of X. There are n auxiliary matrices which are non-zero, and so it follows that W has a weight of n^2 completing the proof. □

Example B.2 found in Appendix B uses an application of Theorem 6.16 to construct three CW$(12, 9; 3)$. Each of the matrices has 24 attached bent sequences, coming from the conjugate transpose of rows from the other two complex weighing matrices.

Remark 6.17. *Given $n > 2$ and $n \neq 6$, there will be at least 2 MSLS$(n+m)$. Then any given matrix from the set of mutually unbiased complex weighing matrices constructed in Theorem 6.16 has many attached bent sequences coming from the conjugate transposes of the rows of the other matrices in the set.*

Remark 6.18. *The matrices from Theorems 6.4 and 6.14 are not always symmetric.*

However, in Examples A.1 and B.2, all three Latin squares used were symmetric, ensuring the resulting matrices were also symmetric.

Bibliography

[1] M. Araya, M. Harada, H. Kharaghani, A. Mohammadian, and B. Tayfeh-Rezaie, *On the classification of skew Hadamard matrices of order 36 and related structures*, 2024. arXiv: 2402.11074 [math.CO].

[2] R. C. Bose and S. S. Shrikhande, "On the Construction of Sets of Mutually Orthogonal Latin Squares and the Falsity of a Conjecture of Euler," *Transactions of the American Mathematical Society*, vol. 95, no. 2, pp. 191–209, 1960.

[3] R. C. Bose, "On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Græco-Latin Squares," *Sankhyā: The Indian Journal of Statistics (1933-1960)*, vol. 3, no. 4, pp. 323–338, 1938, ISSN: 00364452.

[4] A. T. Butson, "Generalized Hadamard Matrices," *Proc. Amer. Math. Soc.*, vol. 13, pp. 894–898, 1962.

[5] C. Colbourn and J. Dinitz, *Handbook of Combinatorial Designs* (Discrete Mathematics and Its Applications). Taylor Francis, 2006, ISBN: 9781584885061.

[6] J Hadamard, "Résolution d'une question relative aux déterminants," *Bulletin des Sciences Mathématiques*, vol. 17, pp. 240–246, 1893.

[7] A. Hanaki, H. Kharaghani, A. Mohammadian, and B. Tayfeh-Rezaie, "Classification of skew-Hadamard matrices of order 32 and association schemes of order 31," *Journal of Combinatorial Designs*, vol. 28, pp. 421–427, Feb. 2020.

[8] W. Holzmann, H. Kharaghani, and W. Orrick, "On the real unbiased Hadamard matrices," *Contemporary Mathematics, Combinatorics and Graphs*, vol. 531, pp. 243–250, 2010.

[9] H. Kharaghani and B. Tayfeh-Rezaie, "A Hadamard matrix of order 428," *Journal of Combinatorial Designs*, vol. 13, no. 6, pp. 435–440, 2005.

[10] H. Kharaghani and B. Tayfeh-Rezaie, "On the classification of Hadamard matrices of order 32," *Journal of Combinatorial Designs*, vol. 18, no. 5, pp. 328–336, 2010.

[11] H. Kharaghani, "New class of symmetric weighing matrices," *Ars. Combin.*, vol. 19, 69–72, 1985.

[12] A. Lam and S. Tantaratana, *Theory and applications of spread-spectrum systems. A course reader for the Institute of Electrical and Electronics Engineers (IEEE) self-study course*. IEEE Press, 1994.

[13] C. W. H. Lam, L. Thiel, and S. Swiercz, "The Non-Existence of Finite Projective Planes of Order 10," *Canadian Journal of Mathematics*, vol. 41, no. 6, 1117–1123, 1989.

[14] V. van der Leest, R. Maes, G.-J. Schrijen, and P. Tuyls, "Hardware Intrinsic Security to Protect Value in the Mobile Market," in *ISSE 2014 Securing Electronic Business Processes*, H. Reimer, N. Pohlmann, and W. Schneider, Eds., Springer Fachmedien Wiesbaden, 2014, pp. 188–198.

[15] E. T. Parker, "Orthogonal Latin Squares," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 45, no. 6, pp. 859–862, 1959, ISSN: 00278424.

[16] Quantum Inspire. "Hadamard gate." Accessed: March 3, 2024. (2024), [Online]. Available: https://www.quantum-inspire.com/kbase/hadamard/.

[17] O. Rioul, P. Solé, S. Guilley, and J.-L. Danger, "On the entropy of Physically Unclonable Functions," in *2016 IEEE International Symposium on Information Theory (ISIT)*, 2016, pp. 2928–2932.

[18] M. Roser, H. Ritchie, and E. Mathieu, "What is Moore's Law?" *Our World in Data*, 2023, https://ourworldindata.org/moores-law.

[19] H. J. Ryser, *Combinatorial Mathematics* (Carus Mathematical Monographs). Mathematical Association of America, 1963.

[20] B. Schmidt, "Cyclotomic integers and finite geometry," *American Mathematical Society*, vol. 12, pp. 929–952, 1998.

[21] S. Searle, H. V. Henderson, *et al.*, "Faults in an algorithm for reparameterizing linear models," 1980.

[22] J. Seberry, "Orthogonal designs," in *Orthogonal Designs: Hadamard Matrices, Quadratic Forms and Algebras*. Cham: Springer International Publishing, 2017, ISBN: 978-3-319-59032-5.

[23] M. Shi, D. Lu, H. Kharaghani, V. Zaitsev, and P. Solé, "Spherical codes attached to complex weighing matrices," Submitted January 2024.

[24] P. Solé, W. Cheng, S. Guilley, and O. Rioul, "Bent Sequences over Hadamard Codes for Physically Unclonable Functions," in *2021 IEEE International Symposium on Information Theory (ISIT)*, 2021, pp. 801–806.

[25] D. Stinson, *Combinatorial Designs: Constructions and Analysis*. Springer New York, 2007, ISBN: 9780387217376.

[26] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," Association for Computing Machinery, 2007, 9–14, ISBN: 9781595936271.

[27] J. Sylvester, "Lx. thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers," *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 34, no. 232, pp. 461–475, 1867.

[28] R. Yarlagadda and J. Hershey, *The m-Sequence*. Boston, MA: Springer US, 1997, pp. 75–82.

Appendix A: Bent Sequences without Zero

Example A.1. *The following is a set of* 3 *MSLS*(4) *previously shown in Example 4.19:*

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \; L_2 = \begin{bmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}, \; L_3 = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \end{bmatrix}.$$

Using the following normalized Hadamard matrix of order 4

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & - & - \\ 1 & - & 1 & - \\ 1 & - & - & 1 \end{pmatrix},$$

we obtain the four corresponding auxiliary matrices

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & - & - \\ 1 & 1 & - & - \\ - & - & 1 & 1 \\ - & - & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & - & 1 & - \\ - & 1 & - & 1 \\ 1 & - & 1 & - \\ - & 1 & - & 1 \end{pmatrix}, \begin{pmatrix} 1 & - & - & 1 \\ - & 1 & 1 & - \\ - & 1 & 1 & - \\ 1 & - & - & 1 \end{pmatrix}.$$

Using the three MSLS(4) *the auxiliary matrices shown above we obtain the following three mutually unbiased Bush-type Hadamard matrices of order 16 using Theorem 6.6.*

$$\begin{pmatrix}
1&1&1&1&1&1&-&-&1&-&1&-&-&1\\
1&1&1&1&1&1&-&-&-&1&-&1&1&-\\
1&1&1&1&-&-&1&1&1&-&1&-&-&1\\
1&1&1&1&-&-&1&1&-&1&-&1&1&-\\
1&1&-&-&1&1&1&1&1&-&-&1&-&1\\
1&1&-&-&1&1&1&1&-&1&1&-&-&1\\
-&-&1&1&1&1&1&1&-&1&1&-&1&-\\
-&-&1&1&1&1&1&1&1&-&-&1&-&1\\
1&-&1&-&-&1&1&1&1&1&1&1&-&-\\
-&1&-&1&1&-&1&1&1&1&1&1&-&-\\
1&-&1&-&-&1&1&-&1&1&1&1&-&-\\
-&1&-&1&1&-&1&1&1&1&1&1&-&-\\
1&-&-&1&1&-&1&-&1&1&1&1&1&1\\
-&1&1&-&-&1&-&1&1&1&1&1&1&1\\
-&1&1&-&1&-&-&-&1&1&1&1&1&1\\
1&-&-&1&-&1&-&-&1&1&1&1&1&1
\end{pmatrix},
\begin{pmatrix}
1&1&1&1&1&-&-&1&1&1&-&-&1&-&1&-\\
1&1&1&1&-&1&-&1&1&-&-&-&1&-&1&1\\
1&1&1&1&-&1&1&-&-&-&1&1&1&-&1&-\\
1&1&1&1&1&-&-&1&-&-&1&1&-&1&-&1\\
1&-&-&1&1&1&1&1&1&-&1&-&1&1&-&-\\
-&1&1&-&1&1&1&1&1&-&1&-&1&1&-&-\\
-&1&1&-&1&1&1&1&1&-&1&-&-&-&1&1\\
1&-&-&1&1&1&1&1&-&1&-&1&-&-&1&1\\
1&1&-&-&1&-&1&-&1&1&1&1&1&-&-&1\\
1&1&-&-&-&1&-&1&1&1&1&1&-&1&1&-\\
-&-&1&1&1&-&1&-&1&1&1&1&-&1&1&-\\
-&-&1&1&1&-&1&-&1&1&1&1&1&-&-&1\\
1&-&1&-&1&1&-&-&1&-&-&1&1&1&1&1\\
-&1&-&1&1&-&-&-&1&1&-&1&1&1&1&1\\
1&-&1&-&-&-&1&1&-&1&1&-&1&1&1&1\\
-&1&-&1&-&-&1&1&1&-&-&1&1&1&1&1
\end{pmatrix}, \text{ and}$$

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

Example A.2. *Using the same three Latin squares shown in Example A.1, we can form three mutually unbiased symmetric Bush-type* $BH(16;4)$ *from the following normalized* $BH(4;4)$

$$\begin{pmatrix}
1&1&1&1\\
1&i&-&j\\
1&-&1&-\\
1&j&-&i
\end{pmatrix}.$$

Denoting $-i=j$*, the following are the four auxiliary matrices of the* $BH(4;4)$

$$\begin{pmatrix}
1&1&1&1\\
1&1&1&1\\
1&1&1&1\\
1&1&1&1
\end{pmatrix},
\begin{pmatrix}
1&i&-&j\\
j&1&i&-\\
-&j&1&i\\
i&-&j&1
\end{pmatrix},
\begin{pmatrix}
1&-&1&-\\
-&1&-&1\\
1&-&1&-\\
-&1&-&1
\end{pmatrix},
\begin{pmatrix}
1&j&-&i\\
i&1&j&-\\
-&i&1&j\\
j&-&i&1
\end{pmatrix}.$$

Note that the normalized $BH(4;4)$ comes from Proposition 3.29. The three matrices obtained using Theorem 6.6 are shown below.

$$\begin{pmatrix}
1&1&1&1&1&i&-j&1&-1&-1&j&-i\\
1&1&1&1&i&-j&1&-1&-1&j&-i&1\\
1&1&1&1&-j&1&i&1&-1&-&i&1&j\\
1&1&1&1&j&1&i&-&-1&-1&i&1&j&-\\
1&i&-j&1&1&1&1&1&j&-i&1&-1&-\\
i&-j&1&1&1&1&1&j&-i&1&-1&-1\\
-&j&1&i&1&1&1&1&-&i&1&j&1&-&-\\
j&1&i&-&1&1&1&1&i&1&j&-&-&1&-&1\\
1&-&1&-&1&j&-&i&1&1&1&1&1&i&-&j\\
-&1&-&1&j&-&i&1&1&1&1&1&i&-&j&1\\
1&-&1&-&-&i&1&j&1&1&1&1&-&j&1&i\\
-&1&-&1&i&1&j&-&1&1&1&1&j&1&i&-\\
1&j&-&i&1&-&1&-&1&i&-&j&1&1&1&1\\
j&-&i&1&-&1&-&1&i&-&j&1&1&1&1&1\\
-&i&1&j&1&-&1&-&-&j&1&i&1&1&1&1\\
i&1&j&-&-&1&-&1&j&1&i&-&1&1&1&1
\end{pmatrix},
\begin{pmatrix}
1&1&1&1&1&j&-i&1&i&-j&1&-&1&-\\
1&1&1&1&j&-i&1&i&-j&1&-&1&-&1\\
1&1&1&1&-i&1&j&-j&1&i&1&-&1&-\\
1&1&1&1&i&1&j&-j&1&i&-&-&1&-&1\\
1&j&-i&1&1&1&1&1&-&1&-&1&i&-&j\\
j&-i&1&1&1&1&1&-&1&-&1&i&-&j&1\\
-&i&1&j&1&1&1&1&1&-&1&-&-&j&1&i\\
i&1&j&-&1&1&1&1&-&1&-&1&j&1&i&-\\
1&i&-&j&1&-&1&-&1&1&1&1&1&j&-&i\\
i&-&j&1&-&1&-&1&1&1&1&1&j&-&i&1\\
-&j&1&i&1&-&1&-&1&1&1&1&-&i&1&j\\
j&1&i&-&-&1&-&1&1&1&1&1&i&1&j&-\\
1&-&1&-&1&i&-&j&1&j&-&i&1&1&1&1\\
-&1&-&1&i&-&j&1&j&-&i&1&1&1&1&1\\
1&-&1&-&-&j&1&i&-&i&1&j&1&1&1&1\\
-&1&-&1&j&1&i&-&i&1&j&-&1&1&1&1
\end{pmatrix},$$

$$\begin{pmatrix}
1&1&1&1&1&-&1&-&1&j&-&i&1&i&-&j\\
1&1&1&1&1&-&1&-&1&j&-&i&1&i&-&j&1\\
1&1&1&1&1&1&-&1&-&-&i&1&j&-&j&1&i\\
1&1&1&1&1&-&1&-&1&i&1&j&-&j&1&i&-\\
1&-&1&-&1&1&1&1&1&i&-&j&1&j&-&i\\
-&1&-&1&1&1&1&1&i&-&j&1&j&-&i&1\\
1&-&1&-&1&1&1&1&-&j&1&i&-&i&1&j\\
-&1&-&1&1&1&1&1&j&1&i&-&i&1&j&-\\
1&j&-&i&1&i&-&j&1&1&1&1&1&-&1&-\\
j&-&i&1&i&-&j&1&1&1&1&1&-&1&-&1\\
-&i&1&j&-&j&1&i&1&1&1&1&1&-&1&-\\
i&1&j&-&j&1&i&-&1&1&1&-&1&-&1\\
1&i&-&j&1&j&-&i&1&-&1&-&1&1&1&1\\
i&-&j&1&j&-&i&1&-&1&-&1&1&1&1&1\\
-&j&1&i&-&i&1&j&1&-&1&-&1&1&1&1\\
j&1&i&-&i&1&j&-&-&1&-&1&1&1&1&1
\end{pmatrix}.$$

In this example, each complex Hadamard matrix has 32 *attached bent sequences. These sequences come from the complex conjugates of the rows of the other two matrices.*

Appendix B: Bent Sequences with Zero

Example B.1. *First, define*

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}.$$

Let ξ be a primitive third root of unity and let

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \xi & \xi^2 \\ 1 & \xi^2 & \xi \end{pmatrix}$$

be the $BH(3;3)$ constructed using Proposition 3.29. Then

$$c_1 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \; c_2 = \begin{pmatrix} 1 & \xi & \xi^2 \\ \xi^2 & 1 & \xi \\ \xi & \xi^2 & 1 \end{pmatrix}, \; c_3 = \begin{pmatrix} 1 & \xi^2 & \xi \\ \xi & 1 & \xi^2 \\ \xi^2 & \xi & 1 \end{pmatrix}$$

are the auxiliary matrices corresponding to H. Define $c_4 = 0_3$ to be the 3×3 all zeroes matrix. The $CW(12, 9; 3)$ constructed from Theorem 6.14 is given as

$$K = \begin{pmatrix} 1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 0 & 0 & 0 \\ 1 & 1 & 1 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 0 & 0 & 0 \\ 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 \\ 0 & 0 & 0 & \xi & 1 & \xi^2 & \xi^2 & 1 & \xi & 1 & 1 & 1 \\ 0 & 0 & 0 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & \xi^2 & \xi \\ \xi^2 & 1 & \xi & 1 & 1 & 1 & 0 & 0 & 0 & \xi & 1 & \xi^2 \\ \xi & \xi^2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \xi^2 & \xi & 1 \\ 1 & \xi^2 & \xi & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi & \xi^2 \\ \xi & 1 & \xi^2 & 0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & 1 & \xi \\ \xi^2 & \xi & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \xi & \xi^2 & 1 \end{pmatrix}.$$

Then using the diagonal blocks of K we define

$$x = \begin{bmatrix} c_1 & c_3 & c_4 & c_2 \end{bmatrix}.$$

Multiplying K by x^* we see

$$Kx^* = \begin{pmatrix} 1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 0 & 0 & 0 \\ 1 & 1 & 1 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 0 & 0 & 0 \\ 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 \\ 0 & 0 & 0 & \xi & 1 & \xi^2 & \xi^2 & 1 & \xi & 1 & 1 & 1 \\ 0 & 0 & 0 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 & 1 \\ 1 & \xi & \xi^2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & \xi^2 & \xi \\ \xi^2 & 1 & \xi & 1 & 1 & 1 & 0 & 0 & 0 & \xi & 1 & \xi^2 \\ \xi & \xi^2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \xi^2 & \xi & 1 \\ 1 & \xi^2 & \xi & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi & \xi^2 \\ \xi & 1 & \xi^2 & 0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & 1 & \xi \\ \xi^2 & \xi & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \xi & \xi^2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & \xi^2 & \xi \\ \xi & 1 & \xi^2 \\ \xi^2 & \xi & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & \xi & \xi^2 \\ \xi^2 & 1 & \xi \\ \xi & \xi^2 & 1 \end{pmatrix} = 3 \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & \xi^2 & \xi \\ \xi & 1 & \xi^2 \\ \xi^2 & \xi & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & \xi & \xi^2 \\ \xi^2 & 1 & \xi \\ \xi & \xi^2 & 1 \end{pmatrix} = 3x^*.$$

Therefore, the columns of x^* give us three self-dual bent sequences attached to K.

Example B.2. *Using the same $BH(3, 3)$ from Example B.1 we form the same four auxiliary matrices c_1, c_2, c_3 and $c_4 = 0_3$ as shown previously. Using the set of four $MSLS(4)$ from Examples 4.19 and A.1 we apply Theorem 6.16 to construct the fol-*

lowing three mutually unbiased $CW(12, 9; 3)$.

$$\begin{pmatrix}
1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 0 & 0 & 0 \\
1 & 1 & 1 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 0 & 0 & 0 \\
1 & 1 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 \\
1 & \xi & \xi^2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & \xi^2 & \xi \\
\xi^2 & 1 & \xi & 1 & 1 & 1 & 0 & 0 & 0 & \xi & 1 & \xi^2 \\
\xi & \xi^2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & \xi^2 & \xi & 1 \\
1 & \xi^2 & \xi & 0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi & \xi^2 \\
\xi & 1 & \xi^2 & 0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & 1 & \xi \\
\xi^2 & \xi & 1 & 0 & 0 & 0 & 1 & 1 & 1 & \xi & \xi^2 & 1 \\
0 & 0 & 0 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 \\
0 & 0 & 0 & \xi & 1 & \xi^2 & \xi^2 & 1 & \xi & 1 & 1 & 1 \\
0 & 0 & 0 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 1 & 1 & 1
\end{pmatrix}, \quad
\begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 1 & \xi & \xi^2 & 1 & \xi^2 & \xi \\
1 & 1 & 1 & 0 & 0 & 0 & \xi^2 & 1 & \xi & \xi & 1 & \xi^2 \\
1 & 1 & 1 & 0 & 0 & 0 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 \\
0 & 0 & 0 & 1 & 1 & 1 & \xi & 1 & \xi^2 & \xi^2 & 1 & \xi \\
0 & 0 & 0 & 1 & 1 & 1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 1 \\
1 & \xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 1 & 1 & 0 & 0 & 0 \\
\xi^2 & 1 & \xi & \xi & 1 & \xi^2 & 1 & 1 & 1 & 0 & 0 & 0 \\
\xi & \xi^2 & 1 & \xi^2 & \xi & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & \xi^2 & \xi & 1 & \xi & \xi^2 & 0 & 0 & 0 & 1 & 1 & 1 \\
\xi & 1 & \xi^2 & \xi^2 & 1 & \xi & 0 & 0 & 0 & 1 & 1 & 1 \\
\xi^2 & \xi & 1 & \xi & \xi^2 & 1 & 0 & 0 & 0 & 1 & 1 & 1
\end{pmatrix}, \text{ and}$$

$$\begin{pmatrix}
1 & 1 & 1 & 1 & \xi^2 & \xi & 0 & 0 & 0 & 1 & \xi & \xi^2 \\
1 & 1 & 1 & \xi & 1 & \xi^2 & 0 & 0 & 0 & \xi^2 & 1 & \xi \\
1 & 1 & 1 & \xi^2 & \xi & 1 & 0 & 0 & 0 & \xi & \xi^2 & 1 \\
1 & \xi^2 & \xi & 1 & 1 & 1 & 1 & \xi & \xi^2 & 0 & 0 & 0 \\
\xi & 1 & \xi^2 & 1 & 1 & 1 & \xi^2 & 1 & \xi & 0 & 0 & 0 \\
\xi^2 & \xi & 1 & 1 & 1 & 1 & \xi & \xi^2 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & \xi & \xi^2 & 1 & 1 & 1 & 1 & \xi^2 & \xi \\
0 & 0 & 0 & \xi^2 & 1 & \xi & 1 & 1 & 1 & \xi & 1 & \xi^2 \\
0 & 0 & 0 & \xi & \xi^2 & 1 & 1 & 1 & 1 & \xi^2 & \xi & 1 \\
1 & \xi & \xi^2 & 0 & 0 & 0 & 1 & \xi^2 & \xi & 1 & 1 & 1 \\
\xi^2 & 1 & \xi & 0 & 0 & 0 & \xi & 1 & \xi^2 & 1 & 1 & 1 \\
\xi & \xi^2 & 1 & 0 & 0 & 0 & \xi^2 & \xi & 1 & 1 & 1 & 1
\end{pmatrix}.$$