5-2016

A Survey on Hadamard Matrices

Adam J. LaClair
University of Tennessee, Knoxville, alaclair@vols.utk.edu

A SURVEY ON HADAMARD MATRICES

by

Adam LaClair

B.S., University of Tennessee Knoxville, 2016

An Honors Thesis
Submitted in Partial Fulfillment of the Requirements for the
Honors Bachelors of Science Degree

Department of Mathematics
in the Undergraduate School
University of Tennessee Knoxville
May, 2016

THESIS APPROVAL

A SURVEY ON HADAMARD MATRICES

By

Adam J. LaClair

A Thesis Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Honors Bachelors of Science

in the field of Honors Mathematics

Approved by:

Remus Nicoară, Director of the Math Honors Program

Undergraduate School
University of Tennessee Knoxville
May 2016

AN ABSTRACT OF THE THESIS OF

Adam J. LaClair, for the Honors Bachelor's of Science degree in Mathematics, at University of Tennessee, Knoxville.

TITLE: A SURVEY ON HADAMARD MATRICES

MAJOR PROFESSOR: Dr. R. Nicoară

In this text, an introductory theory to Hadamard matrices is presented, which includes a presentation of classical theorems, proofs, and examples of Hadamard matrices. After such presentation, this text highlights current results regarding the existence of Butson-type Hadamard matrices. Ultimately, the text concludes with the presentation of the research efforts of A. LaClair, R. Nicoară, N. Geist, C. Worley, and A. Wintenberg in determining the existence of a particular family of Butson-type Hadamard matrices.

DEDICATION

TO MY BROTHER.

ACKNOWLEDGMENTS

I would like to thank Harry Hughes for telling me about CUDA and OpenMP, the Honors and Scholars program of the University of Tennessee for the encouragment and promotion of undergraduate research, my group members, Nathan Geist, Andrew Wintenberg, and Chase Worley, for being able to learn from them while working on this project. Finally, profound thanks goes to Dr. Nicoară for choosing me as one of the participants of this research project - I have learned and benefited so much from this research project - for taking many hours to teach us the theory of Hadamard matrices, for being the most amazing math professor and advisor, and a great friend.

A special thanks goes to my parents for listening to me talk about my research project, supporting me, and offering advice while I have worked on this project.

PREFACE

The proofs, theorems, and examples of this text follows the teachings of Dr. Nicoară over the summer of 2015. While this text is based off the teachings of Dr. Nicoară, all errors, grammatical and logical, omissions of information, or other mistakes are the full responsibility of the author. This text is geared as an elementary introduction to the theory of Hadamard matrices with a focus on preparing the reader to understand the research efforts of the author and his collaborators.

TABLE OF CONTENTS

INTRODUCTION

There are several important remarks that need to be made concerning this text. First, while this text is meant to serve as an elementary introduction to the subject of Hadamard matrices, there are several instances throughout the text where we will assume facts from elementary abstract algebra, linear algebra, set theory, and graph theory. Additionally, we assume a familiarity with basic notations and properties of complex numbers. However, in an effort to make this text more accessible to non-experts, there is an included appendix with notes on quadratic residues and cyclotomic polynomials. An understanding of quadratic residues is needed only for the optional, though interesting, section 2.1 on complex circulant Hadamard matrices. An understanding of cyclotomic polynomials is necessary for chapter 3.

Second, there are numerous exercises throughout this text designed to aid the reader in better understanding the material. All of these exercises should be completed, as many of these results are utilized in the proofs of future theorems.

Finally, this text should be read sequentially as the first chapter develops the most elementary results of Hadamard matrices, the second chapter develops upon these results presenting more profound theorems and results, and the final chapter presents our group's research problem and our efforts to solve this problem. By the conclusion of this text, the reader should be prepared to continue our research efforts and to better understand the current literature on Hadamard matrices.

CHAPTER 1

AN INTRODUCTION TO HADAMARD MATRICES

In mathematics, there are many important classes of matrices, symmetric, orthogonal, Hermitian, etc. Perhaps, less well-known are the Hadamard matrices.

1.1 DEFINITION AND EXAMPLES OF HADAMARD MATRICES

Definition. A matrix $H = (a_{kl})_{k,l}$ having complex entries is said to be **Hadamard** if it satisfies:

1. $|a_{kl}| = 1$
2. All rows of H are mutually orthogonal.

Remark. Recall that for $z, w \in \mathbb{C}^n$ that the inner product on $\mathbb{C}^n$ is defined as

$$z \cdot w := \sum_i z_i \overline{w}_i.$$

From this definition, one readily sees that the following matrices are Hadamard.

Example 1.1.1.

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

Example 1.1.2.

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

1.1.1 Fourier Matrix

At this point, one may wonder for which dimenions is it possible to construct a Hadamard matrix. As it turns out, one can construct a square Hadamard matrix for all $n \in \mathbb{N}$.

Definition. For $n \in \mathbb{N}$, put $\epsilon = e^{\frac{2\pi i}{n}}$, i.e., ϵ is an n-th root of unity. Then, the **Fourier matrix**, denoted F_n, is defined as

$$F_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \epsilon & \epsilon^2 & \dots & \epsilon^{n-1} \\ 1 & \epsilon^2 & (\epsilon^2)^2 & \dots & (\epsilon^2)^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \epsilon^{n-1} & (\epsilon^{n-1})^2 & \dots & (\epsilon^{n-1})^{n-1} \end{pmatrix} = (\epsilon^{kl}) \text{ for } 0 \leq k, l \leq n-1.$$

Exercise. Show that F_n is a Hadamard matrix.

Because F_n has a natural construction for all dimenions, it is often considered to be a *trivial* example of a Hadamard matrix. In the next chapter, we will encounter more complicated examples of Hadamard matrices.

1.1.2 The Adjoint Matrix

In the following, we show a few methods of constructing Hadamard matrices from a given Hadamard matrix.

Definition. Let $H \in M_n(\mathbb{C})$. Then, the **adjoint of H**, denoted by H^*, is defined to be the conjugate transpose of H, i.e., $H^* = \overline{H}^t$.

Lemma 1.1.1. *$H \in M_n(\mathbb{C})$ has orthogonal rows if and only if $H \cdot H^*$ has 0's off of the diagonal of the matrix product. If H is Hadamard, then $H \cdot H^* = nI$.*

Proof. Exercise. □

Exercise. For $H \in M_n(\mathbb{C})$, what is an equivalent reformulation of H^{**}?

Proposition 1.1.2. *If $H \in M_n(\mathbb{C})$ is Hadamard, then H^* is Hadamard.*

Proof. First, observe that all of the entries of H^* are of absolute value 1. Second, observe that by the above lemma that $H \cdot H^* = nI$, and hence that $\frac{1}{n}(H^* \cdot H^{**}) = I$. By the above lemma, this implies that H^* has orthogonal rows, and hence H^* is Hadamard. □

In the remainder of the text, if we say that H is Hadamard, then it is assumed that $H \in M_n(\mathbb{C})$ unless otherwise specified.

Corollary 1.1.3. *If H is Hadamard, then the columns of H are orthogonal.*

Proof. Since H is Hadamard, we know that H^* is also Hadamard, and hence the rows of H^* are orthogonal, but the rows of H^* are precisely the columns of H conjugated. Hence, the columns of H are orthogonal. □

Thus, from this example, we have that seen given a Hadamard matrix, one can obtain a *new* Hadamard matrix via $H \mapsto H^*$.

1.2 EQUIVALENCE CLASS OF HADAMARD MATRICES

In this section, we show two more methods for obtaining Hadamard matrices from an initial Hadamard matrix.

Observe that $\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ is Hadamard, then $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is also Hadamard because we have just permuted the rows. Also, observe that $\begin{pmatrix} 1 & a \\ 1 & -a \end{pmatrix}$ is also Hadamard for all $a \in \mathbb{C}$ with $|a| = 1$.

In general, this leads to the observation that if H is Hadamard, then any permutation of the rows or the columns of H is still a Hadamard matrix. Additionally, multiplication of any row or column by $a \in \mathbb{C}$ with $|a| = 1$ is still a Hadamard matrix. More precisely, we say that

Definition. Hadamard matrices H, K are equivalent iff there exist permutation matrices P_1, P_2 and unitary diagonal matrices D_1, D_2 such that $H = P_1 D_1 K D_2 P_2$.

Exercise. Check the above details, showing that a Hadamard matrix remains Hadamard under arbitrary permutations of rows / columns and / or multiplication by a complex number of absolute value 1.

Exercise. Show that $\sim$ defines an equivalence relation on $M_n(\mathbb{C})$.

The above definition is fundamental because it allows us to study the equivalence class of Hadamard matrices. Thus, a main goal of research related to Hadamard matrices is in determining different equivalence classes of Hadamard matrices, determining ways to distinguish between equivalence classes of Hadamard matrices, and studying the structure of the equivalence class of Hadamard matrices.

From the above, it should be obvious that any Hadamard matrix is equivalent to a Hadamard matrix having 1's on the first row and first column.

Definition. We say that a Hadamard matrix is in **normal form**, **normalized**, or **dephased** if the first row and first column of the matrix consists of only 1's. The part of the matrix within the 1×1 boundary is referred to as the **core** of the matrix.

We study Hadamard matrices exclusively in normal form because this restricts the number of equivalent matrices of H from an infinite set to a finite set. That is if H is a Hadamard matrix in normal form, then the set of equivalent matrices of H in normal form is given by all permutations of the rows and columns of H. In essence, we have removed the option of multiplying rows and columns by a complex number of absolute value 1.

Exercise. Show that F_2 is the only Hadamard matrix of dimenion two upto equivalence.

1.2.1 Haagerup's Invariant

As we remarked upon above, an important problem in the study of Hadamard matrices is the determination of distinct equivalence classes of Hadamard matrices. Below, we

present one such method:

Definition. Haagerup's Invariant of a Hadamard matrix $H = (a_{k,l})$ is the set

$$i(H) = \left\{ a_{i,j} a_{k,l} \overline{a_{k,j} a_{i,l}} \;\middle|\; 1 \leq i, j, k, l \leq n \right.$$

Theorem 1.2.1. *If H, H' are Hadamard matrices satisfying $H \sim H'$, then $i(H) = i(H')$.*

Proof. Exercise. □

It is important to note that Haagerup's invariant is **not** a complete invariant; that is, for general Hadamard matrices, the converse of the above theorem need not be true. In practice, the contrapositive of the above theorem is useful.

Finally, it is worth noting that there exist stronger invariants for determining equivalence of two Hadamard matrices. The interested reader is referred to [6] for a discussion of the *fingerprint* of a matrix.

1.2.2 Haagerup's Equivalence Theorem

In a prior section, we saw that upto equivalence F_2 is the only Hadamard matrix of dimenion two. It turns out that this is also true for $n = 3, 5$.

Theorem 1.2.2 (Haagerup)**.** *For $n = 1, 2, 3, 5$, F_1, F_2, F_3, F_5 are, respectively, the only Hadamard matrices of that dimension upto equivalence.*

Proof. The cases $n = 1, 2$ are trivial. The case $n = 3$ is a valuable exercise. The case $n = 5$ is non-trivial, and the reader is referred to [2]. □

Exercise. Show that

$$\begin{pmatrix} 1 & a & a^4 & a^4 & a \\ a & 1 & a & a^4 & a^4 \\ a^4 & a & 1 & a & a^4 \\ a^4 & a^4 & a & 1 & a \\ a & a^4 & a^4 & a & 1 \end{pmatrix}$$

where $a = e^{2\pi i/5}$ is Hadamard and is equivalent to F_5.

1.2.3 A One Parameter Family

Upto this point, we have seen the classification of the Hadamard matrices of dimension 1, 2, 3, and 5. As it turns out, Hadamard matrices of dimenion 4 is one of the last dimenions for which the complete characterization of Hadamard matrices is known. The space of Hadamard matrices of dimenion 4 consists of an affine, one parameter family passing through F_4.

Theorem 1.2.3. *Every Hadamard matrix of dimenion* 4 *is of the form*

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

for some $z = e^{2\pi it}$ *for* $t \in [0, 2\pi)$.

The proof of the above theorem requires the following lemma.

Lemma 1.2.4. *If* $a, b, c, d \in \mathbb{C}$ *with* $|a| = |b| = |c| = |d| = 1$ *and* $a + b + c + d = 0$, *then* $a = -b$, $a = -c$, *or* $a = -d$.

Proof. Assume the hypotheses for the given lemmata. Then, the conclusion will follow if we can show that

$$(a+b)(a+c)(a+d) = 0.$$

Expanding the LHS of the above equation, we have the following equivalences:

$$\begin{aligned} 0 &= a^3 + a^2(b+c+d) + a(bc+bd+cd) + bcd \\ &= abcd\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d}\right) \quad \text{(Justify this step.)} \\ &= abcd(\overline{a+b+c+d}). \end{aligned}$$

And, since $\overline{a+b+c+d} = 0$ (justify this), the result follows. □

We now sketch the proof of the above theorem leaving the details as an exercise.

Proof. Using the lemma, the Hadamard matrix can be put in the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & b & -b \\ 1 & c & d & e \\ 1 & f & g & h \end{pmatrix}.$$

Next, break into cases examining when c, d, or e is equal to -1. For each case, determine the value of the remaining variables by using the fact that distinct rows / columns are orthogonal. □

1.3 THEOREMS, CONJECTURES, AND PROPERTIES OF HADAMARD MATRICES

Definition. A matrix $A = (a_{ij})_{i,j} \in M_n(\mathbb{C})$ is said to be a **unit matrix** iff $|a_{i,j}| = 1$ for all $1 \leq i, j \leq n$.

Example 1.3.1. $\begin{pmatrix} \frac{1}{i} & e^{2\pi i/7} \\ & -1 \end{pmatrix}$ is a unit matrix.

1.3.1 Determinant of Hadamard Matrices

Hadamard matrices originates from Jacques Hadamard's study of unit matrices having maximal possible determinant. As it turns out Hadamard matrices of dimenion n have maximal possible determinant amongst all unit matrices of dimenion n.

It can be shown that the maximum determinant of a unit $n \times n$ matrix is given by $|\det(A)| = n^{n/2}$. Intuitively, the reason is that A represents a paralleloid in n-dimenional space, and $\det(A)$ is a measure of the hypervolume of this paralleloid. The hypervolume is maximized when the vectors (i.e. rows / columns) are perpindicular to each other, i.e., mutually orthogonal, and in such case the hypervolume is simply the product of the lengths of each vector (verify this in the 2 and 3 dimenional case). Since the length of each vector is $\sqrt{n}$ (verify this), it follows that the product of n vectors is $n^{n/2}$, as desired. For a formal proof of this result involving Gram-Schmidt see [1].

Next, we show that Hadamard matrices obtain this maximal value.

Theorem 1.3.1. *Let $H \in M_n(\mathbb{C})$ be a Hadamard matrix. Then, $|\det(H)| = n^{n/2}$.*

Proof. Using elementary algebra, it can be shown that $\det(H) = \det(H^t) = \det(\overline{H}^t) = \det(H^*)$. Earlier, we showed that for Hadamard matrices that $H \cdot H^* = nI$. This implies that $|\det(H)\det(H^*)| = \det(nI)$, which is equivalent to $\det(H)^2 = n^n$, and hence $\det(H) = n^{n/2}$, as desired. □

Combining these two observations, we have the following theorem of Hadamard.

Theorem 1.3.2. *$H \in M_n(\mathbb{C})$ with unimodular entries is a Hadamard matrix if and only if $|\det(H)| = n^{n/2}$.*

1.3.2 On the Existence of Real Hadamard Matrices

As we showed in section one, there exist complex Hadamard matrices $H \in M_n(\mathbb{C})$ for all $n > 0$. The question remaion do their exist real Hadamard matrices $H \in M_n(\mathbb{R})$ for all $n > 0$? The answer to this question is unknown; however, the conjecture is that

Conjecture 1.3.3. *There exist $H \in M_n(\mathbb{R})$ Hadamard if and only if $n = 1, 2$ or $n \equiv 0 \pmod 4$.*

Remark. The conditions are necessary. Observe that real Hadamard matrices exist of dimenion 1 and 2. Let $H = (a_{ij}) \in M_n(\mathbb{R})$ be a Hadamard matrix with $n > 2$. WLOG, suppose that the Hadamard matrix is in normal form. There must be an equal number of 1's and -1's showing up in rows 2 through n of the Hadamard matrix in order for the first row to be orthogonal to the other rows. This shows that $2 \mid n$. Let $k \in \mathbb{N}$ be such that $n = 2k$, then there are k 1's in the second row. Through rearrangement, we may suppose that $a_{2,j} = 1$ for $1 \leq j \leq k$ and that $a_{2,j} = -1$ for $k + 1 \leq j \leq n$. Convince yourself that the inner product between the second and third rows of H is 0 if and only if $\sum_{l=0}^{k} a_{3,l} = 0 = \sum_{l=0}^{k} a_{3,l+k}$. This implies that there must be an even number of 1's and -1's on the first k positions of the third row, and hence that $2 \mid k$. Thus, in particular, $4 \mid n$.

A lot of research has been done on this conjecture, as this conjecture has remained unsolved for over 100 years. Presently, the smallest order for which it is unknown whether a real Hadamard matrix exists is $4 \cdot 167 = 668$.

1.3.3 On the Non-Existence of Circulant Hadamard Matrices

Another famous conjecture concerning Hadamard matrices is that

Conjecture 1.3.4. *There is no real circulant Hadamard matrix for $n \neq 1, 4$.*

Remark. For $n = 1$, (1) is such a matrix. For $n = 4$,

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

is such an example.

Various research has shown this conjecture for special cases, though a complete proof or counterexample remains as of the present unknown.

CHAPTER 2

ADVANCED CONSTRUCTIONS OF HADAMARD MATRICES

In the previous chapter, we saw one example of a family of Hadamard matrices, Fourier matrices, and several methods for constructing Hadamard matrices from a given Hadamard matrix. In this chapter, we present another method for deriving Hadamard matrices from known Hadamard matrices and introduce two important classes of Hadamard matrices.

2.1 CIRCULANT HADAMARD MATRICES

In the previous chapter, we discussed the conjectured non-existence of circulant, real Hadamard matrices for almost every dimension. Under certain assumptions, there exist infinitely many complex Hadamard circulant matrices. This section, though not necessary for the remainder of the paper, contains the elegant result of Munemasa and Watatani. This section requires a familiarity with quadratic residues for which the reader is referred to the Appendix.

In the proof of the following lemma, we use several results of quadratic residues. In particular, that $\left(\frac{k}{p}\right) = \left(\frac{k^{-1}}{p}\right)$, that the Legendre symbol is multiplicative, and that there is an equal number of quadratic residues and non-residues between 1 and $p-1$.

Lemma 2.1.1. *Let $1 \leq s \leq p-1$ be a fixed integer and p a prime, then*

$$\sum_{k=1}^{s-1} \left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) + \sum_{k=s+1}^{p-1} \left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) = -1.$$

Proof. Combining results from the appendix, we have that for $k \neq 0$ that

$$\left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) = \left(\frac{k^{-1}}{p}\right)\left(\frac{k-s}{p}\right) = \left(\frac{1-k^{-1}s}{p}\right).$$

Next, we observe that

$$A := \{1 - k^{-1}s \,|\, 1 \leq k \neq s \leq p-1\} = \{2, \ldots, p-1\} =: B.$$

This is clear since $1 - k^{-1}s$ maps $\mathbb{F}_p^*$ onto $\{0, 2, \ldots, p-1\}$ and maps s to 0. This implies that

$$\sum_{k=1}^{s-1} \left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) + \sum_{k=s+1}^{p-1} \left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) = \sum_{a\in A} \left(\frac{a}{p}\right) = \sum_{b\in B} \left(\frac{b}{p}\right) = -\left(\frac{1}{p}\right) + \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = -1.$$

□

The results of the following exercises will be used in the proof of the following theorem.

Exercise. Let $1 \leq s \leq p-1$ be a fixed integer and p a prime, then

$$\sum_{k=1}^{s-1} \left(\frac{k}{p}\right) + \sum_{k=s+1}^{p-1} \left(\frac{k}{p}\right) = -\left(\frac{s}{p}\right).$$

Exercise. Let $1 \leq s \leq p-1$ be a fixed integer and p a prime, then

$$\sum_{k=1}^{s-1} \left(\frac{k-s}{p}\right) + \sum_{k=s+1}^{p-1} \left(\frac{k-s}{p}\right) = \left(\frac{s}{p}\right).$$

Theorem 2.1.2. *(Munemasa-Watatani) If p is a prime of the form $4k+3$, then there exists unimodular constants $a, b \in \mathbb{C}$ such that the following matrix C is Hadamard.*

$$C = \begin{pmatrix} c_0 & c_1 & \ldots & c_{p-1} \\ c_{p-1} & c_0 & \ldots & c_{p-2} \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & \ldots & c_0 \end{pmatrix}$$

$$\textit{where each } c_k = \begin{cases} 1, \textit{if } k = 0 \\ a, \textit{if } \left(\frac{k}{p}\right) = 1 \\ b, \textit{if } \left(\frac{k}{p}\right) = -1 \end{cases}$$

Remark. Observe that C is a circulant matrix of size p.

Proof. Observe that because C is circulant if the inner product of the initial row with any row below it is zero, then the inner product of any two distinct rows is also zero. Hence, it suffices to check that for fixed $1 \leq s \leq p-1$, that the inner product of the initial row with the s^{th} row, $\sum_{k=0}^{p-1} c_k\overline{c_{k-s}}$, is identically zero.

A useful result that will aid us in this computation is that for $1 \leq k \leq p-1$ that $c_k = \alpha\left(\frac{k}{p}\right) + \beta$ where $\alpha = (a-b)/2$ and $\beta = (a+b)/2$.

We have the following

$$\begin{aligned}
\sum_{k=0}^{p-1} c_k\overline{c_{k-s}} &= c_0\overline{c_{-s}} + \sum_{k=1}^{s-1} c_k\overline{c_{k-s}} + c_s\overline{c_0} + \sum_{k=s+1}^{p-1} c_k\overline{c_{k-s}} \\
&= \left(\overline{\alpha}\left(\frac{-s}{p}\right) + \overline{\beta}\right) + \sum_{k=1}^{s-1}\left(\alpha\left(\frac{k}{p}\right) + \beta\right)\left(\overline{\alpha}\left(\frac{k-s}{p}\right) + \overline{\beta}\right) \\
&+ \left(\alpha\left(\frac{s}{p}\right) + \beta\right) + \sum_{k=s+1}^{p-1}\left(\alpha\left(\frac{k}{p}\right) + \beta\right)\left(\overline{\alpha}\left(\frac{k-s}{p}\right) + \overline{\beta}\right) \\
&= -\overline{\alpha}\left(\frac{s}{p}\right) + \overline{\beta} + \alpha\overline{\alpha}\sum_{k=1}^{s-1}\left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) + \alpha\overline{\beta}\sum_{k=1}^{s-1}\left(\frac{k}{p}\right) + \overline{\alpha}\beta\sum_{k=1}^{s-1}\left(\frac{k-s}{p}\right) + \beta\overline{\beta}(s-1) \\
&+ \alpha\left(\frac{s}{p}\right) + \beta + \alpha\overline{\alpha}\sum_{k=s+1}^{p-1}\left(\frac{k}{p}\right)\left(\frac{k-s}{p}\right) + \alpha\overline{\beta}\sum_{k=s+1}^{p-1}\left(\frac{k}{p}\right) + \overline{\alpha}\beta\sum_{k=s+1}^{p-1}\left(\frac{k-s}{p}\right) + \beta\overline{\beta}(p-s-1)
\end{aligned}$$

Observe that the above expression simplifies to:

$$\begin{aligned}
&\left(\alpha - \overline{\alpha}\right)\left(\frac{s}{p}\right) + \beta + \overline{\beta} + \alpha\overline{\alpha} - \alpha\overline{\beta}\left(\frac{s}{p}\right) + \overline{\alpha}\beta\left(\frac{s}{p}\right) + \beta\overline{\beta}(p-2) \\
=&\left(\alpha - \overline{\alpha} - \alpha\overline{\beta} + \overline{\alpha}\beta\right)\left(\frac{s}{p}\right) + \beta + \overline{\beta} + \alpha\overline{\alpha} + \beta\overline{\beta}(p-2)
\end{aligned}$$

At this point our goal is to find α and β such that simultaneously $\alpha - \overline{\alpha} - \alpha\overline{\beta} + \overline{\alpha}\beta = 0$ and $\beta + \overline{\beta} + \alpha\overline{\alpha} + \beta\overline{\beta}(p-2) = 0$.

Substituting in for α and β in terms of a and b, the first equation is equivalent to

$$0 = a^2b - ab^2 - b + a - a^2 + b^2 = (a-b)(a-1)(b-1)$$

and the second equation is equivalent to

$$0 = 2a^2b + 2ab^2 + 2b + 2a + 2ab(p-1) + a^2(p-3) + b^2(p-3).$$

Putting $a = 1$, the second equation reduces to

$$b^2 + 2\frac{p+1}{p-1}b + 1 = 0.$$

Let $p = 4m - 1$, then it follows that $b = \frac{-2m \pm i\sqrt{1-4m}}{2m-1}$, and a quick check shows that b is unimodular, which completes the proof. □

It is also true that for all primes p of the form $4k+1$ greater than 13 that there exist a circulant Hadamard matrix of size p inequivalent to $\mathbb{F}_p$. The reader is referred to [3].

2.2 PETRESCU'S MATRIX

In this section, we present the important discovery of Petrescu.

Theorem 2.2.1. *(Petrescu) The matrix*

$$P_7 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \epsilon^1 & \epsilon^4 & \epsilon^5 & \epsilon^3 & \epsilon^3 & \epsilon^1 \\ 1 & \epsilon^4 & \epsilon^1 & \epsilon^3 & \epsilon^5 & \epsilon^3 & \epsilon^1 \\ 1 & \epsilon^5 & \epsilon^3 & \epsilon^1 & \epsilon^4 & \epsilon^1 & \epsilon^3 \\ 1 & \epsilon^3 & \epsilon^5 & \epsilon^4 & \epsilon^1 & \epsilon^1 & \epsilon^3 \\ 1 & \epsilon^3 & \epsilon^3 & \epsilon^1 & \epsilon^1 & \epsilon^4 & \epsilon^5 \\ 1 & \epsilon^1 & \epsilon^1 & \epsilon^3 & \epsilon^3 & \epsilon^5 & \epsilon^4 \end{pmatrix}$$

is Hadamard where $\epsilon = e^{2\pi i/6}$.

Petrescu's result is extremely important in the theory of Hadamard matrices for several reasons.

First, Petrescu's matrix can be extended to a one dimensional affine family of Hadamard matrices given by

$$P_7(a) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathbf{a} & \mathbf{a} & \epsilon^5 & \epsilon^3 & \epsilon^3 & \epsilon^1 \\ 1 & \mathbf{a} & \mathbf{a} & \epsilon^3 & \epsilon^5 & \epsilon^3 & \epsilon^1 \\ 1 & \epsilon^5 & \epsilon^3 & \mathbf{a} & \mathbf{a} & \epsilon^1 & \epsilon^3 \\ 1 & \epsilon^3 & \epsilon^5 & \mathbf{a} & \mathbf{a} & \epsilon^1 & \epsilon^3 \\ 1 & \epsilon^3 & \epsilon^3 & \epsilon^1 & \epsilon^1 & \epsilon^4 & \epsilon^5 \\ 1 & \epsilon^1 & \epsilon^1 & \epsilon^3 & \epsilon^3 & \epsilon^5 & \epsilon^4 \end{pmatrix}$$

where $a = e^{2\pi it/6}$ for $0 \leq t < 2\pi$.

Second, Petrescu's method of finding this matrix involved using computers to minimize a set of equations governing a six dimensional Hadamard matrix. This method has since been implemented by various other researchers to find new examples of Hadamard matrices

and forms the backbone of our particular research.

Third, Petrescu's research has been generalized to yield infinite parametric families for dimensions $p = 13$, 19, and 31. See [5] for more information.

Finally, Petrescu's example is important because it is a non-trivial example of an important family of Hadamard matrices known as Butson type Hadamard matrix, which we discuss next.

2.3 BUTSON TYPE HADAMARD MATRICES

In this section, we make fundamental use of results established in the Appendix on cyclotomic polynomials.

Definition. Let $n, k \in \mathbb{Z}_+$. Then, $\mathrm{BH}(n, k)$ is defined to be the set of all Hadamard matrices of dimension n with all entries a k-th root of unity, i.e., if $H \in \mathrm{BH}(n, k)$, then $H = (a_{i,j})$ where $0 \leq i, j \leq n-1$ and $a_{i,j}^k = 1$ for all i, j; in such instances, H is said to be a **Butson type** Hadamard matrix.

Observation. $F_n \in \mathrm{BH}(n, n)$ and that $P_7 \in \mathrm{BH}(7, 6)$.

Remark. Butson type Hadamard matrices are fundamental in the study of Hadamard matrices essentially because finding Hadamard matrices with arbitrary unimodular entries can be incredibly difficult. Because a Butson type Hadamard matrix has further restrictions upon its entries, it is easier to find new examples of Hadamard matrices by searching for Butson type Hadamard matrices.

2.3.1 Non-Existence Results

We now return to our study of $\mathrm{BH}(n, k)$. A question that we want to answer is: when is $\mathrm{BH}(n, k) \neq \varnothing$? As we have seen, $\mathrm{BH}(n, n)$ and $\mathrm{BH}(7, 6)$ are both nonempty. In the following, we present several fundamental results giving conditions on when $\mathrm{BH}(n, k)$ is empty.

Exercise. Show that if n is odd, then $\mathrm{BH}(n,2) = \varnothing$.

Remark. If the Hadamard conjecture is true, then the even stronger statement $\mathrm{BH}(n,2) = \varnothing$ for all $0 < n \notin 4\mathbb{Z}$.

Theorem 2.3.1. *Let p, q be distinct primes and $0 < l, m \in \mathbb{Z}$, then $BH(p^l, q^m) = \varnothing$.*

Proof. Suppose, by contradiction, that there exists $H = (a_{i,j}) \in \mathrm{BH}(p^l, q^m)$, then we may assume that H is dephased. Put $\epsilon = e^{2\pi i/q^m}$, then there exists $k_1, \ldots, k_{p^l-1}$ such that $(a_{1,j}) = \epsilon^{k_j}$ for $1 \leq j \leq p^l - 1$. It follows that $1 + \epsilon^{k_1} + \cdots + \epsilon^{k_{p^l-1}} = 0$. Put $g(x) = 1 + x^{k_1} + \cdots + x^{k_{p^l-1}}$. Since $g(\epsilon) = 0$, it follows that $\Phi_{q^m}(x) \mid g(x)$, and hence that $g(x) = \Phi_{q^m}(x) \cdot \alpha(x)$. Evaluating at $x = 1$ yields $p^l = q \cdot \alpha(1)$, which implies that $q \mid p^l$, a contradiction. □

Exercise. Show that $\Phi_6(x) = x^2 - x + 1$. Conclude that if $\epsilon = e^{2\pi i/6}$, then $\epsilon + \bar{\epsilon} = 1$.

Next, we focus on a non-existence result of Winston.

Theorem 2.3.2. *(Winston) Let p be a prime of the form $6k + 5$, then $BH(p, 6) = \varnothing$.*

Proof. Assume there exists $H = (a_{i,j}) \in \mathrm{BH}(p, 6)$. Since $a_{i,j} \in \{1, \epsilon, \epsilon^2, \epsilon^3, \epsilon^4, \epsilon^5\}$, it follows that $\det(H) \in \mathbb{Z}[e] = \{a + b\epsilon \mid a, b \in \mathbb{Z}\}$ (verify this). Hence, $\det(H) = x + \epsilon y$ for some $x, y \in \mathbb{Z}$, which implies by Hadamard's theorem that $|\det H| = |x + \epsilon y| = p^{p/2}$, and hence $|x + \epsilon y|^2 = (x + \epsilon y)(x + \bar{\epsilon} y) = x^2 + xy + y^2 = p^p$. Multiplying both sides by four and making smart rearrangements, we obtain that $(2x + y)^2 + 3y^2 = 4p^p$. This implies that there exists $A, B \in \mathbb{Z}$ such that $A^2 + 3B^2 = 4p^p$, and consequently that $A^2 \equiv p \pmod 3$ (verify this). This implies that $\left(\frac{p}{3}\right) = 1$. But, observe that $\left(\frac{p}{3}\right) = \left(\frac{6k+5}{3}\right) = \left(\frac{2}{3}\right) = -1$, which is a contradiction. □

For various generalizations of Winston's theorem, see [7].

2.4 SYLVESTER'S CONSTRUCTION

We conclude this chapter with a construction result of Sylvester.

Theorem 2.4.1. *Let $H \in \mathbb{M}_n(\mathbb{C})$ be a Hadamard matrix. Then, $H_{2n} := \begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ is also Hadamard.*

Proof. Exercise. □

Exercise. Prove that Hadamard's conjecture on the existence of real Hadamard matrices is true for matrices of dimension 2^l for $0 \leq l \in \mathbb{Z}$.

CHAPTER 3

OUR RESEARCH

In the previous chapter, we were introduced to Butson type matrices and saw that Petrescu's matrix is part of an affine parametric family in $\mathrm{BH}(7,6)$. As it turns out for p prime, the Fourier matrix, F_p, is always isolated, i.e., F_p is not part of an affine parametric family of Hadamard matrices. Because families of Hadamard matrices are intrinsically interesting, useful for the classification of all Hadamard matrices of a particular dimension, and find uses in quantum information theory the quest for discovering families of Hadamard matrices is of great interest. Currently, for prime dimensions, only Petrescu's matrices discovered for dimensions $7, 13, 19$, and 31 are known to be part of an infinite affine family of Hadamard matrices; for all other prime dimensions it is unknown whether there exists an infinite family of Hadamard matrices. Observe that of the above dimensions all are of the form $6k+1$. Currently, it is an open problem to determine whether there exist any Butson type Hadamard matrices of dimension 11 which are part of an infinite parametric family. Currently, all known Hadamard matrices of dimension 11 are isolated. To answer this question our group has been studying $\mathrm{BH}(11,\cdot)$ trying to find new examples of such matrices. Below we outline the methods that we have used to answer this question.

3.1 INITIAL OBSERVATIONS

Observation. From the previous chapter, we know that the following sets are empty: $\mathrm{BH}(11,k)$ for $2 \leq k \leq 9$. The reader should justify these assertions. It is unknown whether $\mathrm{BH}(11,10)$ or $\mathrm{BH}(11,12)$ are nonempty.

We seek to answer the question is $\mathrm{BH}(11,12) = \varnothing$?

Put $\epsilon = e^{2\pi i/12}$. Suppose that $H = (a_{i,j}) \in \mathrm{BH}(11,12)$ is in dephased form, then $a_{i,j} = \epsilon^{k_{i,j}}$ for some $0 \leq k_{i,j} \leq 11$.

First, observe that the inner product of any two rows can be expressed in the form

$1 + \epsilon^{k_1} + \cdots + \epsilon^{k_{10}}$ for some $0 \leq k_i \leq 11$. Put $p(x) = 1 + x^{k_1} + \cdots + x^{k_{10}}$. Then, $p(\epsilon) = 0$, which implies that $\Phi_{12}(x) \mid p(x)$. Since $\Phi_{12}(x) = x^4 - x^2 + 1$, we have that

$$p(x) = 1 + x^{k_1} + \cdots + x^{k_{10}} = (x^4 - x^2 + 1) \sum_{i=0}^{7} c_i x^i. \tag{3.1}$$

Remark. In equation (3.1), i ranges between 0 and 7 so that upon expansion with $x^4 - x^2 + 1$ the resulting polynomial has at most degree 11.

Expanding equation (3.1), we find that $p(x)$ is equal to

$$\begin{aligned} &c_7x^{11} + c_6x^{10} + (c_5 - c_7)x^9 + (c_4 - c_6)x^8 + (c_3 - c_5 + c_7)x^7 + (c_2 - c_4 + c_6)x^6 + (c_1 - c_3 + c_5)x^5 \\ &\quad + (c_0 - c_2 + c_4)x^4 + (-c_1 + c_3)x^3 + (-c_0 + c_2)x^2 + (c_1)x + c_0. \end{aligned} \tag{3.2}$$

At this point, we want to find the c_i's. By finding the c_i's we can reverse engineer the problem to find the corresponding k_i's, which is what we are really interested in.

Exercise. If $(c_7, \ldots, c_0) = (0, 0, 0, 1, 0, 5, 0, 5)$, find the corresponding k_i's.

For $p(x)$ to be a valid function in the context of our problem, it is necessary that each coefficient of $p(x)$ is nonnegative and that $p(1) = 11$.

Remark. Observe that $p(0)$ is *not* necessarily 1 since some of the k_i's may be zero!

We obtain the following necessary conditions on the c_i's.

1. $c_7 \geq 0$
2. $c_6 \geq 0$
3. $c_5 \geq c_7$
4. $c_4 \geq c_6$
5. $c_3 \geq c_5 - c_7$
6. $c_2 \geq c_4 - c_6$
7. $c_1 \geq c_3 - c_5$
8. $c_0 \geq c_2 - c_4$
9. $c_3 \geq c_1$
10. $c_2 \geq c_0$
11. $c_1 \geq 0$
12. $c_0 \geq 1$
13. $\sum_{i=0}^{7} c_i = 11$

It is simple matter to write a program that iterates through all possible tuples belonging to $(\mathbb{Z}_{12})^8$ and for each tuple checks whether the above conditions are satisfied. For each tuple of c_i's, we find the corresponding tuple of k_i's belonging to $(\mathbb{Z}_{12})^{10}$.

Put $K := \{\vec{k} = (k_1, \ldots, k_{10}) \mid 1 + \epsilon^{k_1} + \cdots + \epsilon^{k_{10}} = 0\}$. Brute force search reveals that there are 331 *distinct, ordered* vectors of K; however, the cardinality of K is $132,414,240$; this is the number of distinct permutations of the 331 ordered vectors.

If $\vec{k} = (1, \epsilon^{k_1}, \ldots, e^{k_{10}})$ and $\vec{l} = (1, \epsilon^{l_1}, \ldots, e^{l_{10}})$ are two distinct rows of a Hadamard matrix belonging to BH$(11, 12)$, then it is necessary that $1 + e^{k_1} + \cdots + e^{k_{10}} = 0 = 1 + \epsilon^{l_1} + \cdots + e^{l_{10}}$ and that $0 = 1 + \epsilon^{k_1 - l_1} + \cdots + e^{k_{10} - l_{10}}$.

That is if $\vec{k}, \vec{l}$ are two rows of a $(11, 12)$ Butson type Hadamard matrix, then it follows that $(k_1 - l_1, \ldots, k_{10} - l_{10}) \in K$. (Recall that the individual subtractions are done modulo 12 and that we are taking the smallest nonnegative integer as the result of this subtraction.

Going in the reverse direction, to find a $(11, 12)$ Butson type Hadamard matrix, we need a set of 10 vectors belonging to K such that the difference between any two them is back in K.

More formally, we have that

Proposition 3.1.1. *BH*$(11, 12) \neq \varnothing$ *if and only if there exists* $L \subset K \subset (\mathbb{Z}_{12})^{10}$ *such that*

1. $|L| = 11$,
2. $(0, \ldots, 0) \in L$, *and*
3. $\vec{x}, \vec{y} \in L$ *implies that* $\vec{x} - \vec{y} \in L$.

Proof. Exercise. □

We now present the following example to help illustrate the ideas mentioned above.

Example 3.1.1. We list the first five distinct, ordered vectors of K.
$(8, 6, 6, 6, 6, 4, 0, 0, 0, 0), (8, 7, 6, 6, 6, 4, 1, 0, 0, 0), (8, 7, 7, 6, 6, 4, 1, 1, 0, 0),$
$(8, 7, 7, 7, 6, 4, 1, 1, 1, 0), (8, 7, 7, 7, 7, 4, 1, 1, 1, 1) \in K$.

Three possible permutations of the first vector include:

$(8,6,6,6,6,4,0,0,0,0), (4,0,6,0,6,8,0,6,6,0), (0,0,0,0,4,6,6,6,6,8)$.

Now, we illustrate subtraction of two vectors:

$(8,7,7,7,6,4,1,1,1,0) - (4,0,6,0,6,8,0,6,6,0) = (4,7,11,7,0,8,1,7,7,0)$, which is not an element of K.

Exercise. Prove that L cannot be a subgroup of $(\mathbb{Z}_{12})^{10}$.

3.2 EQUIVALENT CHARACTERIZATIONS

We now re-characterize (3.1.1) in terms of a graph theory problem, but first we need to define a graph theoretic term.

Definition. If G is a graph, then a clique of G is a subgraph of G on in which every two vertices of the subgraph share an edge. Thus, a maximal clique of G is the clique(s) of G lying on the largest number of vertices.

Let G be the graph with vertices in bijective correspondence to the vectors of K. We define an edge between any two vertices of G if and only if the difference of the corresponding vectors is an element of K. Then, we have

Proposition 3.2.1. *$BH(11,12) \neq \varnothing$ if and only if G has a maximal clique on at least 10 vertices.*

Proof. Exercise. □

The restatement of proposition (3.1.1) in terms of proposition (3.2.1) is crucial because we are able to exploit the various results of both mathematical and computational graph theory in solving our problem. For instance, we have a straightforward algorithm to test for the existence of a matrix in $\mathrm{BH}(11,12)$; determine the connnectivity of the graph corresponding to K and then find a maximal clique, and more importantly, we can draw from literature a number of algorithms for finding the maximal clique of a graph.

Because we expect the ratio of the number of edges actually appearing in G to the total number of possible edges to be very low (experimental evidence suggests less than one percent), we have utilized the clique finding algorithm presented in [4] because it is designed to find the maximal clique of a massive, sparse graph very quickly.

The biggest challenge in developing a computational solution to this problem is in developing fast code. Because computing edges between nodes is inherently an $O(n^2)$ algorithm in the number of nodes, a naïve approach of visiting each vertex and then calculating its connection with all subsequent vertices is simply not a feasible solution. Because if we assume that a computer can check an average of 10^6 connections between nodes per second, then such a program would take on the order of 278 years! Thus, the most important and challenging part of this research has been in recognizing mathematical optimizations reducing computational costs and in creating optimal, high performance code. The following observation of Nicoară is fundamental.

Proposition 3.2.2. *Let H be a maximal clique of G, v a vertex of H, and S the set of vertices of G which correlate to a permutation of v in K. Then, each element of S is contained in a maximal clique.*

Proof. In the following, we let $'$ denote the bijection between G and K taking a vertex of G to the corresponding vector of K. Observe that $'' = id$.

Let H be a maximal clique. Then, $H' \in \mathrm{BH}(11, 12)$, and v' corresponds to some row of H'. Let $a \in S$, then there exists $\sigma \in S_{11}$ so that $\sigma(v') = a'$. It follows that $\sigma(H')$ (σ is applied to the columns of H') is Hadamard containing a'. Whence $\sigma(H')'$ is a clique of G containing a. □

From this statement, we immediately obtain the following important corollary.

Corollary 3.2.3. *Let K^* denote the set of all distinct, ordered vectors of K. If $BH(11, 12)$ is nonempty, then there exists a Hadamard matrix containing some element of K^*.*

Remark. Recall that $|K^*|= 331$.

This corollary allows us to significantly reduce the computational complexity of our problem. We do so via the following algorithm.

Algorithm 1 Search for matrix in BH$(11, 12)$

```
for k ∈ K* do
    Compute edges between k' and g ∈ G
    if k' and g share an edge then
        N ← g
    end if
    Compute all edges between elements of N
    Find MAX CLIQUE of {k'} ⋃ N
end for
```

In the above, when we are fixing each $k \in K$, we are in essence fixing k as the second row of the Hadamard matrix and searching whether there exists a Hadamard matrix containing this row. If not, then by the corollary, we know that there is no Hadamard matrix containing any permutation of row k.

In the next section, we give the results of the implementation of the above program.

3.3 RESULTS

Using our algorithm described above, we found that $BH(11, k) = \varnothing$ for $k = 10$ and $12 \leq k \leq 21$. This suggests the following conjecture.

Conjecture 3.3.1. *There exists $n \times n$ matrix M in $BH(11, k)$ if and only if $11 \mid k$, in which case M is equivalent to F_{11}.*

Furthermore, using our algorithm we found several examples of what we believe to be new Butson-type Hadamard matrices belonging to $BH(13, 6)$. Below we present each matrix in its dephased, log form.

Example 3.3.1.

$$M_1 = \begin{pmatrix} 5 & 5 & 4 & 4 & 4 & 4 & 2 & 2 & 2 & 1 & 1 & 1 \\ 5 & 5 & 1 & 2 & 2 & 2 & 4 & 4 & 4 & 1 & 1 & 4 \\ 1 & 1 & 2 & 4 & 4 & 1 & 4 & 2 & 2 & 5 & 5 & 4 \\ 1 & 1 & 4 & 2 & 2 & 4 & 1 & 4 & 4 & 5 & 5 & 2 \\ 1 & 4 & 4 & 5 & 1 & 2 & 2 & 5 & 1 & 4 & 2 & 4 \\ 2 & 4 & 1 & 4 & 1 & 5 & 1 & 2 & 4 & 2 & 4 & 5 \\ 2 & 4 & 2 & 1 & 5 & 4 & 4 & 1 & 5 & 4 & 1 & 2 \\ 2 & 4 & 5 & 2 & 4 & 1 & 5 & 4 & 1 & 2 & 4 & 1 \\ 4 & 1 & 4 & 1 & 5 & 2 & 2 & 1 & 5 & 2 & 4 & 4 \\ 4 & 2 & 1 & 1 & 4 & 5 & 1 & 4 & 2 & 4 & 2 & 5 \\ 4 & 2 & 2 & 5 & 1 & 4 & 4 & 5 & 1 & 1 & 4 & 2 \\ 4 & 2 & 5 & 4 & 2 & 1 & 5 & 1 & 4 & 4 & 2 & 1 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 5 & 5 & 5 & 3 & 3 & 3 & 3 & 2 & 2 & 1 & 0 & 0 \\ 1 & 1 & 3 & 1 & 3 & 4 & 5 & 1 & 3 & 5 & 3 & 5 \\ 3 & 0 & 1 & 3 & 1 & 5 & 3 & 0 & 4 & 1 & 4 & 3 \\ 1 & 3 & 4 & 5 & 1 & 1 & 3 & 4 & 4 & 1 & 2 & 5 \\ 3 & 5 & 3 & 5 & 5 & 3 & 0 & 2 & 0 & 1 & 2 & 3 \\ 5 & 3 & 1 & 1 & 4 & 1 & 5 & 4 & 2 & 1 & 4 & 3 \\ 5 & 3 & 1 & 5 & 1 & 3 & 1 & 2 & 4 & 4 & 4 & 1 \\ 2 & 0 & 4 & 4 & 2 & 1 & 0 & 4 & 2 & 4 & 5 & 2 \\ 4 & 0 & 2 & 2 & 4 & 1 & 2 & 4 & 5 & 4 & 2 & 0 \\ 0 & 3 & 5 & 3 & 3 & 5 & 1 & 0 & 0 & 3 & 2 & 3 \\ 2 & 2 & 0 & 2 & 0 & 3 & 4 & 3 & 0 & 4 & 0 & 4 \\ 3 & 3 & 3 & 0 & 5 & 5 & 3 & 0 & 2 & 3 & 0 & 1 \end{pmatrix}$$

$$M_3 = \begin{pmatrix}
5 & 5 & 5 & 4 & 3 & 3 & 2 & 2 & 2 & 2 & 0 & 0 \\
2 & 4 & 2 & 0 & 1 & 4 & 1 & 2 & 4 & 4 & 0 & 4 \\
2 & 0 & 0 & 3 & 2 & 1 & 3 & 5 & 5 & 3 & 5 & 3 \\
2 & 1 & 4 & 1 & 4 & 4 & 5 & 3 & 1 & 1 & 5 & 3 \\
2 & 4 & 1 & 3 & 4 & 4 & 1 & 5 & 1 & 5 & 3 & 1 \\
0 & 4 & 2 & 3 & 5 & 0 & 4 & 2 & 0 & 2 & 2 & 4 \\
5 & 2 & 2 & 3 & 2 & 0 & 5 & 3 & 3 & 5 & 5 & 1 \\
4 & 4 & 0 & 0 & 1 & 2 & 4 & 4 & 2 & 0 & 2 & 3 \\
0 & 2 & 4 & 0 & 3 & 0 & 2 & 0 & 2 & 4 & 3 & 4 \\
4 & 0 & 4 & 2 & 5 & 2 & 0 & 1 & 4 & 4 & 2 & 2 \\
4 & 2 & 2 & 0 & 5 & 2 & 2 & 4 & 5 & 2 & 4 & 0 \\
2 & 2 & 4 & 4 & 1 & 4 & 4 & 0 & 4 & 1 & 2 & 0
\end{pmatrix}$$

It can be calculated that the defect of M_1, M_2, M_3 are: -11, -10, and -9, respectively. Since the defect is an invariant on Hadamard matrices, this shows that M_1, M_2, M_3 are not equivalent as Hadamard matrices.

Future directions of investigation of $BH(11, k)$ could involve a search for a mathematical proof that $BH(11, 10)$ and $BH(11, 12)$ are empty using number theoretic ideas, perhaps similar to those of Winston. Following such a discovery one could attempt to extend this proof for additional values of k.

REFERENCES

[1] T. Draghici, n.d. *Hadamard's Maximum Determinant Problem.* http://faculty.fiu.edu/∼draghici/pastcourses/applinalg_su07/Hadam_handout.pdf Accessed 2016 April 18.

[2] U. Haagerup, *Orthogonal maximal abelian -subalgebras of the $n \times n$ matrices and cyclic n-roots*, Operator Algebras and Quantum Field Theory, MA International Press, (1996) 296322.

[3] P. H. Tiep, *A remark on a theorem of P. de la Harpe and V. E R. Jones*, Arch. Math, **67**, (1996) 367-378.

[4] B. Pattabiraman, M. A. Patwary, A H. Gebremedhin, W. Liao, A. Choudhary, *Fast Algorithms for the Maximum Clique Problem on Massive Sparse Graphs*, Optimization Methods and Software, **0** (2012), 114.

[5] F. Szöllősi, *Construction, classification, and parametrization of complex Hadamard matrices*, arXiv preprint arXiv:1110.5590. 2011 Oct 25.

[6] F. Szöllősi, *Exotic complex Hadamard matrices and their equivalence*, Cryptography and Communications, **2** (2010), 187-198.

[7] A. Winterhof, *On the non-existence of generalised Hadamard matrices*, J. Statist. Plann. Inference, **84** (2000), 337342.

APPENDIX

QUADRATIC RESIDUES

Definition. Let p be a prime and $a \in \mathbb{Z} \setminus \{0\}$. Then, we say that a is a **quadratic residue modulo p** if and only if $(a, p) = 1$ and there exists $x \in \mathbb{Z}$ such that $x^2 \equiv a \pmod{p}$, and we write

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue} \\ 0, & \text{if } a \equiv 0 \pmod{p} \\ -1, & \text{if } a \text{ is not a quadratic residue} \end{cases}$$

Remark. The symbol $\left(\frac{\cdot}{\cdot}\right)$ is known as the Legendre symbol.

It is possible to sufficently generalize the notion of quadratic residues to non-prime integers under certain conditions; however, for our purposes this will be unneeded.

Exercise. Find the quadratic residues of $\mathbb{Z}/7\mathbb{Z}$.

Exercise. Show that if $a, b, p \in \mathbb{Z}$ with p prime and $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Quadratic residues are an extremely important mathematical concept. We present some of the basic properties of quadratic residues and the Legendre symbol below.

Below we adopt the following notation: $\mathbb{F}_p^* := (\mathbb{Z}/p\mathbb{Z})^*$, i.e., $\mathbb{F}_p^*$ is the group of units of $\mathbb{Z}/p\mathbb{Z}$ for p prime.

Theorem 3.3.2. *If $p > 2$ is a prime, then exactly $\frac{p-1}{2}$ elements of F_p^* are quadratic residues.*

Proof. Observe that for $x, y \in \mathbb{F}_p^*$ that $x^2 = y^2 \Leftrightarrow (x-y)(x+y) = 0$, which happens if and only if $x = y$ or $x = -y = p - y$.

Observe that the quadratic residues of $\mathbb{F}_p^*$ are precisely the elements belonging to the set $\{1^2, 2^2, \ldots, (p-1)^2\}$. However, in this set, there are exactly $\frac{p-1}{2}$ distinct elements, since $i^2 = (p-i)^2$ for $1 \leq i \leq p-1$. □

Corollary 3.3.3. *For $p > 2$ prime, $\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$.*

Next, we show that the Legendre symbol defines a group morphism.

Proposition 3.3.4. *The map $f : \mathbb{F}_p^* \to \{-1, 1\} : k \mapsto \left(\frac{k}{p}\right)$ is a group homomorphism.*

Proof. It suffices to show that for $a, b \in \mathbb{F}_p^*$ that $f(ab) = f(a)f(b)$. Recall that $\mathbb{F}_p^*$ is cyclic. Let α be a generator of $\mathbb{F}_p^*$, i.e., $< \alpha >= \mathbb{F}_p^*$. Observe that for $0 \leq k \leq p-2$ that $\left(\frac{\alpha^k}{p}\right) = (-1)^k$. This is because it can be seen that k is even if and only if α^k is a quadratic residue. (Verify this!) Hence, we have that $a = \alpha^a$ and $b = \alpha^l$, then

$$f(ab) = f(\alpha^k \alpha^l) = f(\alpha^{k+l}) = (-1)^{k+l} = f(\alpha^k)f(\alpha^l) = f(a)f(b).$$

This proves the claim. □

Exercise. Show that for $k \in \mathbb{F}_p^*$ that $\left(\frac{k}{p}\right) = \left(\frac{k^{-1}}{p}\right)$.

Proposition 3.3.5. *Show that for $p > 2$ that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.*

Proof. Suppose that p is a prime such that $\left(\frac{-1}{p}\right) = 1$. Pick $1 \leq a \leq (p-1)/2$. Then, observe that $\left(\frac{p-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$. This shows that are an equal number of quadratic residues / non-residues in the interval $1 \leq a \leq (p-1)/2$ as there are within the interval $(p+1)/2 \leq a \leq p-1$, and thus that $\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) = 0$. Clearly, this is possible if and only if $2 \mid (p-1)/2$.

In the foward direction, show that $\left((p-1)/2\right)^2 = -1$. □

While there are many more wonderful properties and theorems regarding the Legendre symbol, the above facts are all that will be needed in this text.

CYCLOTOMIC POLYNOMIALS

Cyclotomic polynomials are special examples of minimal polynomials, and several of the properties that we prove for cyclotomic polynomials hold in a more general setting.

Observation. Let $\epsilon = e^{2\pi i/n}$ for some $0 < n \in \mathbb{Z}$. Then, by Fermat's Little Theorem, ϵ is a root of the polynomial $x^n - 1$.

Exercise. Show that for $\epsilon = e^{2\pi i/n}$ that $\epsilon^{n-1} + \epsilon^{n-2} + \cdots + \epsilon + 1 = 0$ provided that $n > 1$.

We now show how to construct the n^{th} cyclotomic polynomial. In the following, we assume without stating, that $\epsilon = e^{2\pi i/n}$ for some $0 < n \in \mathbb{Z}$. Further, we write $f \in \mathbb{Z}[x]$ to signify that f is a polynomial having all of its coefficients in $\mathbb{Z}$.

As observed above, ϵ is a root of a monic polynomial, that is a polynomial having leading coefficient equal to one. Let S be the set of all nonzero, monic polynomials having coefficients in $\mathbb{Z}$ having ϵ as a root. Clearly, this set is non-empty. Choose a polynomial in S having minimal degree, such a polynomial must exist by the Well-Ordering theorem.

Exercise. Show that if $f(x)$ and $g(x)$ are two polynomials in S of minimal degree, then $f(x) = g(x)$. Thus, it makes sense to speak of **the** polynomial of S of minimal degree.

Hint. Consider $(f - g)(x)$.

Definition. For $0 < n \in \mathbb{Z}$, the n^{th} cyclotomic polynomial is the unique monic polynomial of minimal degree taking ϵ as a root and having all coefficients in $\mathbb{Z}$. This polynomial is denoted as $\Phi_n(x)$.

In the following, we state two fundamental properties of $\Phi_n(x)$ that will be used extensively in following sections.

Proposition 3.3.6. *Show that $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$, i.e. if $f(x) \mid \Phi_n(x)$ for some $f(x) \in \mathbb{Z}[x]$, then either $f(x) \equiv 1$ or $f(x) = \Phi_n(x)$.*

Hint. Recall that $\mathbb{Z}$ is an integral domain.

Corollary 3.3.7. *$\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. Exercise. □

Proposition 3.3.8. *Show that if ϵ is a root of $f(x)$, then $\Phi_n(x) \mid f(x)$.*

Hint. Recall that $\mathbb{Z}[x]$ is a Euclidean domain.

The following result due to Euler gives explicitly $\Phi_p(x)$ for p prime.

Theorem 3.3.9. $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$.

Proof. Let p be a prime, and put $\epsilon = e^{2\pi i/p}$. As we observed above, $\sum_{i=0}^{p-1} \epsilon^i = 0$, and hence it follows that $\Phi_p(x) \mid \sum_{i=0}^{p-1} x^i$. Next, observe that for all $a \in \mathbb{F}_p^*$ we have that $a^{p-1} + \cdots + a + 1 = 0$, which implies that $\Phi_p(a) = 0$ (Verify this!). Since every element of F_p^* is a root of both $\Phi_p(x)$ and $x^{p-1} + \cdots + x + 1$, if follows that $\deg(\Phi_p(x)) = p - 1$ and by unique factorization that $\Phi_p(x) = x^{p-1} + \cdots + x + 1$. □

While the above theorem gives us a nice explicit value for $\Phi_p(x)$, it turns out that it is not nearly as simple to determine the $\Phi_n(x)$ for an arbitrary positive integer. Thus, we state the following result of Gauss, without proof, which can be used to evaluate $\Phi_n(x)$ for $0 < n \in \mathbb{Z}$.

Theorem 3.3.10. *For $0 < n \in \mathbb{Z}$, we have that*

$$x^n - 1 = \prod_{\substack{d \mid n \\ 1 \leq d \leq n}} \Phi_d(x)$$

and $\deg(\Phi_n(x)) = \phi(n)$.

Exercise. Show that for p prime and $0 < k \in \mathbb{Z}$ that $\Phi_{p^k} = \Phi_p(x^{p^{k-1}}) = \sum_{i=0}^{p-1} (x)^{ip^{k-1}}$.

Exercise. Show that for $p > 3$ prime that $\Phi_{2p} = \sum_{i=0}^{p-1} (-x)^i$.

Exercise. Show that $\Phi_{12}(x) = x^4 - x^2 + 1$.