RECURSIVELY-CONSTRUCTED UNIT HADAMARD MATRICES: THEIR EXCESS AND A RESULTING FAMILY OF BIBDS

KAI FENDER

Honours Thesis

Department of Mathematics and Computer Science
University of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

RECURSIVELY-CONSTRUCTED UNIT HADAMARD MATRICES: THEIR EXCESS AND A RESULTING FAMILY OF BIBDS

KAI FENDER

Date of Defense: April 13, 2016, 12:00 PM

Dr. Hadi Kharaghani Supervisor	Professor	Ph.D.
Dr. Amir Akbary-Majdabadno Committee Member	Professor	Ph.D.

Abstract

A *unit Hadamard matrix* is a square matrix H with unimodular entries and mutually orthogonal row vectors. If the entries of H are all roots of unity, H is a *Butson Hadamard matrix*. If the entries of H are all 1 or -1, H is a *Hadamard matrix*. In the second half of the twentieth century interest arose in finding the maximum modulus of the sum of the entries, or *excess*, of a unit Hadamard matrix. In this thesis, we will give a recursive construction for infinite classes of Hadamard, Butson Hadamard and unit Hadamard matrices. We will proceed to use these classes to obtain several lower bounds for the maximal excess problem. Finally, we will show that some of our recursively-constructed Hadamard matrices can be used to construct an infinite class of *balanced incomplete block designs*, another important combinatorial object.

Contents

Chapter 1

Introduction

Hadamard matrices were first studied almost one hundred fifty years ago by James Sylvester. In 1867, Sylvester gave a construction for an interesting infinite class of Hadamard matrices known as the *Sylvester matrices* [21]. After Sylvester, the next major contribution to the study of Hadamard matrices came from the analyst Jacques Hadamard, after whom Hadamard matrices are named. Hadamard was led to Hadamard matrices by attempting to find the maximum determinant of matrices of complex numbers with modulus less than a given positive constant A. In an 1893 paper [10], Hadamard placed an upper bound on the determinant and as an example showed that if $A = 1$, the bound is met by $n \times n$ Vandermonde matrices formed using the n roots of the polynomial $x^n - 1$. Furthermore, he showed that when $A = 1$, this bound is met by real matrices if and only if the matrix is what we now call a Hadamard matrix. To finish his paper, Hadamard gave the first examples of Hadamard matrices of orders 12 and 20, and suggested that the problem of finding (± 1)-matrices with maximal determinants is an interesting one. This problem gave rise to the famous *Hadamard conjecture*, which asserts that there is a Hadmard matrix of order n whenever n is a multiple of 4. To this day the Hadamard conjecture has parried the attacks of many brilliant mathematicians, and remains the most important open question in the study of Hadamard matrices.

Not only did the advent of Hadamard matrices create a field of study fascinating in its own right, but it also introduced a branch of combinatorics that has found applications in areas such as telecommunications, quantum computing, theoretical physics, and experimen-

tal design. As such, the study of Hadamard matrices has garnered not only the interest of mathematicians, but of engineers and physicists as well. For surveys of some applications of Hadamard matrices, we refer the reader to [8, 20].

Since their introduction by Sylvester so many years ago, Hadamard matrices have been generalized in many different ways by many different authors. In addition to Hadamard matrices, this thesis is concerned with two such generalizations: Butson Hadamard matrices [3] and unit Hadamard matrices [22]. These generalizations share most of the key properties of Hadamard matrices, but with loosened requirements on their entries.

This thesis is divided into two main parts: background (Chapter 2) and original results (Chapter 3). More specifically, in Chapter 2 we survey important foundational concepts pertaining to Hadamard matrices, Butson Hadamard matrices, unit Hadamard matrices, and the properties of these matrices such as their structure and excess. Chapter 3 presents the results of the research I began alongside Hadi Kharaghani and Dakota Duffy in the summer of 2015 and continued into the fall and winter myself. This research is based on the combinatorial applications of pairs of matrices satisfying two key properties. Such pairs of matrices will be dubbed q-suitable. Herein, we will see that q-suitable pairs of matrices can be exploited to obtain Hadamard matrices, Butson Hadamard matrices, and unit Hadamard matrices. We will then introduce a recursive construction involving Jacobsthal matrices and pairs of q-suitable matrices. The reader may find this recursive construction reminiscent of the recursive techniques used by other authors to study combinatorial designs [6, 11]. Here, however, we apply the techniques in a novel way to obtain constructions for an infinite class of BIBDs, and for infinite classes of Hadamard matrices, Butson Hadamard matrices, and unit Hadamard matrices with certain interesting properties.

1.1 Summary of Main Results

In this section we will present an overview of Chapter 3, which contains the original results in this thesis. Before giving the overview, it should be noted that with the exception

of Lemma 3.2.8, the results in Chapter 3 are original. We would also like to note that the results of Sections 3.1 and 3.3 were obtained independently by the author, while the results of Section 3.2 were obtained in collaboration with Hadi Kharaghani and Dakota Duffy.

Let q be an odd prime power. In Section 3.1 we give the definition of a q-suitable pair of matrices. Next, assuming the existence of a q-suitable pair (A,B) of $n \times n$ matrices, we present two recursive constructions (one for $q \equiv 3 \pmod 4$ and one for $q \equiv 1 \pmod 4$) for unit Hadamard matrices of order $nq^m(q+1)$ for each integer $m \geq 0$. Of particular interest, we show that if A and B are $(\pm 1, \pm i)$-matrices, then both of our constructions yield BH$(nq^m(q+1),4)$'s, while if A and B are (± 1)-matrices, then our construction for $q \equiv 3 \pmod 4$ yields Hadamard matrices. To conclude the section, assuming A and B are (± 1)-matrices, we give a recursive construction for a unit Hadamard matrix of order nq^m for each integer $m \geq 0$, regardless of the residue of q modulo 4, and we show that these unit Hadamard matrices are unreal BH$(nq^m,6)$'s or unreal BH$(nq^m,12)$'s when $q = 3$.

Section 3.2 is devoted to studying the combinatorial fruits of a basic pair of q-suitable matrices. Using this pair, we will present several interesting results pertaining to the existence, structure, and excess of Hadamard, Butson Hadamard, and unit Hadamard matrices. More specifically, in Section 3.2.1, we give a construction for a Hadamard matrix of order $q^m(q+1)$ whenever $m \geq 0$ is an integer and $q \equiv 3 \pmod 4$ is a prime power. Next, we will use these matrices to derive two lower bounds for the maximal excess problem:

$$\sigma_R(q^{2m}(q+1)) \geq q^{3m}(3q-1)$$

and

$$\sigma_R(q^{2m+1}(q+1)) \geq q^{3m+2}(q+1) + 2q^{m+2}(q^m-1),$$

where $\sigma_R(n)$ denotes the maximum excess of all Hadamard matrices of order n. Moreover, we will show that when m is even and $q = 3$, the constructed matrices are of maximum

excess and regular, giving

$$\sigma_R(4\cdot 3^{2m}) = (4\cdot 3^{2m})^{3/2}.$$

In Section 3.2.2, we construct an unreal, multicirculant, maximal-excess unit Hadamard matrix of order q^m for each integer $m \geq 0$ and prime power $q \equiv 3 \pmod 4$, and we show that if $q = 3$, then this matrix is a BH$(3^m, 6)$ or a BH$(3^m, 12)$.

In Section 3.2.3, we give an application of the basic pair of q-suitable matrices given at the beginning of Section 3.2. Namely, we construct a $(q^{2m+2}, \frac{q^{m+1}(q^{m+1}-1)}{2}, \frac{q^m(q^{m+1}-2)(q+1)}{4})$-design for each integer $m \geq 0$ and prime power $q \equiv 3 \pmod 4$.

In Section 3.3, we assume $q \equiv 3 \pmod 4$ is a prime power, $m \geq 0$ is an integer, and that there exists a symmetric, standardized Hadamard matrix of order $q+5$. Under these assumptions, we present constructions for a Hadamard matrix of order $q^m(q+1)(q+4)$, an unreal unit Hadamard matrix of order $q^m(q+4)$, an unreal BH$(7\cdot 3^m, 6)$, and an unreal BH$(7\cdot 3^m, 12)$. Finally, we use the constructed Hadamard matrices to derive two lower bounds for the maximal excess problem:

$$\sigma_R(q^{2m}(q+1)(q+4)) \geq q^{3m}(q+1)(q+2)(q+4)$$

and

$$\sigma_R(q^{2m+1}(q+1)(q+4)) \geq q^{3m+2}(q+4)(3q+3).$$

1.2 Notation

Many undergraduate, master's, and Ph.D. theses make use of a very good idea: to introduce common mathematical notation in a brief section in the introduction. We will borrow this idea, as enough recurring pieces of mathematical notation will be used that it will be beneficial to introduce them all in one place for the reader's reference, as opposed to scattering their introductions throughout the thesis. As is standard, I_n will be used to denote the $n \times n$ identity matrix. Likewise, the use of J_n will be restricted to denoting the $n \times n$

all-ones matrix. We will use Q and Q_q solely to denote Jacobsthal matrices. The letters H, K and L will be used only to denote Hadamard matrices or their generalizations, such as unit Hadamard matrices and Butson Hadamard matrices. The transpose of a matrix A will be denoted A^T, and its conjugate-transpose, also known as its Hermitian transpose, will be denoted A^*. In general, capital letters will be used as variables exclusively to denote matrices or sets. When writing out matrices explicitly, we will use "$-$" as a shorthand for "-1". For example, we write

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

in lieu of

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

Unless otherwise stated, one should assume that an $n \times m$ matrix's rows and columns are indexed from 1 to n and 1 to m respectively. Finally, j_n will be used to denote the $1 \times n$ all-ones row vector, p will always represent a prime number, q will be used exclusively to refer to prime powers, and $\mathrm{GF}(q)$ will denote the finite field of order q.

Chapter 2

Background

We discussed the history of Hadamard matrices in Chapter 1. It is time to give their formal definition.

Definition 2.0.1. A *Hadamard matrix* of order n is an $n \times n$ (± 1)-matrix H such that $HH^T = nI_n$.

Given an $n \times n$ Hadamard matrix H, the condition $HH^T = nI_n$ is equivalent to requiring that the row vectors of H are pairwise orthogonal. This can be verified by way of the following examples.

Example 2.0.1. The following are Hadamard matrices of orders 1, 2, and 4:

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

2.1 Equivalence of Hadamard Matrices

Looking at the examples of Hadamard matrices in the previous section, one notices that not only are the row vectors of these matrices pairwise orthogonal, but their column vectors are as well. In fact, this is true of all Hadamard matrices, as we will see from the proof of next proposition.

Proposition 2.1.1. *If H is a Hadamard matrix of order n, then so is H^T.*

Proof. Since $HH^T = nI_n$, we see that $H^{-1} = \frac{1}{n}H^T$. It follows that

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

□

The transpose is not the only operation we can perform on a Hadamard matrix to obtain a second Hadamard matrix. Since the row vectors of any Hadamard matrix are pairwise orthogonal, it's not hard to see that if we negate a row or column of a Hadamard matrix, then the resulting matrix also has pairwise orthogonal rows and is therefore a Hadamard matrix. Likewise, if we permute the rows or columns of a Hadamard matrix then the resulting matrix is easily seen to be a Hadamard matrix. These observations are summarized somewhat more formally as follows.

Proposition 2.1.2. *Let H be a Hadamard matrix of order n and let P_1 and P_2 be two signed $n \times n$ permutation matrices. Then P_1HP_2 is a Hadamard matrix of order n.*

Proof. Since P_1 and P_2 are signed permutation matrices we have $P_1P_1^T = P_2P_2^T = I_n$. Using this observation we note

$$(P_1HP_2)(P_1HP_2)^T = P_1HP_2P_2^TH^TP_1^T = P_1HH^TP_1^T = nP_1P_1^T = nI_n.$$

□

Proposition 2.1.2 has given us a method of transforming one Hadamard matrix of order n into another via row and column permutations and negations. This motivates a definition.

Definition 2.1.3. We call two $n \times n$ Hadamard matrices H and K *equivalent* if there exist two signed $n \times n$ permutation matrices P_1 and P_2 such that $H = P_1KP_2$. The *equivalence class* of a Hadamard matrix is the set of all Hadamard matrices with which it is equivalent.

[ht]

Table 2.1: Number of equivalence classes of Hadamard matrices of order $n \leq 32$

n	# Matrices
1	1
2	1
4	1
8	1
12	1
16	5
20	3
24	60
28	487
32	13710027

Put more simply, two Hadamard matrices are equivalent if one can be obtained from the other by a series of row and column permutations and negations. The notion of equivalence of Hadamard matrices begs a simple question: how many distinct equivalence classes of Hadamard matrices are there for a given order? This problem has proved an arduous one, and for all but the smallest orders is virtually intractable without the aid of computer searches. The progress made so far is summarized in Table 2.1. The most recent order to be completely classified is 32. This classification was done by Kharaghani and Tayfey-Rezaie [16], and involved a nine-month-long search done with a computer grid.

While perusing Table 2.1, the reader may have noticed that aside from orders 1 and 2, all orders of Hadamard matrices listed were a multiple of 4. It turns out that with a little work we can show this is a necessary condition for the existence of a Hadamard matrix. The proof of this fact is left until the next section, and will make use of the next definition and the subsequent proposition.

Definition 2.1.4. We say that a Hadamard matrix is *standardized* if its first row and its first column are composed entirely of ones.

Given a Hadamard matrix, we can first negate all rows whose leftmost entry is -1, then negate all columns whose uppermost entry is -1. Doing so, we obtain a standardized

Hadamard matrix. This establishes the following proposition.

Proposition 2.1.1. *Each Hadamard matrix is equivalent to a standardized Hadamard matrix.*

2.2 Existence of Hadamard Matrices

After defining Hadamard matrices, perhaps the most natural question to ask is for which orders a Hadamard matrix can exist. In the previous section we alluded briefly to a necessary condition for the existence of Hadamard matrices. We are now ready to prove that condition.

Proposition 2.2.1. *If there is a Hadamard matrix of order n, then n is either 1, 2, or a positive multiple of 4.*

Proof. We established in Example 2.0.1 that there are Hadamard matrices of orders 1 and 2, so consider a Hadamard matrix H of order $n > 2$. Proposition 2.1.1 tells us that we may assume without loss of generality that H is standardized. From here, permute the columns of H until the first a columns have 1, 1, 1 as their first three entries, the next b columns have 1, 1, -1 as their first three entries, the next c columns have 1, -1, 1 as their first three entries, and the final d columns have 1, -1, -1 as their first three entries. This is summarized visually in the following image of the first three rows of H.

$$\begin{array}{c} \overbrace{\qquad\quad}^{a \text{ columns}}\overbrace{\qquad\quad}^{b \text{ columns}}\overbrace{\qquad\quad}^{c \text{ columns}}\overbrace{\qquad\quad}^{d \text{ columns}} \\ \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1 & 1 & - & - & \cdots & - & - & - & - & \cdots & - & - \\ 1 & 1 & \cdots & 1 & 1 & - & - & \cdots & - & - & 1 & 1 & \cdots & 1 & 1 & - & - & \cdots & - & - \\ \vdots & & & \vdots & & & \vdots & & & \vdots & & \vdots & & & \vdots & & \vdots & & & \vdots \end{pmatrix} \end{array}$$

From here, the fact that the order of H is n together with the orthogonality of the rows of H

yields a system of equations:

$$\begin{cases} a+b+c+d=n & \text{(The order of } H \text{ is } n\text{)} \\ a+b-c-d=0 & \text{(Rows one and two are orthogona)} \\ a-b+c-d=0 & \text{(Rows one and three are orthogonal)} \\ a-b-c+d=0 & \text{(Rows two and three are orthogonal)} \end{cases}$$

A basic computation shows that this system of linear equations has the unique solution $a=b=c=d=n/4$. Of course a,b,c, and d must be integers, so n is a multiple of 4. □

Having found that n being 1, 2, or a multiple of 4 is a necessary condition for the existence of a Hadamard matrix of order n, one may wonder whether this condition is also sufficient. The answer to this question is the most important open problem in the study of Hadamard matrices. It is believed that the condition is indeed sufficient, which brings us to the following well known conjecture.

Conjecture 2.2.2 (The Hadamard Conjecture)**.** There is a Hadamard matrix of order n whenever n is 1, 2, or a multiple of 4.

Recently, a significant milestone was reached in the verification of the Hadamard conjecture. Until 2004, order 428 was the smallest order for which Hadamard matrices had eluded discovery. In 2004, Kharaghani and Tayfeh-Rezaie became the first to discover a Hadamard matrix of order 428 [15], making 668 the smallest order for which no Hadamard matrix is known.

In the next sections we will present some important historical milestones that have helped verify the Hadamard conjecture, including those made by Sylvester [21], Hadamard [10], and Paley [19].

2.3 Sylvester's and Hadamard's Constructions of Hadamard Matrices

Having defined Hadamard matrices and introduced some of their most fundamental concepts, we now turn our attention to the construction of Hadamard matrices. In this section we will present two important constructions discovered while the study of Hadamard matrices was in its infancy. Namely, we will introduce results obtained by Sylvester in 1867 [21] and by Hadamard in 1893 [10]. Without further ado, let us delve into the discoveries made by Sylvester, who was the first mathematician to consider Hadamard matrices.

Theorem 2.3.1 (Sylvester, [21])**.** *Let H be 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. Elementary matrix multiplication gives the result:

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

□

Since (1) is a Hadamard matrix of order 1, we can apply Theorem 2.3.1 m times to (1) to obtain a Hadamard matrix of order 2^m. This proves the following:

Corollary 2.3.1 (Sylvester, [21])**.** *If m is a nonnegative integer, then there is a Hadamard matrix of order 2^m.*

The matrices of order 2^m obtained from Sylvester's construction are known as the *Sylvester Hadamard matrices*. Although simple to describe, this infinite class of matrices continues to prove itself worthy of study to this day. For example, recent results pertaining to Sylvester Hadamard matrices can be found in [18, 1].

Despite Hadamard matrices being his namesake, Jacques Hadamard did not study Hadamard matrices until about two-and-a-half decades after Sylvester. In fact, Hadamard was led to study Hadamard matrices not for their combinatorial properties, but in an attempt to determine the largest possible absolute value of the determinant of a square matrix whose entries are chosen from some set of complex numbers. In studying this problem, Hadamard showed that the absolute value of the determinant of an $n \times n$ matrix M whose entries are from the set $\{z \in \mathbb{C} : |z| \leq 1\}$ never exceeds $n^{n/2}$, and that when M is a (± 1)-matrix, this bound is met if and only if M is a Hadamard matrix [10]. Hadamard's contributions to the study of Hadamard matrices don't end with determinants. He also generalized Sylvester's construction for Hadamard matrices, as we will show shortly. First, however, we require a prerequisite definition: the Kronecker product.

Definition 2.3.2. Let $A = (a_{ij})$ be an $n \times m$ matrix and let $B = (b_{ij})$ be a $r \times s$ matrix. The *Kronecker product* $A \otimes B$ of A and B is the $nr \times ms$ block matrix

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

Example 2.3.3. Here is the Kronecker product of two matrices:

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

It is interesting to note that the matrices in this example are all Hadamard matrices. Shortly, we will see that in fact the Kronecker product of two Hadamard matrices is always another Hadamard matrix.

Several fundamental properties of the Kronecker product are readily verified. For instance, the Kronecker product is bilinear, associative, and it satisfies the following three equations, assuming A, B, C, D are of the appropriate dimensions to discuss the products AC and BD.

(1) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$

(2) $(A \otimes B)^T = A^T \otimes B^T$

(3) $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

The proof of these properties is left as an exercise for the reader.

Using the Kronecker product, Hadamard generalized Sylvester's construction.

Theorem 2.3.4 (Hadamard, [10])**.** *Let H be a Hadamard matrix of order n and K a Hadamard matrix of order m. Then $H \otimes K$ is a Hadamard matrix of order nm.*

Proof. Using the properties of the Kronecker product, we note:

$$(H \otimes K)(H \otimes K)^T = (HH^T) \otimes (KK^T) = (nI_n) \otimes (mI_m) = nmI_{nm}.$$

□

It should be noted that Hadamard did not state Theorem 2.3.4 in terms of Kronecker products. However, as the study of Hadamard matrices evolved, Kronecker products have proved themselves an invaluable tool for construction. As such, we elected to present Hadamard's theorem using Kronecker products in lieu of Hadamard's original statement.

2.4 Jacobsthal Matrices and Paley's Construction for Hadamard Matrices

In the previous section, we saw that when Sylvester introduced the notion of Hadamard matrices, he presented a construction for an infinite class of Hadamard matrices of order 2^m, where $m \geq 0$. The first possible orders of Hadamard matrices not covered by this class are 12 and 20. In 1893, Hadamard concluded his paper on the maximal determinant problem by describing Hadamard matrices of orders 12 and 20 [10]. However, his matrices left something to be desired, as he did not employ any versatile construction to obtain the matrices of orders 12 and 20, and instead presented the matrices as if out of thin air. It was not until 1933 that Paley discovered a truly versatile construction that could be used to obtain Hadamard matrices of orders 12 and 20, amongst infinitely many other orders [19]. In doing so, Paley cleverly used quadratic characters and finite fields to build Hadamard matrices. Paley's use of finite fields made him the first to discover a deep interplay between algebra and Hadamard matrices, laying the foundations for much of the research conducted in the 83 years since the publication of his important paper. As such, before presenting Paley's construction, we must first familiarize ourselves with the tools from field theory required by the construction.

Definition 2.4.1. Let q be a prime power. We say that $a \in \mathrm{GF}(q)$ is a *quadratic residue in* $GF(q)$ if it is nonzero and there is some $b \in \mathrm{GF}(q)$ such that $a = b^2$. If a is nonzero but no such b exists, then a is called a *quadratic non-residue in* $GF(q)$. If $a = 0$, then a is neither a quadratic residue nor a quadratic non-residue.

Remark 2.4.2. It should be noted that the choice to define 0 as neither a quadratic residue nor

a quadratic non-residue is largely a matter of convention. Some authors choose to include 0 in the list of quadratic residues, but in order to simplify the statement of subsequent theorems and definitions we do not.

The next proposition is a generalization to finite fields of a result from elementary number theory. It will be of use shortly when we introduce *Jacobsthal matrices*.

Proposition 2.4.3. *Let q be an odd prime power. Then there are $\frac{q-1}{2}$ quadratic residues and $\frac{q-1}{2}$ quadratic non-residues in $GF(q)$.*

Proof. Since each of the $q-1$ nonzero elements of $\mathrm{GF}(q)$ is either a quadratic residue or a quadratic non-residue, we need only show that there are $\frac{q-1}{2}$ quadratic residues in $\mathrm{GF}(q)$. Let $\mathrm{GF}(q)^*$ denote the multiplicative group of nonzero elements of $\mathrm{GF}(q)$. Define $\phi : \mathrm{GF}(q)^* \to \mathrm{GF}(q)^*$ by $\phi(a) = a^2$. Then ϕ is a group homomorphism, so by the First Isomorphism Theorem

$$\mathrm{GF}(q)^* / \ker\phi \cong \phi(\mathrm{GF}(q)^*).$$

From here, Lagrange's theorem tells us

$$|\phi(GF(q)^*)| = \frac{|\mathrm{GF}(q)^*|}{|\ker\phi|}.$$

Observe that $\ker\phi = \{\pm 1\}$. Indeed, $\phi(a) = 1$ if and only if $(a-1)(a+1) = 0$, and since $\mathrm{GF}(q)$ has no zero divisors, we must have $a = \pm 1$. Thus

$$|\phi(\mathrm{GF}(q)^*)| = \frac{|\mathrm{GF}(q)^*|}{|\{\pm 1\}|} = \frac{q-1}{2}.$$

Noting that $\phi(\mathrm{GF}(q)^*)$ is precisely the set of all quadratic residues in $\mathrm{GF}(q)$, the result now follows. □

Definition 2.4.4. Let q be a prime power. The *quadratic character on GF*(q) is the function $\chi_q : \mathrm{GF}(q) \to \mathbb{Z}$ defined by

$$\chi_q(a) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue in GF}(q) \\ -1 & \text{if } a \text{ is a quadratic non-residue in GF}(q) \\ 0 & \text{if } a = 0. \end{cases}$$

Definition 2.4.5. Let q be an odd prime power and let $\mathrm{GF}(q) = \{a_1, \ldots, a_q\}$. A *Jacobsthal matrix* is a $q \times q$ matrix $Q_q = (q_{ij})$ whose entries are defined by

$$q_{ij} = \chi_q(a_i - a_j).$$

Remark 2.4.6. It should be noted that in the above definition we used the phrase *a Jacobsthal matrix* as opposed to *the Jacobsthal matrix* for good reason. Jacobsthal matrices of order q are not unique, and instead vary depending on the order in which you index the elements of $\mathrm{GF}(q)$.

Before we proceed, it is instructive to examine some examples of Jacobsthal matrices.

Example 2.4.7 (A Jacobsthal Matrix of Order 3)**.** Since 3 is prime, we can work with $\mathbb{Z}_3$ to construct a Jacobsthal matrix of order 3. Observe that

$$1^2 \equiv 2^2 \equiv 1 \pmod 3.$$

It follows that the only quadratic residue in $\mathbb{Z}_3$ is 1, and the only non-residue is 2. Therefore,

indexing the rows and columns of Q_3 by 0, 1, and 2, we obtain

$$Q_3 = \begin{matrix} \\ 0 \\ 1 \\ 2 \end{matrix} \begin{matrix} \begin{matrix} 0 & 1 & 2 \end{matrix} \\ \begin{pmatrix} \chi_3(0) & \chi_3(-1) & \chi_3(-2) \\ \chi_3(1) & \chi_3(0) & \chi_3(-1) \\ \chi_3(2) & \chi_3(1) & \chi_3(0) \end{pmatrix} \end{matrix} = \begin{matrix} \\ 0 \\ 1 \\ 2 \end{matrix} \begin{matrix} \begin{matrix} 0 & 1 & 2 \end{matrix} \\ \begin{pmatrix} 0 & - & 1 \\ 1 & 0 & - \\ - & 1 & 0 \end{pmatrix} \end{matrix}$$

We will make use of the following important properties of Jacobsthal matrices throughout the remainder of this thesis.

Theorem 2.4.8. *Let q be an odd prime power. Then*

(1) If $q \equiv 1 \pmod 4$, then Q_q is symmetric.

(2) If $q \equiv 3 \pmod 4$, then Q_q is antisymmetric.

(3) $J_q Q_q = Q_q J_q = 0$.

(4) $Q_q Q_q^T = qI_q - J_q$.

Proof. Before we proceed, we leave it to the reader to verify that χ_q is a homomorphism and that

$$\chi_q(-1) = \begin{cases} 1 & \text{If } q \equiv 1 \pmod 4 \\ -1 & \text{If } q \equiv 3 \pmod 4. \end{cases} \tag{2.1}$$

Using these facts, we prove the theorem. Let $Q_q = (q_{ij})$ and let $\mathrm{GF}(q) = \{a_1, \ldots, a_q\}$.

(1) If $q \equiv 1 \pmod 4$, then using the fact that χ_q is a homomorphism together Equation (2.1), we obtain

$$q_{ij} = \chi_q(a_i - a_j) = \chi_q(-1)\chi_q(a_j - a_i) = \chi_q(a_j - a_i) = q_{ji}.$$

Thus Q_q is symmetric.

(2) Similarly, if $q \equiv 3 \pmod 4$, then

$$q_{ij} = \chi_q(a_i - a_j) = \chi_q(-1)\chi_q(a_j - a_i) = -\chi_q(a_j - a_i) = -q_{ji}.$$

Thus Q_q is antisymmetric.

(3) The definition of Jacobsthal matrices shows that each column sum and row sum of Q_q must be equal to

$$\sum_{a \in \mathrm{GF}(q)} \chi_q(a).$$

On the other hand, Proposition 2.4.3 tells us half of the nonzero elements of $\mathrm{GF}(q)$ are quadratic residues and half are non-residues. Together with the fact that $\chi_q(0) = 0$, this implies

$$\sum_{a \in \mathrm{GF}(q)} \chi_q(a) = 0.$$

Thus each row and column sum of Q_q is zero. It is now immediate that

$$J_q Q_q = Q_q J_q = 0.$$

(4) Let r_i and r_j denote the i^{th} and j^{th} row vectors of Q_q. Since there are $q-1$ nonzero entries in each row of Q_q, each of which is either 1 or -1, we see that if $i = j$, then

$r_i \cdot r_j = q-1$. Next, assume $i \neq j$. Then

$$\begin{aligned}
r_i \cdot r_j &= \sum_{b \in \mathrm{GF}(q)} \chi_q(a_i - b)\chi_q(a_j - b) \\
&= \sum_{c \in \mathrm{GF}(q)} \chi_q(c)\chi_q(a_j - (a_i - c)) && \text{(Where } c = a_i - b\text{)} \\
&= \sum_{c \in \mathrm{GF}(q)\setminus\{0\}} \chi_q(c)\chi_q(a_j - (a_i - c)) && \text{(Since } \chi_q(0) = 0\text{)} \\
&= \sum_{c \in \mathrm{GF}(q)\setminus\{0\}} (\chi_q(c))^2\chi_q(1 + c^{-1}(a_j - a_i)) && \text{(}c^{-1} \text{ exists since } c \neq 0\text{)} \\
&= \sum_{c \in \mathrm{GF}(q)\setminus\{0\}} \chi_q(1 + c^{-1}(a_j - a_i)). && \text{(Since } \chi_q(c) \in \{\pm 1\}\text{)}
\end{aligned}$$

Now, since $a_j \neq a_i$, as c runs through all the nonzero elements of $\mathrm{GF}(q)$, the term $c^{-1}(a_j - a_i)$ runs through all nonzero elements of $\mathrm{GF}(q)$. Therefore,

$$\begin{aligned}
r_i \cdot r_j &= \sum_{d \in \mathrm{GF}(q)\setminus\{1\}} \chi_q(d) \\
&= \left(\sum_{d \in \mathrm{GF}(q)} \chi_q(d) \right) - \chi_q(1) \\
&= -\chi_q(1) && \text{(By Proposition 2.4.3)} \\
&= -1. && \text{(Since 1 is a quadratic residue for any } q\text{)}
\end{aligned}$$

In summary, we have shown

$$r_i \cdot r_j = \begin{cases} q-1 & \text{if } i = j \\ -1 & \text{otherwise.} \end{cases}$$

It follows immediately that $Q_q Q_q^T = qI_q - J_q$.

□

With the four properties of Jacobsthal matrices described in the above theorem added

to our toolkit, we can now present Paley's two constructions for Hadamard matrices.

Theorem 2.4.9 (Paley, [19]). *Let $q \equiv 3 \pmod 4$ be a prime power. Then*

$$I_{q+1} + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q_q \end{pmatrix}$$

is a Hadamard matrix of order $q+1$, where j_q denotes the $1 \times q$ all-ones matrix.

Proof. With Theorem 2.4.8 under our belts, the proof becomes a straightforward calculation.

$$\begin{aligned}
&\left(I_{q+1} + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q_q \end{pmatrix}\right)\left(I_{q+1} + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q_q \end{pmatrix}\right)^T \\
&= I_{q+1} + \begin{pmatrix} 0 & -j_q \\ j_q^T & Q_q^T \end{pmatrix} + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q_q \end{pmatrix} + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q_q \end{pmatrix}\begin{pmatrix} 0 & -j_q \\ j_q^T & Q_q^T \end{pmatrix} \\
&= I_{q+1} + \begin{pmatrix} 0 & -j_q \\ j_q^T & -Q_q \end{pmatrix} + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q_q \end{pmatrix} + \begin{pmatrix} q & 0 \\ 0 & J_q + (qI_q - J_q) \end{pmatrix} \qquad \text{(By Theorem 2.4.8)} \\
&= (q+1)I_{q+1}.
\end{aligned}$$

□

Theorem 2.4.10 (Paley, [19]). *Let $q \equiv 1 \pmod 4$ be a prime power. Then*

$$\begin{pmatrix} 1 & - \\ - & - \end{pmatrix} \otimes I_{q+1} + \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} \otimes \begin{pmatrix} 0 & j_q \\ j_q^T & Q_q \end{pmatrix}$$

is a Hadamard matrix of order $2(q+1)$, where j_q denotes the $1 \times q$ all-ones matrix.

Proof. Let H denote the matrix in the statement of the theorem, let

$$L = \begin{pmatrix} 1 & - \\ - & - \end{pmatrix}, \qquad \text{and let} \qquad K = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}.$$

Now, observing that Q_q is symmetric by Theorem 2.4.8 and that $LK^T = -KL^T$, we obtain

$$\begin{aligned} HH^T &= \left(L \otimes I_{q+1} + K \otimes \begin{pmatrix} 0 & j_q \\ j_q^T & Q_q \end{pmatrix} \right) \left(L \otimes I_{q+1} + K \otimes \begin{pmatrix} 0 & j_q \\ j_q^T & Q_q \end{pmatrix} \right)^T \\ &= (LL^T) \otimes I_{q+1} + (KK^T) \otimes \left(\begin{pmatrix} 0 & j_q \\ j_q^T & Q_q \end{pmatrix} \begin{pmatrix} 0 & j_q \\ j_q^T & Q_q^T \end{pmatrix} \right) \\ &= 2I_2 \otimes I_{q+1} + 2I_2 \otimes \begin{pmatrix} q & 0 \\ 0 & J_q + (qI_q - J_q) \end{pmatrix} \\ &= 2I_{2(q+1)} + 2I_2 \otimes (qI_{q+1}) \\ &= 2(q+1)I_{2(q+1)}. \end{aligned}$$

□

2.5 The Structure of Jacobsthal Matrices

Recall from the previous section our example of a Jacobsthal matrix of order 3:

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

This matrix enjoys a nice structure; each row is the same as the previous but with every element shifted one position to the right (with entries in the last column being wrapped

around to the first column). Such structure arises so often in the study of combinatorial matrices that it merits its own definition.

Definition 2.5.1. We call an $n \times n$ matrix $M = \left(m_{ij}\right)$ *circulant* if $m_{ij} = m_{i,j-i+1}$, where $j-i+1$ is reduced modulo n. If this is the case we write $M = \text{circ}(m_{1,1}, m_{1,2}, ..., m_{1,n})$.

It turns out that $q = 3$ is not the only prime power for which there is a circulant Jacobsthal matrix. In fact, whenever q is prime it is possible to construct a circulant Jacobsthal matrix of order q. Moreover, for any prime power q one can construct a Jacobsthal matrix whose structure is *multicirculant*. Before we define multicirculant structure, we must introduce a prerequisite definition.

Definition 2.5.2. We call an $n \times n$ matrix M *block-circulant* if it is of the form

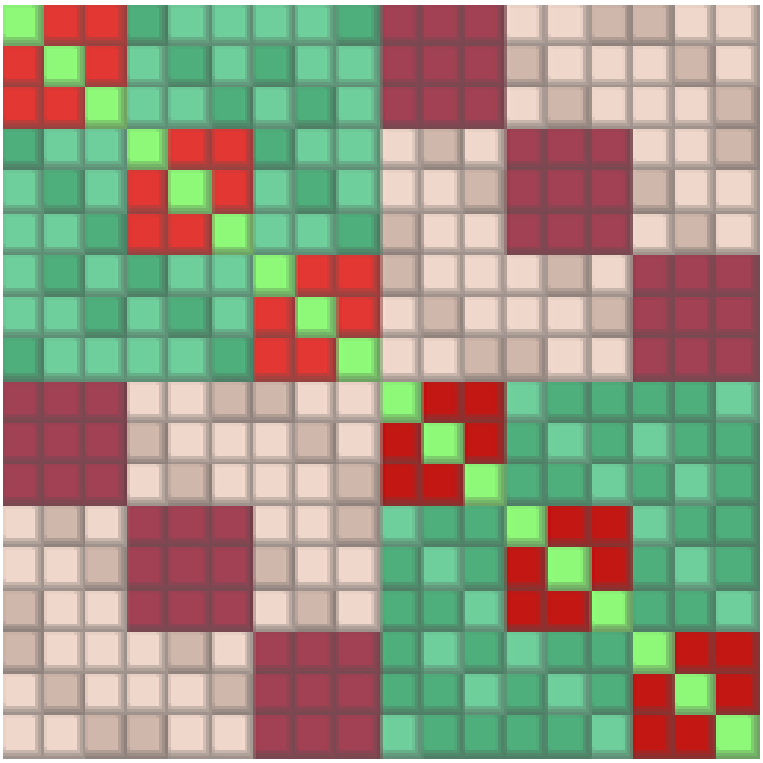
$$M = \text{circ}(M_1, M_2, ..., M_k),$$

where each M_i is a matrix of order a and $ka = n$.

Definition 2.5.3. Let M be a matrix of order n. If $n = 1$, then we call M a multicirculant matrix. If $n > 1$, then we call M multicirculant if and only if it is a block-circulant matrix whose blocks are multicirculant matrices.

In less formal language, a multicirculant matrix is a block-circulant matrix whose blocks are block-circulant, whose blocks' blocks are in turn block-circulant, whose blocks' blocks' blocks are also block-circulant, etc. Multicirculant structure is best understood by way of an example.

Example 2.5.4. A multicirculant matrix.



It is straightforward to observe that the Kronecker product of two multicirculant matrices is itself a multicirculant matrix. Moreover, if A and B are two multicirculant $n \times n$ matrices such that all their multicirculant blocks are of the same dimensions, then $A+B$ is also a multicirculant matrix. These facts will be of use in Chapter 3. For the time being, however, we will content ourselves with proving Jacobsthal matrices can always be made multicirculant. To begin, we must introduce some new notation.

Given an $n \times m$ matrix $A = (a_{ij})$ with entries in a set S and an element x of S, let $[x,A]$ denote the $n \times m$ matrix whose entry in its i^{th} row and j^{th} column is the ordered pair (x, a_{ij}). If a_{ij} is itself an ordered n-tuple $(a_{ij}^{(1)}, \ldots, a_{ij}^{(n)})$, then (x, a_{ij}) denotes the ordered $(n+1)$-tuple $(x, a_{ij}^{(1)}, \ldots, a_{ij}^{(n)})$. We will make use of this notation in our proof that Jacobsthal matrices can be made multicirculant. We will also make use of the following definition.

Definition 2.5.5. Let p be a prime and m a positive integer and consider the additive group $(\mathbb{Z}_p)^m$. Let $S = (s_{ij})$ be a $p^m \times p^m$ matrix whose rows and columns are indexed by the

elements of $(\mathbb{Z}_p)^m$ in the order

$$(0,\ldots,0,0),(0,\ldots,0,1),\ldots,(0,\ldots,0,p-1),(0,\ldots,0,1,0),(0,\ldots,0,1,1),\ldots,(p-1,\ldots,p-1).$$

(That is, the ordered tuple $(a_1,\ldots,a_{p^m})$ comes before the ordered tuple $(b_1,\ldots,b_{p^m})$ if and only if the decimal number $(a_1a_2\ldots a_{p^m})_{10}$ is less than the decimal number $(b_1b_2\ldots b_{p^m})_{10}$). We call S the *subtraction table* for $(\mathbb{Z}_p)^m$ if $s_{ij}=i-j$ for each $i,j\in(\mathbb{Z}_p)^m$.

Example 2.5.6. The definition of subtraction tables is quite wordy, so we consider an example: the subtraction table for $\mathbb{Z}_2\times\mathbb{Z}_2$.

$$\begin{array}{c} \\ (0,0) \\ (0,1) \\ (1,0) \\ (1,1) \end{array}\begin{array}{c} \begin{array}{cccc} (0,0) & (0,1) & (1,0) & (1,1) \end{array} \\ \begin{pmatrix} (0,0) & (0,1) & (1,0) & (1,1) \\ (0,1) & (0,0) & (1,1) & (1,0) \\ (1,0) & (1,1) & (0,0) & (0,1) \\ (1,1) & (1,0) & (0,1) & (0,0) \end{pmatrix} \end{array}$$

Notice that the matrix in Example 2.5.6 is multicirculant. This turns out to be true of the subtraction table for $(\mathbb{Z}_p)^m$ for any prime p and positive integer m. To prove this, we define a new class of matrices.

Given a prime p and a positive integer m, we define a $p^m\times p^m$ multicirculant matrix $M_m^{(p)}$ with entries in $(\mathbb{Z}_p)^m$ by

$$M_m^{(p)}=\begin{cases}\operatorname{circ}(0,p-1,p-2,\ldots,1) & \text{if } m=1\\ \operatorname{circ}([0,M_{m-1}^{(p)}],[p-1,M_{m-1}^{(p)}],[p-2,M_{m-1}^{(p)}],\ldots,[1,M_{m-1}^{(p)}]) & \text{otherwise.}\end{cases}$$

For example, if $p = 2$, then

$$M_1^{(2)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad M_2^{(2)} = \left(\begin{array}{cc|cc} (0,0) & (0,1) & (1,0) & (1,1) \\ (0,1) & (0,0) & (1,1) & (1,0) \\ \hline (1,0) & (1,1) & (0,0) & (0,1) \\ (1,1) & (1,0) & (0,1) & (0,0) \end{array}\right).$$

Looking at these matrices, one notices that $M_1^{(2)}$ is the subtraction table for $\mathbb{Z}_2$ and $M_2^{(2)}$ is the subtraction table for $\mathbb{Z}_2 \times \mathbb{Z}_2$. In fact, we can show that $M_m^{(p)}$ is the subtraction table for $(\mathbb{Z}_p)^m$ for any prime p and integer $m > 0$.

Lemma 2.5.7. *Let p be a prime and let m be a positive integer. Then $M_m^{(p)}$ is the subtraction table for $(\mathbb{Z}_p)^m$.*

Proof. We induct on m. For the base case note that $-a \equiv p - a \pmod{p}$ for any $a \in \mathbb{Z}$. Using this fact we see that $M_1^{(p)}$ is the subtraction table for $\mathbb{Z}_p$. Now assume the lemma holds for some positive integer m. Let $0 \leq i, j \leq p-1$, let S be the subtraction table for $(\mathbb{Z}_p)^m$, and consider the subtraction table for $(\mathbb{Z}_p)^{m+1}$ as a block matrix composed of $p^m \times p^m$ blocks. Then the subtraction table for $(\mathbb{Z}_p)^{m+1}$ is composed of p rows of blocks (block rows) and p columns of blocks (block columns). Let us index these block rows and block columns from 0 to $p-1$. Notice that the block in the i^{th} block row and j^{th} block column of this subtraction table is $[i-j, S]$, where $i-j$ is reduced modulo p so that it lies in the set $\{0, 1, \ldots, p-1\}$. By the induction hypothesis $S = M_m^{(p)}$, so the block in the i^{th} block row and j^{th} block column of the subtraction table for $(\mathbb{Z}_p)^{m+1}$ is $[i-j, M_m^{(p)}]$. It follows that the subtraction table for $(\mathbb{Z}_p)^{m+1}$ is

$$\operatorname{circ}([0, M_m^{(p)}], [p-1, M_m^{(p)}], [p-2, M_m^{(p)}], \ldots, [1, M_m^{(p)}]).$$

This is precisely $M_{m+1}^{(p)}$, which completes the proof. □

Lemma 2.5.8. *Let p be a prime and let m be a positive integer. The subtraction table for $(\mathbb{Z}_p)^m$ is multicirculant.*

Proof. Lemma 2.5.7 tells us $M_m^{(p)}$ is the subtraction table for $(\mathbb{Z}_p)^m$. It is immediate from the definition of $M_m^{(p)}$ that $M_m^{(p)}$ is multicirculant. □

Proposition 2.5.9. *Let m be a positve integer and p an odd prime. Then one can construct a multicirculant Jacobsthal matrix of order p^m. If $m = 1$, then one can construct a circulant Jacobsthal matrix of order p^m.*

Proof. As a group under addition, $\mathrm{GF}(p^m)$ is isomorphic to $(\mathbb{Z}_p)^m$. Let

$$\phi : (\mathbb{Z}_p)^m \to \mathrm{GF}(p^m)$$

be such a group isomorphism. Let $(\mathbb{Z}_p)^m = \{x_1, \ldots, x_{p^m}\}$, where the elements are indexed such that the $p^m \times p^m$ matrix $S = (s_{ij})$ defined by $s_{ij} = x_i - x_j$ is the subtraction table for $(\mathbb{Z}_p)^m$. Define a Jacobsthal matrix $Q_{p^m} = (q_{ij})$ of order p^m by $q_{ij} = \chi_{p^m}(\phi(x_i) - \phi(x_j))$. Since ϕ is an isomorphism, it follows that $q_{ij} = \chi_{p^m}(\phi(x_i - x_j))$. Lemma 2.5.8 tells us S is multicirculant. It follows that Q_{p^m} is a multicirculant Jacobsthal matrix of order p^m. □

2.6 Unit and Butson Hadamard Matrices

In the past century-and-a-half, many generalizations of Hadamard matrices have been studied. In this thesis we shall concern ourselves with two such generalizations: Butson Hadamard matrices and unit Hadamard matrices. Butson Hadamard matrices were first introduced by Butson [3]. Similar to Hadamard matrices, they require their rows to be pairwise orthogonal. However, they remove the constraint that their entries must be in the set $\{\pm 1\}$, instead requiring only that their entries are k^{th} roots of unity. Unit Hadamard matrices, first studied by Sylvester [21], further loosen constraints by allowing their entries to be any complex number of modulus 1. Formally, these matrices are defined in the following way.

Definition 2.6.1. A *Butson Hadamard matrix* is an $n \times n$ matrix H whose entries are all complex k^{th} roots of unity such that $HH^* = nI_n$. For short, we refer to such a matrix as a $\text{BH}(n,k)$. If all of the entries of H are in $\mathbb{C} \setminus \mathbb{R}$, we call H an *unreal* $\text{BH}(n,k)$.

Remark 2.6.2. The reader should be advised that some authors refer to a Butson Hadamard matrix of order n over k^{th} roots of unity as a $\text{BH}(k,n)$ as opposed to our chosen $\text{BH}(n,k)$.

Definition 2.6.3. A *unit Hadamard matrix* is an $n \times n$ matrix H whose entries are unimodular complex numbers such that $HH^* = nI_n$. For short, we refer to such a matrix as a $\text{UH}(n)$. If all of the entries of H are in $\mathbb{C} \setminus \mathbb{R}$, we call H an *unreal* $\text{UH}(n)$.

Remark 2.6.4. The reader should be advised that some authors use the names *complex Hadamard matrix* or *generalized Hadamard matrix* for what we call a unit Hadamard matrix. However, we will avoid these names as they have been used by many different authors to refer to many different types of matrices.

For an in-depth examination of unit Hadamard matrices and Butson Hadamard matrices, we refer the reader to [22].

Example 2.6.5. Let ω be a primitive cube root of unity. The following is a $\text{BH}(3,3)$ and a $\text{UH}(3)$:

$$\begin{pmatrix} \omega & \omega^2 & \omega^2 \\ \omega^2 & \omega & \omega^2 \\ \omega^2 & \omega^2 & \omega \end{pmatrix}$$

As an interesting application of Butson Hadamard matrices, consider $\text{BH}(n,4)$'s, which were first studied by Turyn [23, 24]. It was shown by Turyn that the existence of a $\text{BH}(n,4)$ implies the existence of a Hadamard matrix of order $2n$. This fact is encompassed in the following theorem:

Theorem 2.6.6. *Let H be a $BH(n,4)$ and let*

$$X = \begin{pmatrix} 1 & - \\ 1 & 1 \end{pmatrix} \text{ and } Y = \begin{pmatrix} - & - \\ 1 & - \end{pmatrix}.$$

Let H' be the matrix obtained by applying the maps $\pm 1 \mapsto \pm X$ and $\pm i \mapsto \pm Y$ to the entries of H. Then H' is a Hadamard matrix of order $2n$.

Similarly to Hadamard matrices, there is a condition on the orders for which $\mathrm{BH}(n,4)$'s can exist: n must be even. Analogously to the Hadamard conjecture, it is conjectured that the converse is also true.

Conjecture 2.6.7 (Seberry, cf. [4])**.** If n is even, then there is a $\mathrm{BH}(n,4)$.

In contrast to Hadamard matrices and Butson Hadamard matrices, the orders for which a unit Hadamard matrix exist are completely determined. This fact is summarized by the following theorem.

Theorem 2.6.8. *There is a unit Hadamard matrix of order n for each $n \geq 1$.*

Proof. We claim that the $n \times n$ Fourier matrix $F = (f_{jk})$ defined by

$$f_{jk} = e^{2\pi i jk/n}$$

for each $0 \leq j,k < n$ is a $\mathrm{UH}(n)$. Indeed, the claim is trivial if $n = 1$, so assume $n > 1$ and let r_j and r_k be the j^{th} and k^{th} rows of F. Then for $j \neq k$ we have

$$\begin{aligned} r_j \cdot r_k &= \sum_{m=0}^{n-1} f_{jm}\overline{f_{km}} \\ &= \sum_{m=0}^{n-1} (e^{2\pi i(j-k)/n})^m. \end{aligned}$$

Since $j \neq k$ and $n > 1$, we can apply the geometric series formula.

$$r_j \cdot r_k = \frac{1 - (e^{2\pi i(j-k)/n})^n}{1 - e^{2\pi i(j-k)/n}} = 0.$$

On the other hand, if $j = k$ it's clear that $r_j \cdot r_k = n$. Thus $FF^* = nI_n$. □

2.7 The Excess of Unit Hadamard Matrices

In the late seventies the study of the maximum sum of the entries of Hadamard matrices began to garner researchers' attention. Pioneering work was done in this area in 1977 by Best [2]. Later, other authors would generalize the scope of this research to study the maximum modulus of the sum of the entries, or the *excess*, of Butson Hadamard matrices and unit Hadamard matrices (see, for example, [14]). In this thesis, we shall be concerned both with the excess of Hadamard matrices and unit Hadamard matrices. To begin, we introduce some notation.

Notation 2.7.1. If A is a matrix, we denote the sum of its entries by $S(A)$.

Two useful properties of S are readily seen to be true:

(1) $S(A+B) = S(A) + S(B)$

(2) $S(A \otimes B) = S(A)S(B)$.

Definition 2.7.1. If H is a unit Hadamard matrix, we define its *excess* to be the quantity $|S(H)|$, and we denote its excess $\sigma(H)$.

With the excess of unit Hadamard matrices defined, it is natural to ask what is the maximum excess of all unit Hadamard matrices or Hadamard matrices of a given order. To

study this problem we present two additional pieces of notation.

Notation 2.7.2. Given a positive integer n, let

$$\sigma_R(n) = \max\{\sigma(H) : H \text{ is a Hadamard matrix of order } n\}$$

and

$$\sigma_U(n) = \sup\{\sigma(H) : H \text{ is a unit Hadamard matrix of order } n\}.$$

We shall refer to these quantities respectively as the maximum excess of real Hadamard matrices of order n and the maximum excess of unit Hadamard matrices of order n.

In his early study of the maximum excess problem, Best used a clever application of the Cauchy-Schwarz inequality to prove a nice upper bound for $\sigma_R(n)$ [2]. For the sake of this thesis, we present a more general version of Best's upper bound which is formulated in terms of unit Hadamard matrices.

Theorem 2.7.2. *Let n be a positive integer. Then $\sigma_R(n) \leq \sigma_U(n) \leq n\sqrt{n}$.*

Proof. The first inequality is clear since all Hadamard matrices are unit Hadamard matrices. For the second inequality, let H be a unit Hadamard matrix of order n and let c_i denote the i^{th} column sum of H. Let j_n denote the $1 \times n$ all-ones matrix and use the Cauchy-Schwartz inequality to observe that

$$\begin{aligned}
\sigma_U(n) &= \left|\sum_i c_i\right| \\
&\leq \sum_i |c_i| \\
&= j_n \cdot (|c_1|, |c_2|, ..., |c_n|) \\
&\leq \sqrt{n\sum_i |c_i|^2}.
\end{aligned}$$

Therefore, it is enough to show $\sum_i |c_i|^2 = n^2$. Notice that

$$j_n H H^* j_n^T = j_n n I_n j_n^T = n^2.$$

However, we also have

$$j_n H H^* j_n^T = [c_1\ c_2 \cdots c_n]\,[c_1\ c_2 \cdots c_n]^* = \sum_i |c_i|^2.$$

Thus $\sum_i |c_i|^2 = n^2$ and the result follows. □

Best showed that his bound is met by a Hadamard matrix H if and only if all of the row sums of H are equal. There is a special name for such a Hadamard matrix.

Definition 2.7.3. A Hadamard matrix is called *regular* if all of its row sums are equal.

For many additional interesting upper and lower bounds on the excess of Hadamard matrices, we refer the reader to [7, 9, 12, 17].

Before proceeding to the next section, we present one basic fact which will be used repeatedly in Chapter 3.

Proposition 2.7.4. *Let q be an odd prime power and let Q be a Jacobsthal matrix of order q. Then*

$$S(Q) = 0.$$

Proof. Recall from Section 2.4 that there are as many quadratic residues as there are quadratic non-residues in GF(q). Together with the definition of Jacobsthal matrices and of the quadtratic character, this implies the result. □

2.8 Balanced Incomplete Block Designs

To conclude our the chapter, we switch our focus from Hadamard matrices, their properties, and their generalizations, to another combinatorial object: *balanced incomplete block*

designs. Historically, balanced incomplete block designs were introduced to aid in the design of experiments. However, in this thesis we shall study balanced incomplete block designs for their combinatorial intrigue as opposed to their applications in experimental design.

Definition 2.8.1. A pair $(V, \mathcal{B})$ is called a *balanced incomplete block design*, or *BIBD*, with *parameters* v, b, r, k, λ if each of the following hold.

1. V is a v-set.

2. $\mathcal{B}$ is a collection of b k-subsets (*blocks*) of V.

3. Each element of V is contained in exactly r blocks.

4. Any 2-subset of V is contained in exactly λ blocks.

For short, we refer to such a design as a BIBD(v, b, r, k, λ).

Example 2.8.2. A BIBD$(4, 6, 3, 2, 1)$:

$$V = \{a, b, c, d\}$$

$$\mathcal{B} = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}\}$$

It is straightforward to verify that not all parameters of a BIBD are independent, as we see from the following theorem.

Theorem 2.8.3. *In any BIBD*(v, b, r, k, λ)*, we have* $bk = vr$ *and* $r(k-1) = \lambda(v-1)$.

Proof. Let $(V, \mathcal{B})$ be a BIBD(v, b, r, k, λ), and consider the set

$$S = \{(a, B) : a \in V, B \in \mathcal{B}, \text{ and } a \in B\}.$$

To prove the theorem, we determine the cardinality of S in two ways. First, for each block B, there are k elements of V in B. Since there are b choices for B, it follows that $|S| = bk$. On

the other hand, for each element $a \in V$, a appears in exactly r blocks. There are v choices for a, so $|S| = vr$. Combining the two expressions for $|S|$, we obtain $bk = vr$.

To prove $r(k-1) = \lambda(v-1)$, let $V = \{a_1, \ldots, a_v\}$ and define a graph whose nodes are the elements of V such that there are no loops and there's an edge between distinct nodes a_i and a_j for every block containing both a_i and a_j. We count the number of edges incident with a_i in two different ways. First of all, there are λ edges between a_i and each of the $v-1$ other nodes since every pair of nodes appear together in λ blocks. Thus there are $\lambda(v-1)$ edges incident with a_i. On the other hand, a_i appears in a total of r blocks, and in each of these blocks there are $k-1$ other nodes. Thus there are $r(k-1)$ edges incident with a_i. It follows that $r(k-1) = \lambda(v-1)$. □

Theorem 2.8.3 confirms that not all parameters of a BIBD(v,b,r,k,λ) are independent. For this reason, BIBD(v,b,r,k,λ)'s are often simply referred to as (v,k,λ)-designs.

It is often inconvenient to represent BIBDs as the sets described in their definition. When this is the case, it is often much more desirable to represent BIBDs as $(0,1)$-matrices as described below.

Definition 2.8.4. Let $(V,\mathcal{B})$ be a BIBD(v,b,r,k,λ) and index the elements of V and $\mathcal{B}$ from 1 to v and 1 to b respectively. The *incidence matrix* of $(V,\mathcal{B})$ is a $v \times b$ matrix $A = (a_{ij})$, in which $a_{ij} = 1$ when the i^{th} element of V occurs in the j^{th} block of $\mathcal{B}$, and $a_{ij} = 0$ otherwise.

The next theorem provides a useful method of verifying whether a given $(0,1)$-matrix is the incidence matrix of a BIBD. It amounts to a restatement of the definition of BIBDs in terms of incidence matrices, and is easily seen to be true after a brief period of reflection. It

was taken from Colbourn and Dinitz [4], and will be used in Chapter 3.

Theorem 2.8.5. *If A is the incidence matrix of a (v,k,λ)-design, then $AA^T = (r-\lambda)I_v + \lambda J_v$ and $J_v A = k\hat{J}$, where $\hat{J}$ is the $v \times b$ all ones matrix. Moreover, any matrix A satisfying these conditions also satisfies $\lambda(v-1) = r(k-1)$ and $bk = vr$; when $k < v$, it is the incidence matrix of a (v,k,λ)-design.*

With this theorem under our belts, we are ready to move on to study the original results in this thesis.

Chapter 3

Results

This chapter is devoted to studying the applications of pairs of $n \times n$ matrices A and B with unimodular entries satisfying $AB^* = BA^*$ and $BB^* + AA^* = n(q+1)I_n$ for some odd prime power q. We will see that pairs of matrices with these properties are a valuable tool, and can be used to construct Hadamard matrices, Butson Hadamard matrices, and unit Hadamard matrices. Moreover, in certain cases we will see that the combinatorial matrices constructed using A and B have interesting properties, such as multicirculant structure and large excess. Finally, as an application we will construct an infinite family of BIBDs.

3.1 Applications of q-Suitable Pairs of Matrices

We begin with a definition that is at the heart of this entire chapter.

Definition 3.1.1. Let q be an odd prime power and let A and B be two $n \times n$ matrices. We call A and B *amicable* if $AB^* = BA^*$. We call the ordered pair (A,B) a *q-suitable pair* if A and B are amicable, have exclusively unimodular entries, and satisfy $qAA^* + BB^* = (q+1)nI_n$.

Any q-suitable pair can be used to obtain a unit Hadamard matrix. In fact, when the entries of both matrices in a q-suitable pair come strictly from the set $\{\pm 1\}$, they can be used to construct a real Hadamard matrix. This result is summarized in the next theorem.

Theorem 3.1.2. *Let q be an odd prime power, let (A,B) be a q-suitable pair of $n\times n$ matrices, let Q be a Jacobsthal matrix for $GF(q)$, let j_q be the $1\times q$ all-ones matrix, and let I'_{q+1} be the matrix obtained by negating the first row of I_{q+1}. Then*

(i) $\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes A + I'_{q+1} \otimes B$ *is a unit Hadamard matrix if* $q \equiv 3 \pmod 4$.

(ii) $\begin{pmatrix} 0 & j_q \\ -j_q^T & Q \end{pmatrix} \otimes A + i I'_{q+1} \otimes B$ *is a unit Hadamard matrix if* $q \equiv 1 \pmod 4$.

Moreover, if A and B are (± 1)-matrices, then the matrix in (i) is a Hadamard matrix, and if A and B are $(\pm 1, \pm i)$-matrices, then the matrices in (i) and (ii) are $BH((q+1)n,4)$'s.

Proof. Let H_1 denote the matrix in (i) and H_2 denote the matrix in (ii). Since (A,B) is a q-suitable pair and since the main diagonal of Q is composed entirely of zeros, we see that H_1 and H_2 have exclusively unimodular entries. Recall that $QQ^T = qI_q - J_q$ and that Q is symmetric if $q \equiv 1 \pmod 4$ and antisymmetric if $q \equiv 3 \pmod 4$. Using these facts together with the q-suitability of the pair (A,B), we see:

$$\begin{aligned} H_1 H_1^* &= \begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \begin{pmatrix} 0 & j_q \\ j_q^T & Q^T \end{pmatrix} \otimes AA^* + \begin{pmatrix} 0 & j_q \\ -j_q^T & Q \end{pmatrix} \otimes AB^* \\ &\quad + \begin{pmatrix} 0 & -j_q \\ j_q^T & -Q \end{pmatrix} \otimes BA^* + I_{q+1} \otimes BB^* \\ &= qI_{q+1} \otimes AA^* + I_{q+1} \otimes BB^* \\ &= I_{q+1} \otimes (qAA^* + BB^*) \\ &= I_{q+1} \otimes ((q+1)nI_n) \\ &= (q+1)nI_{(q+1)n}. \end{aligned}$$

Similarly,

$$\begin{aligned} H_2H_2^* &= \begin{pmatrix} 0 & j_q \\ -j_q^T & Q \end{pmatrix}\begin{pmatrix} 0 & -j_q \\ j_q^T & Q \end{pmatrix} \otimes AA^* - i\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes AB^* \\ &\quad + i\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes BA^* + I_{q+1} \otimes BB^* \\ &= qI_{q+1} \otimes AA^* + I_{q+1} \otimes BB^* \\ &= (q+1)nI_{(q+1)n}. \end{aligned}$$

This shows that both H_1 and H_2 are unit Hadamard matrices. Since the main diagonal of Q is composed entirely of zeros we see that if A and B are (± 1)-matrices, then so is H_1, meaning H_1 is a Hadamard matrix. Similarly, if A and B are $(\pm 1, \pm i)$ matrices, then so are H_1 and H_2, meaning H_1 and H_2 are BH$((q+1)n, 4)$'s. □

Remark 3.1.3. Throughout this chapter we will define Q and I'_{q+1} as we did in Theorem 3.1.2, and we will let j_m denote the all-ones $1 \times m$ matrix.

Theorem 3.1.2 is an application of q-suitable pairs. Next, we will present a method to explode any q-suitable pair into two infinite classes of q-suitable pairs, thereby obtaining two infinite classes of unit Hadamard matrices.

Theorem 3.1.4. *Let q be a prime power and suppose (Y,X) is a q-suitable pair. Let*

$$\mathcal{X}_m = \begin{cases} X & \text{if } m = 0 \\ J_q \otimes \mathcal{Y}_{m-1} & \text{otherwise} \end{cases} \qquad \mathcal{Y}_m = \begin{cases} Y & \text{if } m = 0 \\ I_q \otimes \mathcal{X}_{m-1} + Q \otimes \mathcal{Y}_{m-1} & \text{otherwise} \end{cases}$$

and

$$\mathcal{W}_m = \begin{cases} X & \text{if } m = 0 \\ J_q \otimes \mathcal{Z}_{m-1} & \text{otherwise} \end{cases} \qquad \mathcal{Z}_m = \begin{cases} Y & \text{if } m = 0 \\ I_q \otimes \mathcal{W}_{m-1} + iQ \otimes \mathcal{Z}_{m-1} & \text{otherwise} \end{cases}.$$

The matrices $\mathcal{X}_m$ and $\mathcal{Y}_m$ are amicable, as are $\mathcal{W}_m$ and $\mathcal{Z}_m$. Moreover,

(i) If $q \equiv 3 \pmod 4$, then $(\mathcal{Y}_m, \mathcal{X}_m)$ is a q-suitable pair.

(ii) If $q \equiv 1 \pmod 4$, then $(\mathcal{Z}_m, \mathcal{W}_m)$ is a q-suitable pair.

Proof. First we remark that since X and Y have exclusively unimodular entries, a basic induction using the fact that the main diagonal of Q is composed entirely of zeros shows $\mathcal{X}_m$ and $\mathcal{Y}_m$ have exclusively unimodular entries. To prove the amicability of $\mathcal{X}_m$ and $\mathcal{Y}_m$ we induct on m. The base case $m = 0$ is true by assumption. Now suppose $\mathcal{X}_m$ and $\mathcal{Y}_m$ are amicable for some $m \geq 0$. Since $J_q Q^T = Q^T J_q = 0$, we find

$$\begin{aligned} \mathcal{X}_{m+1}\mathcal{Y}_{m+1}^T &= (J_q \otimes \mathcal{Y}_m)(I_q \otimes \mathcal{X}_m + Q \otimes \mathcal{Y}_m)^T \\ &= J_q \otimes (\mathcal{Y}_m \mathcal{X}_m^T) \\ &= J_q \otimes (\mathcal{X}_m \mathcal{Y}_m^T) \\ &= (I_q \otimes \mathcal{X}_m + Q \otimes \mathcal{Y}_m)(J_q \otimes \mathcal{Y}_m)^T \\ &= \mathcal{Y}_{m+1}\mathcal{X}_{m+1}^T \end{aligned}$$

It follows that $\mathcal{X}_m$ and $\mathcal{Y}_m$ are amicable for each integer $m \geq 0$. The amicability of $\mathcal{W}_m$ and $\mathcal{Z}_m$ can be proven similarly.

Next, we'll prove (i) by induction on m. Assume $q \equiv 3 \pmod 4$, so $Q^T = -Q$. As with amicability, the base case $m = 0$ is true by assumption. Now suppose (i) holds for some $m \geq 0$. Using the facts that Q is antisymmetric, that $QQ^T = qI_q - J_q$, and that $\mathcal{X}_m$ and $\mathcal{Y}_m$ are amicable, we obtain:

$$\begin{aligned}
&\mathcal{X}_{m+1}\mathcal{X}_{m+1}^T + q\,\mathcal{Y}_{m+1}\mathcal{Y}_{m+1}^T \\
&\qquad = (J_q \otimes \mathcal{Y}_m)(J_q \otimes \mathcal{Y}_m)^T + q\,(I_q \otimes \mathcal{X}_m + Q \otimes \mathcal{Y}_m)(I_q \otimes \mathcal{X}_m + Q \otimes \mathcal{Y}_m)^T \\
&\qquad = q\,J_q \otimes \mathcal{Y}_m\mathcal{Y}_m^T + q\,I_q \otimes \mathcal{X}_m\mathcal{X}_m^T - q\,Q \otimes \mathcal{X}_m\mathcal{Y}_m^T + q\,Q \otimes \mathcal{Y}_m\mathcal{X}_m^T + q\,QQ^T \otimes \mathcal{Y}_m\mathcal{Y}_m^T \\
&\qquad = q\,J_q \otimes \mathcal{Y}_m\mathcal{Y}_m^T + q\,I_q \otimes \mathcal{X}_m\mathcal{X}_m^T + q\,(qI_q - J_q) \otimes \mathcal{Y}_m\mathcal{Y}_m^T \\
&\qquad = q\,I_q \otimes (\mathcal{X}_m\mathcal{X}_m^T + q\,\mathcal{Y}_m\mathcal{Y}_m^T) \\
&\qquad = nq^{m+1}(q+1)\,I_{nq^{m+1}}
\end{aligned}$$

It follows that (i) holds for each integer $m \geq 0$. We can prove (ii) similarly. □

Later it will be of interest to determine the sum of the entries of matrices $\mathcal{X}_m$ and $\mathcal{Y}_m$ constructed using Theorem 3.1.4. As such, we introduce the following easy proposition.

Proposition 3.1.5. *Let q be a prime power and suppose X and Y are two $n \times n$ matrices. Let*

$$\mathcal{X}_m = \begin{cases} X & \text{if } m = 0 \\ J_q \otimes \mathcal{Y}_{m-1} & \text{otherwise} \end{cases} \qquad \mathcal{Y}_m = \begin{cases} Y & \text{if } m = 0 \\ I_q \otimes \mathcal{X}_{m-1} + Q \otimes \mathcal{Y}_{m-1} & \text{otherwise} \end{cases}.$$

Then for all integers $m \geq 0$ we have:

(i) $S(\mathcal{X}_{2m}) = q^{3m}S(X)$

(ii) $S(\mathcal{Y}_{2m}) = q^{3m}S(Y)$

(iii) $S(\mathcal{X}_{2m+1}) = q^{3m+2}S(Y)$

(iv) $S(\mathcal{Y}_{2m+1}) = q^{3m+1}S(X)$.

Proof. First recall three facts from Chapter 2:

(1) $S(Q) = 0$

(2) $S(A \otimes B) = S(A)S(B)$ for all matrices A and B.

(3) $S(A+B) = S(A) + S(B)$ whenever A and B have the same dimensions.

Using these facts, observe that the following holds for all $m \geq 2$:

$$\begin{aligned} S(\mathcal{X}_m) &= S(J_q \otimes \mathcal{Y}_{m-1}) \\ &= S(J_q)S(I_q \otimes \mathcal{X}_{m-2} + Q \otimes \mathcal{Y}_{m-2}) \\ &= q^2(S(I_q)S(\mathcal{X}_{m-2}) + S(Q)S(\mathcal{Y}_{m-2})) \\ &= q^3 S(\mathcal{X}_{m-2}) \end{aligned} \tag{3.1}$$

Similarly,

$$S(\mathcal{Y}_m) = q^3 S(Y_{m-2}) \tag{3.2}$$

We can now prove (i) by induction. Note that the base case holds since $\mathcal{X}_0 = X$. Now suppose $k \geq 0$ and that $S(\mathcal{X}_{2k}) = q^{3k}S(X)$. Together with Equation 3.1 this implies $S(\mathcal{X}_{2(k+1)}) = q^3 S(\mathcal{X}_{2k}) = q^{3(k+1)}S(X)$. This proves that (i) holds for all integers $m \geq 0$.

Using Eqs. 3.1 and 3.2 it is straightforward to prove (ii), (iii), and (iv) by induction. We will skip these proofs since they are extremely similar to the proof of (i). □

Together, Theorems 3.1.4 and 3.1.2 present us with a tool for constructing infinite classes of Hadamard and unit Hadamard matrices. According to Theorem 3.1.2, for any odd prime power q, any q-suitable pair provides us with a unit Hadamard matrix. According to Theorem 3.1.4, any q-suitable pair can be used recursively to obtain an infinite class of pairs of q-suitable matrices. Therefore, any pair of q-suitable matrices provides us with an infinite class of unit Hadamard matrices. This establishes the following corollary.

Corollary 3.1.6. *Let q be an odd prime power. If there is a q-suitable pair of $n \times n$ matrices (Y,X), then there is a unit Hadamard matrix of order $nq^m(q+1)$ for each integer $m \geq 0$. Moreover, there is a $BH(nq^m(q+1),4)$ if X and Y are $(\pm 1, \pm i)$-matrices. Finally, there is a Hadamard of order $nq^m(q+1)$ if X and Y are (± 1)-matrices and $q \equiv 3 \pmod 4$.*

In addition to the matrices obtained above, any q-suitable pair of matrices of order n provide us with the means of constructing unit Hadamard matrices of order nq^m for each prime power $q \equiv 3 \pmod 4$ and each integer $m \geq 0$. Moreover, we will show that when $q = 3$, the aforementioned unit Hadamard matrices are in fact unreal Butson Hadamard matrices. For this we will require a lemma.

Lemma 3.1.7. *Let m be a positive integer. Then $\frac{1}{\sqrt{m+1}} + i\frac{\sqrt{m}}{\sqrt{m+1}}$ is a root of unity if and only if $m = 3$. Similarly, $\frac{\sqrt{m}}{\sqrt{m+1}} + i\frac{1}{\sqrt{m+1}}$ is a root of unity if and only if $m = 3$.*

Proof. Let $\zeta_1 = \frac{1}{\sqrt{m+1}} + i\frac{\sqrt{m}}{\sqrt{m+1}}$ and $\zeta_2 = \frac{\sqrt{m}}{\sqrt{m+1}} + i\frac{1}{\sqrt{m+1}}$. If $m = 3$ then ζ_1 is a sixth root of unity and ζ_2 is a twelfth root of unity. For the converse, assume without loss of generality that ζ_1 is a primitive n^{th} root of unity and that ζ_2 is a primitive k^{th} root of unity. Notice that ζ_1 and ζ_2 are roots of the polynomial $x^4 + 2\frac{m-1}{m+1}x^2 + 1$. Thus $\phi(n) = [\mathbb{Q}(\zeta_1) : \mathbb{Q}] \leq 4$ and $\phi(k) = [\mathbb{Q}(\zeta_2) : \mathbb{Q}] \leq 4$, where ϕ denotes Euler's totient function. Therefore, we can conclude that $n,k \in \{1,2,3,4,5,6,8,10,12\}$. Examining these cases by hand shows that $n = k = 3$ is the only allowable possibility. □

Theorem 3.1.8. *Let q be an odd prime power and let (Y,X) be a q-suitable pair of $n \times n$ (± 1)-matrices. Let*

$$K = \frac{1}{\sqrt{q+1}}X + i\sqrt{\frac{q}{q+1}}Y$$

and

$$L = \sqrt{\frac{q}{q+1}}Y + i\frac{1}{\sqrt{q+1}}X.$$

Then K and L are unreal $UH(n)$'s. Moreover, if $q = 3$, then K is an unreal $BH(n,6)$ and L is an unreal $BH(n,12)$. If $q \neq 3$, then K and L are not Butson Hadamard matrices.

Proof. Since X and Y are (± 1)-matrices one readily sees that K is a matrix with unimodular unreal entries. Next, using the q-suitability of the pair (Y,X), observe that:

$$\begin{aligned} KK^* &= \left(\frac{1}{\sqrt{q+1}}X + i\sqrt{\frac{q}{q+1}}Y\right)\left(\frac{1}{\sqrt{q+1}}X^* - i\sqrt{\frac{q}{q+1}}Y^*\right) \\ &= \frac{1}{q+1}XX^* - i\frac{\sqrt{q}}{q+1}XY^* + i\frac{\sqrt{q}}{q+1}YX^* + \frac{q}{q+1}YY^* \\ &= \frac{1}{q+1}\left(XX^* + qYY^*\right)) \\ &= nI_n. \end{aligned}$$

This shows K is a unit Hadamard matrix. Similarly, we can show L is a unit Hadamard matrix. Now, if $q = 3$, then the entries of K are in the set $\{e^{2k\pi i/6} : k = \pm 1, \pm 2\}$ while the entries of L are in the set $\{e^{k\pi i/6} : k = \pm 1, \pm 5\}$. It follows that if $q = 3$, then K is an unreal $\mathrm{BH}(n,6)$ and L is an unreal $\mathrm{BH}(n,12)$. Finally, note that if ζ is an n^{th} root of unity and n is even, then $-\zeta$ and $\overline{\zeta}$ are also n^{th} roots of unity. Therefore, Lemma 3.1.7 shows that if $q \neq 3$, then the entries of K and L are not roots of unity, so K and L cannot be Butson Hadamard matrices. □

The following corollary is an immediate consequence of Theorems 3.1.4 and 3.1.8.

Corollary 3.1.9. *Let $q \equiv 3 \pmod 4$ be a prime power and let $m \geq 0$ be an integer. If there is a q-suitable pair of $n \times n$ (± 1)-matrices, then there is an unreal $UH(nq^m)$, an unreal $BH(3^m n, 6)$, and an unreal $BH(3^m n, 12)$.*

3.2 A Basic Pair of q-Suitable Matrices

In this section we give a basic example of a q-suitable pair, then appeal to Theorems 3.1.2, 3.1.4, and 3.1.8 to obtain infinite classes of Hadamard matrices, Butson Hadamard matrices, and unit Hadamard matrices. The recursive construction given in Theorem 3.1.4 yields matrices with very predictable and easily studied properties which are completely determined by the base case. In particular, the construction lends itself quite nicely to the

study of the excess and the structure of the matrices it produces, as we shall see in the coming pages.

The most basic pair of q-suitable matrices is undoubtedly (J_1, J_1). Indeed, J_1 is obviously amicable with itself, and for any q we have $J_1 J_1^T + q J_1 J_1^T = (q+1) I_1$. Therefore, the results of Section 3.1 allow us to use J_1 to construct infinite classes of Hadamard matrices, Butson Hadamard matrices, and unit Hadamard matrices.

For each odd prime power q and integer $m \geq 0$, let

$$\mathcal{J}_m^{(q)} = \begin{cases} J_1 & \text{if } m = 0 \\ J_q \otimes \mathcal{A}_{m-1}^{(q)} & \text{otherwise} \end{cases} \qquad \mathcal{A}_m^{(q)} = \begin{cases} J_1 & \text{if } m = 0 \\ I_q \otimes \mathcal{J}_{m-1}^{(q)} + Q \otimes \mathcal{A}_{m-1}^{(q)} & \text{otherwise} \end{cases}$$

and

$$\mathcal{C}_m^{(q)} = \begin{cases} J_1 & \text{if } m = 0 \\ J_q \otimes \mathcal{D}_{m-1}^{(q)} & \text{otherwise} \end{cases} \qquad \mathcal{D}_m^{(q)} = \begin{cases} J_1 & \text{if } m = 0 \\ I_q \otimes \mathcal{C}_{m-1}^{(q)} + i\,Q \otimes \mathcal{D}_{m-1}^{(q)} & \text{otherwise} \end{cases}.$$

Since J_1 is q-suitable with itself, Theorem 3.1.2 immediately yields the following matrices:

(i) $\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_m^{(q)} + I'_{q+1} \otimes \mathcal{J}_m^{(q)}$ is a Hadamard matrix of order $q^m(q+1)$ if $q \equiv 3 \pmod 4$

(ii) $\begin{pmatrix} 0 & j_q \\ -j_q^T & Q \end{pmatrix} \otimes \mathcal{D}_m^{(q)} + iI'_{q+1} \otimes \mathcal{C}_m^{(q)}$ is a BH$(q^m(q+1), 4)$ if $q \equiv 1 \pmod 4$.

Similarly, Theorem 3.1.8 yields:

(iii) $\frac{1}{\sqrt{q+1}} \mathcal{J}_m^{(q)} + i\sqrt{\frac{q}{q+1}}\,\mathcal{A}_m^{(q)}$ is an unreal unit Hadamard matrix of order q^m whenever $q \equiv 3 \pmod 4$. If $q = 3$, then it's an unreal BH$(3^m, 6)$.

(iv) $\sqrt{\frac{q}{q+1}}\,\mathcal{A}_m^{(q)} + i\frac{1}{\sqrt{q+1}} \mathcal{J}_m^{(q)}$ is an unreal unit Hadamard matrix of order q^m whenever $q \equiv 3 \pmod 4$. If $q = 3$, then it's an unreal BH$(3^m, 12)$.

Furthermore, Theorem 3.1.8 tells us that if $q \neq 3$, then the matrices in (iii) and (iv) are not Butson Hadamard matrices. It should be noted that unreal BH$(3^m, 6)$'s were already recently discovered by Compton et al. [5]. However, the unreal BH$(3^m, 6)$'s constructed with $\mathcal{J}_m^{(3)}$ and $\mathcal{A}_m^{(3)}$ in (iii) enjoy two properties lacked by the matrices discovered by Compron et al.: they have maximum excess and can be constructed to be multicirculant by using the appropriate Jacobsthal matrix Q to obtain $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$. This shall be proved in Section 3.2.2. First, however, in Section 3.2.1 we study the properties of the matrices in (i).

3.2.1 An Infinite Class of Hadamard Matrices with Large Excess

In this section we turn our attention to the excess of the Hadamard matrices of order $q^m(q+1)$ we constructed from $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$, where $q \equiv 3 \pmod 4$ is a prime power. In doing so, we will find that $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ lead us to an infinite family of Hadamard matrices with large excess. Using these matrices, we will obtain a lower bound for the maximal excess of a Hadamard matrix of order $q^m(q+1)$. Of particular interest, $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ give an infinite family of regular Hadamard matrices when m is even and $q = 3$. For brevity, throughout this section we will use $H_m^{(q)}$ to denote the Hadamard matrices of order $q^m(q+1)$ obtained from $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$. That is,

$$H_m^{(q)} = \begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_m^{(q)} + I'_{q+1} \otimes \mathcal{J}_m^{(q)}.$$

Where no ambiguity arises, we will supress the superscripts on $H_m^{(q)}$, $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$.

Proposition 3.1.5 suggests that we must study the excess of $H_m^{(q)}$ in two cases: first when m is even, and again when m is odd. The even case is the simplest, and we'll pursue it first. Using Proposition 3.1.5 it is straightforward to determine the excess of $H_{2m}^{(q)}$. This result is

summarized as follows.

Proposition 3.2.1. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. Then*

$$\sigma(H_{2m}^{(q)}) = q^{3m}(3q-1).$$

Moreover, $\sigma(H_{2m}^{(q)}) = (q^{2m}(q+1))^{3/2}$ if and only if $q = 3$.

Proof. Using Proposition 3.1.5 and the fact that $S(Q) = 0$, we obtain

$$\begin{aligned} S(H_{2m}) &= S\left(\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_{2m} + I'_{q+1} \otimes \mathcal{J}_{2m}\right) \\ &= 2q\,S(\mathcal{A}_{2m}) + (q-1)\,S(\mathcal{J}_{2m}) \\ &= 2q^{3m+1}S(J_1) + (q-1)q^{3m}S(J_1) \\ &= q^{3m}(3q-1). \end{aligned}$$

Thus $\sigma(H_{2m}) = q^{3m}(3q-1)$. For the next part of the lemma, suppose $\sigma(H_{2m}^{(q)}) = (q^{2m}(q+1))^{3/2}$. Then

$$q^{3m}(3q-1) = (q^{2m}(q+1))^{3/2}.$$

Cancelling q^{3m} from both sides, squaring, then rearranging gives:

$$q(q-3)^2 = 0.$$

Since $q > 0$, it follows that $q = 3$. The converse is true since $\sigma(H_{2m}) = q^{3m}(3q-1)$. □

Recall now from Chapter 2 that $n\sqrt{n}$ is an upper bound for the excess of any Hadamard matrix of order n and that the excess of a Hadamard matrix attains this upper bound if and only if the matrix is regular. This implies the following two corollaries to Proposition 3.2.1.

Corollary 3.2.2. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. Then $H_{2m}^{(q)}$ is regular if and only if $q = 3$.*

Corollary 3.2.3. *Let $m \geq 0$ be an integer and $q \equiv 3 \pmod 4$ be a prime power. Then*

$$\sigma_R(q^{2m}(q+1)) \geq q^{3m}(3q-1)$$

and

$$\sigma_R(4 \cdot 3^{2m}) = (4 \cdot 3^{2m})^{3/2}.$$

Next, we turn our attention to the Hadamard matrices $H_{2m+1}^{(q)}$. Ultimately, we will establish a lower bound for the excess of these matrices by negating appropriate rows and columns. To this end, we introduce some new notation.

Notation 3.2.1. Let $B = \left(b_{ij}\right)$ be an $n \times m$ matrix. Index the rows and columns of B by $1,2,...,n$ and $1,2,...,m$ respectively. For each $i \in \{1,2,...,n\}$ and $j \in \{1,2,...,m\}$, let $\rho_i(B)$ denote the number of ones in the i^{th} row of B, and let $\kappa_j(B)$ denote the number of ones in the j^{th} column of B. In other words,

$$\rho_i(B) = \sum_{\substack{k \in \{1,...,m\} \\ b_{ik}=1}} 1$$

and

$$\kappa_j(B) = \sum_{\substack{k \in \{1,...,n\} \\ b_{kj}=1}} 1.$$

Lemma 3.2.4. *Let $m \geq 0$ be an integer, let $q \equiv 3 \pmod 4$ be a prime power, let $i \in \{1,2,...,q^{2m}\}$, and let $j \in \{1,2,...,q^{2m+1}\}$. Then both of the following hold:*

(i) $\rho_i(\mathcal{A}_{2m}^{(q)}) = \kappa_i(\mathcal{A}_{2m}^{(q)}) = \frac{q^m(q^m+1)}{2}$

(ii) $\rho_j(\mathcal{A}_{2m+1}^{(q)}) = \kappa_j(\mathcal{A}_{2m+1}^{(q)}) = \frac{q^m(q^{m+1}+1)}{2}$.

Proof. First it should be recalled that if $m \geq 2$, then

$$\mathcal{A}_m = I_q \otimes \mathcal{J}_{m-1} + Q \otimes \mathcal{A}_{m-1} = I_q \otimes J_q \otimes \mathcal{A}_{m-2} + Q \otimes \mathcal{A}_{m-1}.$$

Now observe that since the main diagonal of Q is composed entirely of zeros, the entry in the k^{th} row and l^{th} column of $I_q \otimes J_q \otimes \mathcal{A}_{m-2}$ is nonzero if and only if the entry in the k^{th} row and l^{th} column of $Q \otimes \mathcal{A}_{m-1}$ is zero. Therefore, for each $i \in \{1, 2, \ldots, q^m\}$ we have

$$\begin{aligned} \rho_i(\mathcal{A}_m) &= \rho_i(I_q \otimes J_q \otimes \mathcal{A}_{m-2} + Q \otimes \mathcal{A}_{m-1}) \\ &= \rho_i(I_q \otimes J_q \otimes \mathcal{A}_{m-2}) + \rho_i(Q \otimes \mathcal{A}_{m-1}). \end{aligned}$$

Together with the fact that each row and column of Q contains $\frac{q-1}{2}$ ones, $\frac{q-1}{2}$ negative ones, and a single zero, this implies that for each $i \in \{1, 2, ..., q^m\}$ and $m \geq 2$ we have

$$\rho_i(\mathcal{A}_m) = q\,\rho_a(\mathcal{A}_{m-2}) + \frac{q^{m-1}(q-1)}{2} \tag{3.3}$$

and

$$\kappa_i(\mathcal{A}_m) = q\,\kappa_a(\mathcal{A}_{m-2}) + \frac{q^{m-1}(q-1)}{2}, \tag{3.4}$$

where a denotes the unique element of $\{1, 2, ..., q^{m-2}\}$ such that $i \equiv a \pmod{q^{m-2}}$. From here we prove (i) and (ii).

(i) We induct on m. First we prove $\rho_i(\mathcal{A}_{2m}) = \frac{q^m(q^m+1)}{2}$. For the base case, recall that $\mathcal{A}_0 = J_1$, so $\rho_1(\mathcal{A}_0) = 1$. Now let $k \geq 0$ be an integer and suppose the lemma holds for $m = k$. Let $i \in \{1, 2, ..., q^{2(k+1)}\}$ and let a denote the unique element of $\{1, 2, ..., q^{2k}\}$

such that $i \equiv a \pmod{q^{2k}}$. Applying Equation (3.3) gives

$$\begin{aligned}\rho_i(\mathcal{A}_{2(k+1)}) &= q\,\rho_a(\mathcal{A}_{2k}) + \frac{q^{2k+1}(q-1)}{2} \\ &= q \cdot \frac{q^k(q^k+1)}{2} + \frac{q^{2k+1}(q-1)}{2} \\ &= \frac{q^{k+1}(q^{k+1}+1)}{2},\end{aligned}$$

where the second line follows from the induction hypothesis. Thus $\rho_i(\mathcal{A}_{2m}) = \frac{q^m(q^m+1)}{2}$ for all positive integers m. The validity of the formula $\kappa_i(\mathcal{A}_{2m}) = \frac{3^m(3^m+1)}{2}$ can be demonstrated by replacing ρ with κ in the above proof, and by appealing to Equation (3.4) instead of Equation (3.3).

(ii) This part can be proved with an almost identical induction to the proof of (i).

□

Corollary 3.2.5. *Let $m \geq 0$ be an integer, let $q \equiv 3 \pmod 4$ be a prime power, and let $i \in \{1, 2, .., q^{2m+1}\}$. Then*

$$\rho_i(\mathcal{J}^{(q)}_{2m+1}) = \kappa_i(\mathcal{J}^{(q)}_{2m+1}) = \frac{q^{m+1}(q^m+1)}{2}.$$

Proof. The corollary is easily verified for $m = 0$, so assume $m > 0$. In that case we have

$$\mathcal{J}_{2m+1} = J_q \otimes \mathcal{A}_{2m},$$

hence

$$\rho_i(\mathcal{J}_{2m+1}) = q\,\rho_a(\mathcal{A}_{2m})$$

and

$$\kappa_i(\mathcal{J}_{2m+1}) = q\,\kappa_a(\mathcal{A}_{2m}),$$

where a is the unique element of $\{1,2,...,q^{2m}\}$ such that $i \equiv a \pmod{q^{2m}}$. The corollary follows by applying Lemma 3.2.4. □

Lemma 3.2.6. *Let $m \geq 0$ be an integer, let $q \equiv 3 \pmod 4$ be a prime power, and consider the Hadamard matrix $H_{2m+1}^{(q)}$. The first q^{2m+1} row sums of $H_{2m+1}^{(q)}$ are zero. Likewise, the first q^{2m+1} column sums of $H_{2m+1}^{(q)}$ are zero.*

Proof. Due to Lemma 3.2.4 and the definitions of H_{2m+1} and $\mathcal{J}_{2m+1}$, it suffices to only show that the first q^{2m+1} row sums of H_{2m+1} are zero. Now note that since the first row of I'_{q+1} is $(-1,0,0,\ldots,0)$, for each $i \in \{1,\ldots,q^{2m+1}\}$ we have

$$\rho_i\left(I'_{q+1} \otimes \mathcal{J}_{2m+1}\right) = q^{2m+1} - \rho_i(\mathcal{J}_{2m+1}).$$

Together with Lemma 3.2.4 and Corollary 3.2.5, this implies that for each $i \in \{1,...,q^{2m+1}\}$ we have

$$\begin{aligned}
\rho_i\left(H_{2m+1}\right) &= \rho_i\left(\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_{2m+1} + I'_{q+1} \otimes \mathcal{J}_{2m+1}\right) \\
&= \rho_i\left(\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_{2m+1}\right) + \rho_i\left(I'_{q+1} \otimes \mathcal{J}_{2m+1}\right) \\
&= q\rho_i(\mathcal{A}_{2m+1}) + q^{2m+1} - \rho_i(\mathcal{J}_{2m+1}) \\
&= \frac{q^{m+1}(q^{m+1}+1)}{2} + q^{2m+1} - \frac{q^{m+1}(q^m+1)}{2} \\
&= \frac{q^{2m+1}(q+1)}{2}
\end{aligned}$$

Therefore, each of the first q^{2m+1} rows of H_{2m+1} contains $\frac{q^{2m+1}(q+1)}{2}$ ones. Since H_{2m+1} is of order $q^{2m+1}(q+1)$, the remaining $\frac{q^{2m+1}(q+1)}{2}$ entries in each of the first q^{2m+1} rows are negative ones, so each of the first q^{2m+1} row sums of H_{2m+1} are zero. □

Lemma 3.2.7. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. Then*

$$\sigma(H_{2m+1}^{(q)}) = q^{3m+2}(q+1).$$

Proof. Applying Proposition 3.1.5, observe that

$$\begin{aligned} S(H_{2m+1}) &= S\left(\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_{2m+1} + I'_{q+1} \otimes \mathcal{J}_{2m+1}\right) \\ &= 2q^{3m+2}S(\mathcal{J}_0) + (q-1)q^{3m+2}S(\mathcal{A}_0) \\ &= q^{3m+2}(q+1). \end{aligned}$$

The result is now immediate. □

When $q \equiv 3 \pmod 4$ is a prime power, the following lemma will help us to establish a lower bound for $\sigma_R(q^{2m+1}(q+1))$.

Lemma 3.2.8 (Kharaghani, [13])**.** *Let $H = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$ and $G = \begin{pmatrix} A & -C \\ -B & D \end{pmatrix}$ be two block matrices. If $S(B) = S(C) = -S(A)$, then $S(G) = S(H) + 4S(A)$.*

Proof. Observe that

$$\begin{aligned} S(H) + 4S(A) &= S(A) + S(B) + S(C) + S(D) + 4S(A) \\ &= S(A) - S(A) - S(A) + S(D) + 4S(A) \\ &= S(A) - S(B) - S(C) + S(D) \\ &= S(G). \end{aligned}$$

□

Theorem 3.2.9. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. Then*

$$\sigma_R(q^{2m+1}(q+1)) \geq q^{3m+2}(q+1) + 2q^{m+2}(q^m-1).$$

Proof. Recall that

$$H_{2m+1} = \begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_{2m+1} + I'_{q+1} \otimes \mathcal{J}_{2m+1}.$$

We show that by negating q rows and q columns of H_{2m+1}, we obtain a Hadamard matrix of excess $q^{3m+2}(q+1) + 2q^{m+2}(q^m-1)$. By Lemma 3.2.6, the first q^{2m+1} row and column sums of H_{2m+1} are zero. Since $-\mathcal{J}_{2m+1} = -J_q \otimes \mathcal{A}_{2m}$, it is clear that rows

$$1, q^{2m}+1, 2\cdot q^{2m}+1, \ldots, (q-1)q^{2m}+1$$

of $-\mathcal{J}_{2m+1}$ are all the same. Moreover, Corollary 3.2.5 tells us that there are exactly

$$q^{2m+1} - \frac{q^{m+1}(q^m+1)}{2} = \frac{q^{m+1}(q^m-1)}{2}$$

ones in each of these q identical rows. Therefore, by permuting the corresponding rows and columns of H_{2m+1} we can obtain an equivalent Hadamard matrix with a $q \times \frac{q^{m+1}(q^m-1)}{2}$ block of ones in its top left-hand corner and whose first q^{2m+1} row and column sums are zero. Call this new Hadamard matrix H'_{2m+1}. Notice that $S(H'_{2m+1}) = S(H_{2m+1})$. Now negate the first q rows and the first $\frac{q^{m+1}(q^m-1)}{2}$ columns of H'_{2m+1} to obtain a third equivalent Hadamard matrix, say H''_{2m+1}. Then H'_{2m-1} and H''_{2m-1} satisfy the conditions of Lemma 3.2.8, so

$$S(H''_{2m+1}) = S(H_{2m+1}) + 4 \cdot \frac{q^{m+2}(q^m-1)}{2}.$$

Appealing to Lemma 3.2.7 and simplifying, we obtain:

$$S(H''_{2m+1}) = q^{3m+2}(q+1) + 2q^{m+2}(q^m - 1).$$

It follows that $\sigma_R(q^{2m+1}(q+1)) \geq q^{3m+2}(q+1) + 2q^{m+2}(q^m-1)$. □

It is interesting to asymptotically compare the lower bound for $\sigma_R(q^{2m+1}(q+1))$ given by Theorem 3.2.9 with Best's upper bound $(q^{2m+1}(q+1))^{3/2}$ given by Theorem 2.7.2. Doing so, one can use the squeeze theorem to find

$$\lim_{m\to\infty} \frac{(q^{2m+1}(q+1))^{3/2}}{q^{3m+2}(q+1) + 2q^{m+2}(q^m-1)} = \sqrt{\frac{q+1}{q}}. \tag{3.5}$$

This suggests that the two bounds are very similar asymptotically. In Table 3.1, we explicitly compare these bounds for orders less than 1000. The bounds compare very well for all cases shown in the table except the last line, when $q = 3$ and $m = 2$. In fact, the lower bound given by Theorem 3.2.9 meets the largest known excess given by Jenkins et al. [12] in all cases except when $q = 3$, $m = 2$. Moreover, our bound is known to be the maximum excess when $q = 3$ and $m = 0$ [2]. Together with the asymptotic comparison in Equation (3.5), this suggests the following problem.

Problem 3.2.2. Let $m \geq 0$ be an integer, let $q \equiv 3 \pmod 4$ be a prime power, and let $\mathcal{C}$ be the set of all Hadamard matrices equivalent to $H^{(q)}_{2m+1}$. Does the following equation hold?

$$\max_{H\in\mathcal{C}} \sigma(H) \stackrel{?}{=} q^{3m+2}(q+1) + 2q^{m+2}(q^m-1).$$

Table 3.1: Excess of Hadamard Matrices of Order $q^{2m+1}(q+1) < 1000$

Order $q^{2m+1}(q+1)$	q	m	Best's Bound $(q^{2m+1}(q+1))^{\frac{3}{2}}$	Theorem 3.2.9 Bound
12	3	0	42	36**
56	7	0	419	392*
108	3	1	1122	1080*
132	11	0	1517	1452*
380	19	0	7408	7220*
552	23	0	12969	12696*
756	27	0	20787	20412*
972	3	2	30304	27540

* largest known excess according to [12]

** maximum excess

3.2.2 An Infinite Class of Unreal Multicirculant Unit Hadamard Matrices of Maximum Excess

Recall that when $q \equiv 3 \pmod 4$ is a prime power, $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ give us the following infinite classes.

(i) $\frac{1}{\sqrt{q+1}}\mathcal{J}_m^{(q)} + i\sqrt{\frac{q}{q+1}}\mathcal{A}_m^{(q)}$ is an unreal unit Hadamard matrix of order q^m. If $q = 3$, then it's an unreal BH$(3^m, 6)$.

(ii) $\sqrt{\frac{q}{q+1}}\mathcal{A}_m^{(q)} + i\frac{1}{\sqrt{q+1}}\mathcal{J}_m^{(q)}$ is an unreal unit Hadamard matrix of order q^m. If $q = 3$, then it's an unreal BH$(3^m, 12)$.

At the beginning of Section 3.2, we commented that the unreal BH$(3^m, 6)$'s in (i) have maximum excess and can be constructed to be multicirculant by using the appropriate choice of Jacobsthal matrix Q in the definition of $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$. This distinguishes our BH$(3^m, 6)$'s from the unreal BH$(3^m, 6)$'s obtained by Compton et al. in [5]. However, the unreal BH$(3^m, 6)$'s in (i) are not the only multicirculant, orthogonal matrices we can obtain from $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$. In this section we will show that all of the unit Hadamard matrices of order q^m in (i) and (ii) have maximum excess and can be constructed in such a way that they are multicirculant.

Lemma 3.2.10. *Let $m \geq 0$ be an integer and $q \equiv 3 \pmod 4$ a prime power. By using the correct Jacobsthal matrix in the definition of $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$, it is possible to make $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ multicirculant.*

Proof. Recall the definition of $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$.

$$\mathcal{J}_m^{(q)} = \begin{cases} J_1 & \text{if } m = 0 \\ J_q \otimes \mathcal{A}_{m-1}^{(q)} & \text{otherwise} \end{cases} \qquad \mathcal{A}_m^{(q)} = \begin{cases} J_1 & \text{if } m = 0 \\ I_q \otimes \mathcal{J}_{m-1}^{(q)} + Q \otimes \mathcal{A}_{m-1}^{(q)} & \text{otherwise.} \end{cases}$$

We know from Proposition 2.5.9 that we can choose the Jacobsthal matrix Q in this definition to be multicirculant. Now recall that the Kronecker product of multicirculant matrices is multicirculant, and that the sum of two multicirculant matrices is multicirculant as long as all of the multicirculant blocks in both summands have the same dimensions. Using these facts together with the fact that J_q and I_q are multicirculant, a simple induction shows $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ are multicirculant whenever Q is multicirculant. □

Theorem 3.2.11. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. Then there exists an unreal multicirculant unit Hadamard matrix of order q^m with excess $q^{\frac{3m}{2}}$. Moreover, there exists an unreal multicirculant $BH(3^m, 6)$ and $BH(3^m, 12)$, both with excess $3^{\frac{3m}{2}}$.*

Proof. According to Lemma 3.2.10, we can choose $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ to be multicirculant. Let

$$K_m^{(q)} = \frac{1}{\sqrt{q+1}} \mathcal{J}_m^{(q)} + i\sqrt{\frac{q}{q+1}} \mathcal{A}_m^{(q)}$$

and

$$L_m^{(q)} = \sqrt{\frac{q}{q+1}} \mathcal{A}_m^{(q)} + i\frac{1}{\sqrt{q+1}} \mathcal{J}_m^{(q)}.$$

We established at the beginning of Section 3.2 that these matrices are unreal unit Hadamard matrices of order q^m. Since $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$ are multicirculant and all their multicirculant blocks have the same dimensions, $K_m^{(q)}$ and $L_m^{(q)}$ are also multicirculant. To compute the

excess of $K_m^{(q)}$ and $L_m^{(q)}$ we consider separately the cases when m is odd and even. First, use Proposition 3.1.5 to observe that

$$\begin{aligned} S\left(K_{2m}^{(q)}\right) &= \frac{1}{\sqrt{q+1}} S(\mathcal{J}_{2m}) + i\sqrt{\frac{q}{q+1}} S(\mathcal{A}_{2m}) \\ &= \frac{1}{\sqrt{q+1}} q^{3m} S(\mathcal{J}_0) + i\sqrt{\frac{q}{q+1}} q^{3m} S(\mathcal{A}_0) \\ &= \frac{q^{3m}}{\sqrt{q+1}} (1 + i\sqrt{q}) . \end{aligned}$$

Therefore,

$$\sigma\left(K_{2m}^{(q)}\right) = \left| \frac{q^{3m}}{\sqrt{q+1}} (1 + i\sqrt{q}) \right| = q^{\frac{3(2m)}{2}}.$$

Using a similar computation one can show that

$$\sigma\left(K_{2m+1}^{(q)}\right) = q^{\frac{3(2m+1)}{2}}.$$

Therefore, for any $m \geq 0$ we have

$$\sigma\left(K_m^{(q)}\right) = q^{\frac{3m}{2}}.$$

Similarly, one can show that

$$\sigma\left(L_m^{(q)}\right) = q^{\frac{3m}{2}}.$$

Finally, Theorem 3.1.8 tells us that if $q = 3$, then $K_m^{(q)}$ and $L_m^{(q)}$ are BH$(3^m, 6)$'s and BH$(3^m, 12)$'s respectively, which completes the proof. □

Corollary 3.2.12. *If $m \geq 0$ is an integer and $q \equiv 3 \pmod 4$ is a prime power, then*

$$\sigma_U(q^m) = q^{\frac{3m}{2}}.$$

Proof. Since $n\sqrt{n}$ is an upper bound for the excess of any unit Hadamard matrix of order n, Theorem 3.2.11 implies the result. □

3.2.3 A Family of BIBDs

As a final application of $\mathcal{J}_m^{(q)}$ and $\mathcal{A}_m^{(q)}$, we show that they can be used to obtain a BIBD with parameters $q^{2m+2}, q^{2m+1}(q+1), \frac{q^m(q^{m+1}-1)(q+1)}{2}, \frac{q^{m+1}(q^{m+1}-1)}{2}, \frac{q^m(q^{m+1}-2)(q+1)}{4}$ for each prime power $q \equiv 3 \pmod 4$ and integer $m \geq 0$.

Theorem 3.2.13. *There is a* $(q^{2m+2}, \frac{q^{m+1}(q^{m+1}-1)}{2}, \frac{q^m(q^{m+1}-2)(q+1)}{4})$*-design for each integer* $m \geq 0$ *and prime power* $q \equiv 3 \pmod 4$.

Proof. Let

$$M = \begin{pmatrix} j_q^T & Q \end{pmatrix} \otimes \mathcal{A}_{2m+1} + \begin{pmatrix} 0_{q\times 1} & I_q \end{pmatrix} \otimes \mathcal{J}_{2m+1},$$

where $0_{q\times 1}$ denotes the $q \times 1$ zero matrix. Since $\mathcal{A}_{2m+1}$ and $\mathcal{J}_{2m+1}$ are q-suitable, Theorem 3.1.2 tells us that the row vectors of M are mutually orthogonal and that M is a (± 1)-matrix. Now let $\hat{J}$ be the $q^{2m+2} \times q^{2m+1}(q+1)$ all-ones matrix and let $B = \frac{1}{2}(\hat{J} - M)$. We use Theorem 2.8.5 to show that B is the incidence matrix of a $(q^{2m+2}, \frac{q^{m+1}(q^{m+1}-1)}{2}, \frac{q^m(q^{m+1}-2)(q+1)}{4})$-design. It is clear from the definitions of $\hat{J}$ and M that B is a $(0,1)$-matrix. Using the fact that the row vectors of M are mutually orthogonal, notice that

$$\begin{aligned} BB^T &= \frac{1}{4}(\hat{J} - M)(\hat{J}^T - M^T) \\ &= \frac{1}{4}(q^{2m+1}(q+1)J_{q^{2m+2}} - \hat{J}M^T - M\hat{J}^T + q^{2m+1}(q+1)I_{q^{2m+2}}). \end{aligned} \tag{3.6}$$

Next, observe that Lemma 3.2.4 and Corollary 3.2.5 imply that all row sums of M are equal to $q^m(q+1)$. Applying this fact to Equation (3.6) yields:

$$\begin{aligned} BB^T &= \frac{1}{4}(q^{2m+1}(q+1)J_{q^{2m+2}} - 2q^m(q+1)J_{q^{2m+2}} + q^{2m+1}(q+1)I_{q^{2m+2}}) \\ &= \frac{q^m(q^{m+1}-2)(q+1)}{4}J_{q^{2m+2}} + \left(\frac{q^m(q^{m+1}-1)(q+1)}{2} - \frac{q^m(q^{m+1}-2)(q+1)}{4}\right)I_{q^{2m+2}}. \end{aligned} \tag{3.7}$$

Now note that Lemma 3.2.4 and Corollary 3.2.5 imply that all column sums of B are equal

to $\frac{q^{m+1}(q^m-1)}{2}$. It follows that

$$J_{q^{2m+2}}B = \frac{q^{m+1}(q^{m+1}-1)}{2}\hat{f}. \tag{3.8}$$

Finally, observe that

$$\frac{q^{m+1}(q^{m+1}-1)}{2} < q^{2m+2}. \tag{3.9}$$

Theorem 2.8.5 together with Equations (3.7), (3.8) and (3.9) imply that B is the incidence matrix of a $(q^{2m+2}, \frac{q^{m+1}(q^{m+1}-1)}{2}, \frac{q^m(q^{m+1}-2)(q+1)}{4})$-design. □

3.3 A Second Example of q-Suitable Matrices

In this section we'll explore a second example of a q-suitable pair. Again, we will use Theorem 3.1.4 to explode the pair of q-suitable matrices into an infinite class of q-suitable matrices, thereby obtaining an infinite class of Hadamard matrices from Theorem 3.1.2. Similar to our first example of q-suitable matrices, we will find that the Hadamard matrices obtained in this section will again have large excess. Without further ado, let's examine the motivation for our next construction.

Let Y be the core of a symmetric, standardized Hadamard matrix of order $n+1$. Let X be the $n \times n$ matrix defined by $X = \text{circ}(-,1,1,\ldots,1)$. It's straightforward to see that

$$XX^T = 4I_n + (n-4)J_n$$

and

$$YY^T = (n+1)I_n - J_n.$$

Therefore,

$$XX^T + (n-4)YY^T = n(n-3)I_n.$$

This suggests that if $n-4$ is equal to some odd prime power q, then there's hope that (Y,X)

may be a q-suitable pair (of course, we'd still need to check amicability). It's straightforward to check for which q we have $n-4=q$. Indeed, assume $n-4=q$. Then since $n+1$ is the order of a Hadamard matrix, we must have $q+4=n\equiv 3 \pmod 4$, so $q\equiv 3 \pmod 4$. Therefore, (Y,X) is a q-suitable pair if $n=q+4$ for some prime power $q\equiv 3 \pmod 4$ and if X and Y are amicable. It turns out that it's not difficult to establish the amicability of X and Y, as we will show in the proof of the following proposition.

Proposition 3.3.1. *Let $q\equiv 3 \pmod 4$ be a prime power, let X be the $(q+4)\times(q+4)$ matrix defined by $X=circ(-,1,1,\ldots,1)$, and let Y be the core of a symmetric, standardized Hadamard matrix of order $q+5$. Then (Y,X) is a q-suitable pair.*

Proof. We proved above that $XX^T+qYY^T=(q+1)(q+4)I_{q+4}$, so it remains to show that X and Y are amicable. Note that $X=J_{q+4}-2I_{q+4}$. Also, since Y is the core of a symmetric, standardized Hadamard matrix, we have $J_{q+4}Y^T=YJ_{q+4}=-J_{q+4}$. Therefore,

$$XY^T=(J_{q+4}-2I_{q+4})Y^T=-J_{q+4}-2Y^T=-J_{q+4}-2Y=Y(J_{q+4}-2I_{q+4})^T=YX^T.$$

Thus X and Y are amicable, so (Y,X) is a q-suitable pair as claimed. □

Let q, X, and Y be as described in Proposition 3.3.1. Since (Y,X) is a q-suitable pair, it is easy to see that $(-Y,X)$ is also q-suitable. In what follows, we will work with $-Y$ and X in lieu of Y and X for reasons that shall be explained shortly. Since the pair $(-Y,X)$ is q-suitable, we can use $-Y$ and X along with the results of Section 3.1 to obtain infinite classes of Hadamard, Butson Hadamard, and unit Hadamard matrices. More specifically, let

$$\mathcal{X}_m^{(q)}=\begin{cases}X & \text{if } m=0\\ J_q\otimes\mathcal{Y}_{m-1}^{(q)} & \text{otherwise}\end{cases}\qquad \mathcal{Y}_m^{(q)}=\begin{cases}-Y & \text{if } m=0\\ I_q\otimes\mathcal{X}_{m-1}^{(q)}+Q\otimes\mathcal{Y}_{m-1}^{(q)} & \text{otherwise.}\end{cases} \tag{3.10}$$

Then Theorem 3.1.4 and Proposition 3.3.1 tell us that the matrices $\mathcal{X}_m^{(q)}$ and $\mathcal{Y}_m^{(q)}$ are amicable and that

$$\mathcal{X}_m^{(q)}(\mathcal{X}_m^{(q)})^T + q\mathcal{Y}_m^{(q)}(\mathcal{Y}_m^{(q)})^T = q^m(q+4)(q+1)I_{(q+4)q^m}.$$

Therefore, Theorem 3.1.2 implies

(i) $\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{Y}_m^{(q)} + I'_{q+1} \otimes \mathcal{X}_m^{(q)}$ is a Hadamard matrix of order $q^m(q+1)(q+4)$ whenever $q \equiv 3 \pmod 4$

Similarly, Theorem 3.1.8 yields:

(ii) $\frac{1}{\sqrt{q+1}}\mathcal{X}_m^{(q)} + i\sqrt{\frac{q}{q+1}}\mathcal{Y}_m^{(q)}$ is an unreal unit Hadamard matrix of order $q^m(q+4)$. If $q = 3$, then it's an unreal BH$(7 \cdot 3^m, 6)$.

(iii) $\sqrt{\frac{q}{q+1}}\mathcal{Y}_m^{(q)} + i\frac{1}{\sqrt{q+1}}\mathcal{X}_m^{(q)}$ is an unreal unit Hadamard matrix of order $q^m(q+4)$. If $q = 3$, then it's an unreal BH$(7 \cdot 3^m, 12)$.

It should be noted that unreal Butson Hadamard matrices of the same parameters as in (ii) and (iii) can be obtained from the work of Compton et al. in [5]. Unfortunately, the unreal Butson Hadamard matrices in (ii) and (iii) do not enjoy the same multicirculant structure or maximum excess as those presented in Section 3.2. Instead, they merely provide an alternate construction to that given by Compton et al.

The matrices from (i) can be used to obtain another interesting lower bound for the maximum excess problem. It is straightforward to compute the excess of these matrices using Proposition 3.1.5, and the outcomes of these computations are given in the following two theorems.

Theorem 3.3.2. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. If there is a symmetric, standardized Hadamard matrix of order $q+5$, then*

$$\sigma_R(q^{2m}(q+1)(q+4)) \geq q^{3m}(q+1)(q+2)(q+4).$$

Proof. Let $X = J_{q+4} - 2I_{q+4}$ and let Y be the core of a symmetric, standardized Hadamard matrix of order $q+5$. Form the matrices $\mathcal{X}_{2m}^{(q)}$ and $\mathcal{Y}_{2m}^{(q)}$ as defined in Equation (3.10). Then, as established above this theorem, the following is a Hadamard matrix of order $q^{2m}(q+1)(q+4)$.

$$\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{Y}_{2m}^{(q)} + I'_{q+1} \otimes \mathcal{X}_{2m}^{(q)}$$

Negating the first $q^{2m}(q+4)$ columns of this matrix, we obtain an equivalent Hadamard matrix:

$$\begin{pmatrix} 0 & j_q \\ -j_q^T & Q \end{pmatrix} \otimes \mathcal{Y}_{2m}^{(q)} + I_{q+1} \otimes \mathcal{X}_{2m}^{(q)}.$$

Now, using Proposition 3.1.5 observe that

$$\begin{aligned} S\left(\begin{pmatrix} 0 & j_q \\ -j_q^T & Q \end{pmatrix} \otimes \mathcal{Y}_{2m}^{(q)} + I_{q+1} \otimes \mathcal{X}_{2m}^{(q)}\right) &= S(I_{q+1})S(\mathcal{X}_{2m}^{(q)}) \\ &= (q+1)q^{3m}S(X) \\ &= q^{3m}(q+1)(q+2)(q+4). \end{aligned}$$

Thus $\sigma_R(q^{2m}(q+1)(q+4)) \geq q^{3m}(q+1)(q+2)(q+4)$. □

Theorem 3.3.3. *Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. If there is a symmetric, standardized Hadamard matrix of order $q+5$, then*

$$\sigma_R(q^{2m+1}(q+1)(q+4)) \geq q^{3m+2}(q+4)(3q+3).$$

Proof. Let $X = J_{q+4} - 2I_{q+4}$ and let Y be the core of a symmetric, standardized Hadamard matrix of order $q+5$. Form the matrices $\mathcal{X}_{2m+1}^{(q)}$ and $\mathcal{Y}_{2m+1}^{(q)}$ as defined in Equation (3.10). Then, as established above this theorem, the following is a Hadamard matrix of order

$q^{2m+1}(q+1)(q+4)$.

$$\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{Y}_{2m+1}^{(q)} + I'_{q+1} \otimes \mathcal{X}_{2m+1}^{(q)}$$

We compute its excess to prove the theorem. Appealing to Proposition 3.1.5, we have

$$\begin{aligned} S\left(\begin{pmatrix} 0 & j_q \\ j_q^T & Q \end{pmatrix} \otimes \mathcal{Y}_{2m+1}^{(q)} + I'_{q+1} \otimes \mathcal{X}_{2m+1}^{(q)}\right) &= 2qS(\mathcal{Y}_{2m+1}^{(q)}) + (q-1)S(\mathcal{X}_{2m+1}^{(q)}) \\ &= 2qq^{3m+1}S(X) + (q-1)q^{3m+2}S(-Y) \\ &= 2q^{3m+2}(q+2)(q+4) + (q-1)q^{3m+2}(q+4) \\ &= q^{3m+2}(q+4)(3q+3). \end{aligned}$$

Therefore, $\sigma_R(q^{2m+1}(q+1)(q+4)) \geq q^{3m+2}(q+4)(3q+3)$. □

Remark 3.3.4. In the proof of Theorem 3.3.3 we saw the justification for using $-Y$ in the definition of $\mathcal{X}_m^{(q)}$ and $\mathcal{Y}_m^{(q)}$ in lieu of Y. Namely, $S(-Y) > S(Y)$, which helped us obtain a larger lower bound for the maximal excess problem.

Similarly to in Section 3.2, it is interesting to asymptotically compare the lower bounds in Theorems 3.3.2 and 3.3.3 with Best's $n\sqrt{n}$ upper bound given in Theorem 2.7.2. Doing so, one finds

$$\lim_{m\to\infty} \frac{q^{3m}(q+1)(q+2)(q+4)}{(q^{2m}(q+1)(q+4))^{3/2}} = \frac{q+2}{\sqrt{(q+1)(q+4)}} \tag{3.11}$$

$$\lim_{m\to\infty} \frac{q^{3m+2}(q+4)(3q+3)}{(q^{2m+1}(q+1)(q+4))^{3/2}} = \frac{3q^2}{q^{3/2}\sqrt{(q+1)(q+4)}} \tag{3.12}$$

These limits show that asymptotically, the bound given in Theorem 3.3.2 is very similar to Best's $n\sqrt{n}$ bound, while the bound given in Theorem 3.3.3 differs asymptotically from Best's $n\sqrt{n}$ bound by a factor of $q^{1/2}$. In Table 3.2, we explicitly compare these bounds for orders less than 1000. The bounds compare very well for all cases shown in the table except

[ht]

Table 3.2: Excess of Hadamard Matrices of Order $q^m(q+1)(q+4) < 1000$

Order $q^m(q+1)(q+4)$	q	m	Best's Bound	$\mathcal{X}_m^{(q)}, \mathcal{Y}_m^{(q)}$ Construction
28	3	0	148	140*
84	3	1	770	756*
88	7	0	826	792*
180	11	0	2415	2340*
252	3	2	4000	3780*
460	19	0	9866	9660*
616	7	1	15289	12936
648	23	0	16495	16200*
756	3	3	20787	20412*
868	27	0	25573	25172*

* largest known excess according to [12]

** maximum excess

for order 616. In fact, the lower bounds given by Theorems 3.3.2 and 3.3.3 meet the largest known excess given by Jenkins et al. [12] in all cases except for order 616. Moreover, our bound is known to be the maximum excess for orders 28 and 84 [12]. However, it should be noted that the apparent agreement in Table 3.2 of our bounds with Best's bound when m is odd is simply due to the fact that m is small in our table, as is indicated by Equation (3.12). On the other hand, Equation (3.11) suggests that the bounds in Theorem 3.3.2 should compare quite well with Best's bound not only for the smaller values of m shown in the table, but for larger values as well. Together with the fact that our bounds attain the maximum known excesses given in [12] when m is even, this suggests the following problem.

Problem 3.3.1. Let $m \geq 0$ be an integer and let $q \equiv 3 \pmod 4$ be a prime power. Does the following equality hold?

$$\sigma_R(q^{2m}(q+1)(q+4)) \stackrel{?}{=} q^{3m}(q+1)(q+2)(q+4).$$

If it does not hold for each m and q, when does it hold?

Bibliography

[1] J. Andrés Armario. On permanents of Sylvester Hadamard matrices. *ArXiv e-prints*, November 2013.

[2] M.R. Best. The excess of a Hadamard matrix. *Indag. Math.*, 39:357–361, 1977.

[3] A.T. Butson. Generalized Hadamard matrices. *Proc. Amer. Math. Soc.*, 13:894–898, 1962.

[4] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and its Applications*. Chapman & Hall/CRC, 2006.

[5] B Compton, R Craigen, and W De Launey. Unreal BH$(n,6)$'s and Hadamard matrices. *Des., Codes and Cryptogr.*, 79, 2016.

[6] R. Craigen and H. Kharaghani. A recursive method for orthogonal designs. *Metrika*, 62(2):185–193.

[7] R. Craigen and H. Kharaghani. Weaving hadamard matrices with maximum excess and classes with small excess. *Journal of Combinatorial Designs*, 12(4):233–255, 2004.

[8] Seberry J. Evangelaras H., Koukouvinos C. Applications of hadamard matrices. *Journal of Telecommunications and Information Technology*, pages 3 – 10, 2003.

[9] N. Farmakis and S. Kounias. The excess of hadamard matrices and optimal designs. *Discrete Mathematics*, 67(2):165 – 176, 1987.

[10] J. Hadamard. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathmatiques*, 17:240–246, 1893.

[11] Yury J. Ionin and Hadi Kharaghani. A recursive construction for new symmetric designs. *Designs, Codes and Cryptography*, 35(3):303–310.

[12] B.A. Jenkins, C. Koukouvinos, S. Kounias, J. Seberry, and R. Seberry. Some results on the excesses of hadamard matrices. *JCMCC*, 4:155–185, 1989.

[13] H. Kharaghani. An infinite class of Hadamard matrices of maximal excess. *Discrete Math.*, 89:307–312, 1991.

[14] H. Kharaghani and Jennifer Seberry. The excess of complex hadamard matrices. *Graphs and Combinatorics*, 9(1):47–56.

[15] H. Kharaghani and B. Tayfeh-Rezaie. A hadamard matrix of order 428. *J. of Combin. Designs*, 13(6):435–440, 2005.

[16] H. Kharaghani and B. Tayfeh-Rezaie. Hadamard matrices of order 32. *J. of Combin. Designs*, 21(5):212–221, 2013.

[17] C. Koukouvinos and J. Seberry. Hadamard matrices of order 8 (mod 16) with maximal excess. *Discrete Mathematics*, 92(1):173 – 176, 1991.

[18] M. Mitrouli. Sylvester Hadamard matrices revisited. *Spec. Matrices*, 2:120–124, 2014.

[19] R. E. A. C. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.

[20] J. Seberry, B.J. Wysocki, and T.A. Wysocki. On some applications of hadamard matrices. *Metrika*, 62:221–239, 2005.

[21] J.J. Sylvester. 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. *Phil. Mag.*, 34:461–475, 1867.

[22] F. Szöllősi. *Construction, classification and parametrization of complex Hadamard matrices*. PhD thesis, Central European University, 2011.

[23] R.J. Turyn. Sequences with small correlation. In *Error Correcting Codes (H.B. Mann, ed.)*. Wiley, 1968.

[24] R.J. Turyn. Complex Hadamard matrices. In *Combinatorial structures and their applications: proceedings of the Calgary international conference*, pages 435–437, 1970.