8-2017

Classification Results of Hadamard Matrices

Gregory Allen Schmidt
University of Tennessee, Knoxville, gschmid1@vols.utk.edu

To the Graduate Council:

I am submitting herewith a thesis written by Gregory Allen Schmidt entitled "Classification Results of Hadamard Matrices." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Mathematics.

Remus Nicoara, Major Professor

We have read this thesis and recommend its acceptance:

Jerzy Dydak, Morwen Thistlethwaite

Accepted for the Council:
Dixie L. Thompson

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Classification Results of Hadamard Matrices

A Thesis Presented for the

Master of Science

Degree

The University of Tennessee, Knoxville

Gregory Allen Schmidt

August 2017

I dedicate this work to my loving wife, Daniela, and my adorable children, Jacob and Isabella. Their love and support has been a blessing to me.

Acknowledgements

I would like to thank Dr. Remus Nicoara for all of his help throught the course of my studies at the University of Tennessee, Knoxville. Without his guidance, this paper would not have been possible.

Abstract

In 1893 Hadamard proved that for any $n \times n$ matrix A over the complex numbers, with all of its entries of absolute value less than or equal to 1, it necessarily follows that

$$|det(A)| \leq n^{n/2}[\text{n raised to the power n divided by two}],$$

with equality if and only if the rows of A are mutually orthogonal and the absolute value of each entry is equal to 1 (See [2], [3]). Such matrices are now appropriately identified as Hadamard matrices, which provides an active area of research in both theoretical and applied fields of the sciences. In pure mathematics, Hadamard matrices are of interest due to their intrisic beauty as well as their applications to areas such as combinatorics, information theory, optics, operator algebras and quantum mechanics.

In this text we will introduce some fundamental properties of Hadamard matrices as well as provide a proofs of some classification results for real Hadamard matrices.

Table of Contents

Chapter 1

Introduction

Hadamard matrices form an important class of matrices, with applications ranging from binary codes and information theory, to operator algebras and quantum mechanics. This class of matrices has the orthogonal property and was introduced by Slyvester in 1867. In 1893 Hadamard determined that such matrices $H \in M_n(\mathbb{R})$ maximize $|det(H)|$ for $H = (h_{k,l})$, with $|h < k, l| \leq 1$ for all $1 \leq k, l \leq n$. In this case $|det(H)| = n^{n/2}$ (see [3]). There is an intuitive geometric reason, which explains why this is true. The volume of an n-dimensional paralleloid of sides less than or equal to $\sqrt{n}$ is maximum if it is a box, i.e. the vectors that determine its sides are orthogonal, which is to say that the $n \times n$ matrix formed from the n vectors that determine the sides of the paralleloid is an orthogonal matrix.

1.1 Definition and Examples of Hadamard Matrices

Definition: Let $H \in M_{n\times n}(\mathbb{C})$. H is said to be a Hadamard matrix of order n if:

1. Each entry $h_{k,l}$ of H is of norm 1, i.e. $|h_{k,l}| = 1$ for $1 \leq k, l \leq n$, and
2. H has mutually orthogonal rows.

From the above definition, we can easily produce several examples of Hadamard matrices.

Example 1.1.4 Let $n \geq 1$, and put $\epsilon = e^{\frac{2\pi i}{n}}$. Then,

$$F_n = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \epsilon & \epsilon^2 & \cdots & \epsilon^{n-1} \\ 1 & \epsilon^2 & (\epsilon^2)^2 & \cdots & (\epsilon^2)^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \epsilon^{n-1} & (\epsilon^{n-1})^2 & \cdots & (\epsilon^{n-1})^{n-1} \end{bmatrix} = (\epsilon^{kl}) \;\; 0 \leq k, l \leq n-1$$

is commonly known as the Fourier matrix of order n. Since each of the entries of F_n are roots of unity, it is clear that $|(\epsilon^{kl})| = 1$ for all $0 \leq k, l \leq n-1$. Let $\mathbf{f}_k$ and $\mathbf{f}_l$ be any two rows of F_n. Then $\langle \mathbf{f}_k, \mathbf{f}_l \rangle = 1 + \epsilon^{k-l} + \cdots + \epsilon^{(n-1)(k-l)}$. If $k = l$ then $\langle \mathbf{f}_k, \mathbf{f}_l \rangle = n$. If $k \neq l$ then $e^{(k-l)}$ is an n^{th} root of unity and so $\langle \mathbf{f}_k, \mathbf{f}_l \rangle = 0$ as the sum of n n^{th} roots of unity is 0. Thus distinct rows of F_n are mutually orthogonal and so F_n is Hadamard. F_n is commonly known as the Fourier matrix of order n.

Thus for every $n \geq 1$ there exists at least one $n \times n$ complex Hadamard matrix, the Fourier matrix. However, real Hadamard matrices do not exist for all dimensions $n \geq 1$.

Theorem (Hadamard) Let $A = (a_{ij})$ be a real Hadamard matrix of order $n > 2$. Then n is divisible by 4.

Proof. Since any two distinct columns i, j of A are orthogonal, we have that

$$0 = \sum_{k=1}^{n} (a_{ij} a_{ik}) = \pm 1 \pm 1 \cdots \pm 1.$$

It thus follows that n must be even and any two distinct columns must also have identical entries in exactly $n/2$ rows. Next consider three distinct columns i, j, k of A. We thus have that

$$\sum_{l=1}^{n} (a_{ij} + a_{ik})(a_{ij} + a_{il}) = \sum_{l=1}^{n} (a_{ik}^2) + \sum_{l=1}^{n} (a_{ij} a_{il}) + \sum_{l=1}^{n} (a_{ik} a_{ij}) + \sum_{l=1}^{n} (a_{ik} a_{il}) = n + 0 + 0 + 0 = n.$$

When $a_{ij} = a_{ik} = a_{il}$ we have that $(a_{ij} + a_{ik})(a_{ij} + a_{il}) = 4$, with $(a_{ij} + a_{ik})(a_{ij} + a_{il}) = 0$ otherwise. Thus, $n = 4p$, where p is the number of rows such that $a_{ij} = a_{ik} = a_{il}$. In particular, we have that any 3 columns of A have the same entry in exactly $n/4$ rows. The result follows. □

The following is a famous conjecture that has remained unsolved for over 100 years:
Conjecture: (Hadamard). A real $n \times n$ Hadamard matrix exists for $n = 1, n = 2$, and for all $n \in \mathbb{N}$ such that $n \equiv 0 \mod 4$.

Example 1.1.2 Let $H_1 = [1]$, $H_2 = \begin{bmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{bmatrix}$, and $H_4 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix}$. It is easily verified that H_1, H_2, and H_4 are all real Hadamard matrices. In fact, for any Hadamard matrix H_n or order n, we can construct a Hadamard matrix of order $2n$ as follows:

$$H_{2n} = \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}.$$

We compute the product of H_{2n} with its conjugate transpose to verify that H_{2n} is in fact Hadamard.

$$\begin{aligned} H_{2n}H_{2n}^* &= \begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix} \begin{bmatrix} H_n^* & H_n^* \\ H_n^* & -H_n^* \end{bmatrix} \\ &= \begin{bmatrix} H_nH_n^* + H_nH_n^* & H_nH_n^* - H_nH_n^* \\ H_nH_n^* - H_nH_n^* & H_nH_n^* + H_nH_n^* \end{bmatrix} \\ &= \begin{bmatrix} 2nI_{2n} & 0 \\ 0 & 2nI_{2n} \end{bmatrix} \\ &= 2nI_n \end{aligned}$$

This shows that the rows of H_{2n} are mutually orthogonal. It is clear that every entry of H_{2n} is of modulus 1, and so it follows that H_{2n} is Hadamard. The method by which we constructed the previous matrices is known as the Sylvester construction, which produces Hadamard matrices of order 2^k for all $k \in \mathbb{N}$.

Definition 1.1.3 If M and N are matrices, then their *Kronecker Product* $M \otimes N$ is the matrix U, which is constructed by replacing each entry $M_{i,j}$ of M with $M_{i,j}N$.

Example 1.1.4 Let H_m and H_n be Hadamard matrices of order m and n, respectively.

Then the Kronecker product $H_m \otimes H_n$ is a Hadamard matrix of order mn. Notice that in example 1.1.2, the Hadamard matrix $H_{2n} = H_n \otimes H_n$. We now present a family of Hadamard matrices using the Paley construction 1 [10]. Paley's construction makes use of quadratic residues over a field $\mathbb{F}_p$ (p prime), which we introduce below.

Definition 1.1.5 An element $r \in \mathbb{F}_p$ is said to be a *quadratic residue* if $r = s^2$ has a solution in $\mathbb{F}_p$.

Example 1.1.6 When $p = 7$, we have that

$$0 \equiv 0^2 \mod 7, \quad 1 \equiv 1^2 \mod 7, \quad 2 \equiv 3^2 \mod 7, \quad 4 \equiv 2^2 \mod 7,$$

$$1 \equiv 6^2 \mod 7, \quad 2 \equiv 4^2 \mod 7, \quad 4 \equiv 5^2 \mod 7.$$

Thus, the only quadratic residues in $\mathbb{F}_7$ are $0, 1, 2$, and 4.

Lemma 1.1.7 If $q = p^r$, where p is an odd prime, then exactly half of the nonzero elements of $\mathbb{F}_q$ are quadratic residues. Moreover, -1 is a quadratic residue if and only if $q \equiv 1 \mod 4$.

Definition 1.1.8 Let p be prime. The *Legendre symbol* $\chi(x)$ is defined to be

$$\chi(x) = \begin{cases} 0, & \text{if } x \text{ is a multiple of p} \\ 1, & \text{if } x \text{ is a quadratic residue modulo p} \\ -1, & \text{if } x \text{ is not a quadratic residue modulo p} \end{cases}$$

Consider the $p \times p$ matrix Q with entries $q_{ij} = \chi(j - i)$, indexed starting at 0. For example, when $p = 5$. Since 1 and 4 are the only nonzero quadrati residues in $\mathbb{F}_5$, we obtain

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

which is known as a *Jacobsthal matrix*. We now introduce Paley's construction of Hadamard matrices.

Theorem 1.1.9 If $q \equiv 3 \mod 4$ and Q is a *Jacobsthal matrix* for $\mathbb{F}_q$, then

$$H = \begin{bmatrix} 1 & 1^n \\ (1^n)^T & Q - I \end{bmatrix},$$

is a Hadamard matrix of order $q + 1$.

Proof. See [1]. □

Definition 1.1.10 A complex $n \times n$ matrixM is said to be *dephased* when all of the entries in the first row and first column are equal to one. In the case that M is a real $n \times n$ matrix, M is said to be *normalized*.

Definition 1.1.11 The *core* of an $n \times n$ matrix is the lower right submatrix of size $n - 1$. We note that the matrix H in theorem 1.1.9 is a normalized Hadamard matrix with core $Q - I$. The following result is due to Williamson (See [10] [8]).

Theorem 1.1.12 Suppose there exists $n \times n$ matrices A, B, C and D satisfying the following properties:

1. A, B, C and D are symmetric matrices having entries ± 1;
2. A, B, C and D commute with each other;
3. $A^2 + B^2 + C^2 + D^2 = 4nI_n$.

Then there is a Hadamard matrix of order $4n$ given by

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

Definition 1.1.13 Matrices A, B, C and D satisfying conditions $(1) - (3)$ are referred to as *Williamson matrices*.

1.2 Properties of Hadamard Matrices

Theorem 1.2.1 (Hadamard, 1893) Let A be an $n \times n$ complex matrix with linearly independent columns $\mathbf{z}_1, \mathbf{z}_2, \cdots, \mathbf{z}_n$. Then

$$|det(A)|^2 = |det(A \cdot A^*)| \leq \prod_{k=1}^{n} \|\mathbf{z}_k\|^2,$$

with equality if and only if $A \cdot A^*$ is a diagonal matrix.

Proof. We begin by applying the Gram-Schmidt process to construct mutually orthogonal vectors $\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_n$ such that $\mathbf{y}_k = c_1\mathbf{z}_1 + c_2\mathbf{z}_2 + \cdots + \mathbf{z}_k$. Let

$$\mathbf{y}_k = \sum_{i=1}^{k-1} \alpha_{ki}\mathbf{y}_i, \quad \text{where} \quad \alpha_{ki} = \frac{\langle \bar{\mathbf{z}_k}, \mathbf{y}_i \rangle}{\langle \bar{\mathbf{y}}_i, \mathbf{y}_i \rangle}.$$

Since $\mathbf{z}_1, \mathbf{z}_2, \cdots, \mathbf{z}_k$ are all linearly independent, it follows that $\mathbf{y}_k \neq 0$ for all k and

$$\langle \bar{\mathbf{y}}_k, \mathbf{y}_i \rangle = \langle \bar{\mathbf{z}}_k, \mathbf{y}_i \rangle - \alpha_{k1}\langle \bar{\mathbf{y}}_1, \mathbf{y}_i \rangle - \cdots - \alpha_{ki}\langle \bar{\mathbf{y}}_i, \mathbf{y}_i \rangle = \langle \bar{\mathbf{z}}_k, \mathbf{y}_i \rangle - \alpha_{ki}\langle \bar{\mathbf{y}}_i, \mathbf{y}_i \rangle = 0.$$

Let $B = (\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_n)$. Since all of the $\mathbf{y}_k's$ are mutually orthogonal, it follows that $B \cdot B^* = D$, where $D = (d_{ij})$ is a diagonal matrix with $d_{ii} = \|\mathbf{y}_i\|^2$ for all $1 \leq i \leq n$. Let

$$T = \begin{bmatrix} 1 & \alpha_{12} & \cdots & \alpha_{1n} \\ 0 & 1 & \cdots & \alpha_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

and notice that $B = TA$. Thus, we have that

$$det(B) = det(TA) = det(T)det(A) = det(A).$$

It thus follows that$|det(B)|^2 = |det(A)|^2$. We also have that

$$|det(B)|^2 = det(B \cdot B^*)| = \prod_{k=1}^{n} \|\mathbf{y}_k\|^2$$

Recalling that $\mathbf{z}_k = \sum_{i=1}^{k-1} \alpha_{ki}\mathbf{y}_i$ and using the orthogonality of the $\mathbf{y}'_k s$ we obtain

$$\langle \bar{\mathbf{z}}_k, \mathbf{z}_k \rangle = \|\mathbf{z}_k\|^2 = \langle \bar{\mathbf{y}}_k, \mathbf{y}_k \rangle + \sum_{i=1}^{k-1} |\alpha_{ki}|^2 \langle \bar{\mathbf{y}}_i, \rangle \mathbf{y}_i = \|\mathbf{y}_k\|^2 + \sum_{i-1}^{k-1} |\alpha_{ki}|^2 \|\mathbf{y}_i\|^2.$$

We thus have that $\|\mathbf{y}_k\|^2 \leq \|\mathbf{z}_k\|^2$ for all k, with equality if and only if $\mathbf{y}_k = \mathbf{z}_k$. Therefore, it follows that

$$|det(A)|^2 = |det(B)|^2 = \prod_{k=1}^{n} \|\mathbf{y}_k\|^2 \leq \Pi_{k=1}^{n} \|\mathbf{z}_k\|^2,$$

with equality if and only if $\mathbf{y}_k = \mathbf{z}_k$ for all k i.e. if and only if $A \cdot A^*$ is a diagonal matrix. □

Corollary 1.2.2 Let $A = (z_{ij})$ be an $n \times n$ complex matrix with $|z_{ij}| \leq 1$. Then $|det(A)| \leq n^{n/2}$, with equality if and only if $|z_{ij}| = 1$ and $AA^* = nI$.

Proof. Let $\mathbf{z}_k$ denote the k^{th} of A. If the columns of A are not linearly independent, then $det(AA^*) = 0$ and the inequality holds. If the columns of A are linearly independent, then

$$\|\mathbf{z}_k\|^2 = |z_{1k}|^2 + \cdots + |z_{nk}|^2 \leq n$$

as $|z_{ik}| \leq 1$ for all $1 \leq i, k \leq n$. It follows that

$$|det(A)|^2 \leq \Pi_{k=1}^{n} \|\mathbf{z}_k\|^2 \leq n^n.$$

We thus have that

$$|det(A)| \leq n^{n/2},$$

with equality if and only if $|z_{ij}| = 1$ and $AA^* = nI$. □

Proposition 1.2.3 Let H be an $n \times n$ complex Hadamard matrix. Then $HH^* = nI$.

Proof. When $H \in M_n(\mathbb{C})$ is Hadamard, each of the rows of H are orthogonal vectors of norm $\sqrt{n}$. We can thus divide each entry of H by $\frac{1}{\sqrt{n}}$ to obtain an $n \times n$ matrix whose conjugate transpose is also its inverse, i.e. $H = \sqrt{n}H_n$, where $H_n H_n^* = I$. Thus

$$HH^* = (\sqrt{n}H_n)(\sqrt{n}H_n)^* = nH_nH_n^* = nI,$$

as was to be shown. □

Theorem 1.2.4 Let $A \in M_n(\mathbb{D})$, where $\bar{\mathbb{D}} = \{z : |z| \leq 1\}$. Then A has maximum determinant if and only if A is Hadamard.

Proof. Suppose $A \in M_n(\mathbb{C})$ has maximum determinant, i.e. $|det(A)| = n^{n/2}$. Then from corollary 1.2.2 each of the entries of A have modulus equal to 1 and $AA^* = nI$. Therefore, all rows of A are mutually orthogonal and it follows that A is Hadamard.

Now suppose that $A \in M_n(\mathbb{C})$ is Hadamard. Then each entry of A is of modulus 1 and each row of A has norm $\sqrt{n}$ Since every row of A is mutually orthogonal $AA^* = D_n$, where $D_n = (d_{ij})$ is a diagonal matrix. But every row of A has norm $\sqrt{n}$ and so $d_{ij} = n$ whenever $i = j$, i.e. $D_n = nI_n$. Hence it follows from theorem that $det(A) = n^{n/2}$, i.e. A has maximum determinant □

Proposition 1.2.5 If a matrix H' is formed by interchanging two rows or columns of the matrix H, then H' is Hadamard if and only if H is Hadamard.

Proposition 1.2.6 If $H \in M_n(\mathbb{C})$ is Hadamard, then H^* is Hadamard.

Proof. Since H is Hadamard, all of its entries are of absolute value 1. Thus, all of the entries of H^* are of absolute value 1 as well. Since $H \cdot H^* = nI$, we have that $\frac{1}{n}(H^* \cdot H^{**}) = I$, and from corollary 1.2. and theorem 1.2.4 it follows that H^* is Hadamard. □

Corollary 1.2.7 If H is Hadamard, then the columns of H are orthogonal.

Proof. The proof is straightforward. The fact that H is Hadamard, provides that H^* is also Hadamard. Thus, the rows of H^* are orthogonal, which are simply the conjugate of the columns of H. □

We have in general, that any permutation of rows or columns of a Hadamard matrix is still a Hadamard matrix. Furthermore, multiplication of any row or column of a Hadamard matrix by some $a \in \mathbb{C}$ with $|a| = 1$, produces another Hadamard matrix. This naturally leads us to define when two Hadamard matrices are equivalent.

Definition 1.2.8 Let H and K be Hadamard matrices. We say that H and K are equivalent if and only if there exist permutation matrices P_1 and P_2, and unitary diagonal matrices D_1 and D_2 such that $H = P_1 D_1 K D_2 P_2$. In this case, we write $H \sim K$.

Proposition 1.2.9 $\sim$ is an equivalence relation on $M_n(\mathbb{C})$.

Proof. We begin by noting that any $n \times n$ permutation matrix P is nonsingular with $P^{-1} = P^*$, which is also a permutation matrix. Furthermore, for any $n \times n$ matrix D, PD gives the rows of D interchanged according to the permutation vectors of P and DP gives the columns of D interchanged according to the permutation vectors of P. In the case that D is diagonal, there exists a permutation matrix P' such that $P'D = DP$. We proceed with our proof:

1. $H \sim H$ is clear.

2. Suppose $H \sim K$. We show that $K \sim H$. Let P_1, P_2 be permutation matrices and $D_1 D_2$ diagonal matrices such that $H = P_1 D_1 K D_2 P_2$. Then

$$\begin{aligned} K &= D_1^{-1} P_1^{-1} H P_2^{-1} D_2^{-1} \\ &= D_1^{-1} P_1^* H P_2^* D_2^{-1} \\ &= P' D_1^{-1} H D_2^{-1} P_2' \end{aligned}$$

Therefore, $K \sim H$.

3. If $H \sim K$ and $K \sim M$, then there exists permutation matrices P_1, P_2, P_3, P_4 and diagonal matrices D_1, D_2, D_3, D_4 such that $H = P_1 D_1 K D_2 P_2$ and $K = P_3 D_3 M D_4 P_4$. Thus

$$\begin{aligned} H &= P_1 D_1 P_3 D_3 M D_4 P_4 D_2 P_2 \\ &= P_1 P_3' D_1 D_3 M D_4 D_2 P_4' P_2, \end{aligned}$$

where P_3' and P_4' are permutation matrices such that $D_1P_3 = P_3'D_1$ and $P_4D_2 = D_2P_4'$. But the product of two permutation matrices is a permutation matrix as is the product of two diagonal matrices a diagonal matrix. Hence we have that $H \sim M$, and $\sim$ is a bona fide equivalence relation. $\square$

Note that any Hadamard matrix is equivalent to a normalized Hadamard matrix (See [9]). An area of current interest involves the determination of equivalence classes of Hadamard matrices and the intrinsic properties that these classes posses. One such example being *Haagerup's Invariant*, which is defined for a Hadamard matrix $H = (h_{i,j})$ as the set

$$\Lambda(H) = \{h_{i,j}h_{k,l}\overline{h}_{k,j}\overline{h}_{i,l} | 1 \leq i, j, k, l \leq n\}.$$

Lemma 1.2.10 If H and K are Hadamard matricies such that $H \sim K$, then $\Lambda(H) = \Lambda(K)$. See [7]).

Using Mathematica we computed $\Lambda(F_2) = \{\pm 1\}$, $\Lambda(F_2 \otimes F_2) = \{\pm 1\}$ and $F_4 = \{\pm 1, \pm i\}$. A priori to computing the Hageerup invariant for F_2 and $F_2 \otimes F_2$ we know due to difference in dimension that these two matrices cannot be equivalent, irrespective of the fact that $\Lambda(F_2) = \Lambda(F_2 \otimes F_2)$. However, $F_2 \otimes F_2$ and F_4 are of the same dimension but $\Lambda F_2 \otimes F_2 \neq \Lambda F_4$ demonstrates that these two matrices are not equivalent.

Theorem 1.2.11 (Haagerup). The only Hadamard matrices up to equivalence of order $1, 2, 3$, and 5 are F_1, F_2, F_3 and F_5, respectively. See [7] for proof. We provide as an example a Hadamard matrix of dimension 5, which is thus equivalent to F_5:

$$H = \begin{bmatrix} 1 & a & a^4 & a^4 & a \\ a & 1 & a & a^4 & a^4 \\ a^4 & a & 1 & a & a^4 \\ a^4 & a^4 & a & 1 & a \\ a & a^4 & a^4 & a & 1 \end{bmatrix}.$$

One of the few remaining classical results of Hadamard matrices is for Hadamard matrices of dimension 4. The space of Hadamard matrices of this dimension passes through F_4 and consist of an affine one parameter family. They are characterized by the following theorem.

Theorem 1.2.12 Every $4\times$ Hadamard matrix is of the form

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

for some $z = e^{2\pi it}$ with $t \in [0, 2\pi)$. To prove this theorem, we need the following lemma.

Lemma 1.2.13 If a, b, c and $d \in \mathbb{C}$ with $|a| = |b| = |c| = |d| = 1$ and $a+b+c+d = 0$, then $a = -b, a = -c$, or $a = -d$.

Proof. We note that $a = -b, a = -c$, or $a = -d$ is equivalent to $(a+b)(a+c)(a+d) = 0$. Thus, we aim to show that

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

We begin by expanding the LHS of our equation to obtain

$$\begin{aligned} a^3 + a^2(b+c+d) + a(bc+bd+cd) + bcd &= abcd(1/a + 1/b + 1/c + 1/d) \\ &= abcd((\overline{a+b+c+d}). \end{aligned}$$

The result follows as $(\overline{a+b+c+d}) = 0$. □

The proof of the theorem 1.2.12 follows from lemma 1.2.13 since we can put any Hadamard matrix in the form

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

Recall that distinct rows (columns) are orthogonal, and consider the cases when c, d or e are equal to -1. The orthogonality allows us in each case to determine the value of the remaining variables.

Chapter 2

Circulant Hadamard Matrices

2.1 Circulant Hadamard Matrices

In this chapter, we discuss an important class of Hadamard matrices, known as circulant Hadamard matrices.

Definition 2.1.1 A matrix $M \in M_n(\mathbb{C})$ is said to be *circulant* if $M_{i,j} = M_{i',j'}$ whenever $i - j \equiv i' - j' \mod n$. We could equivalently define the matrix M to be circulant if the ith row of M is the first row of M shifted right $i - 1$ positions. Thus, the matrix

$$A = \begin{bmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{bmatrix}$$

is circulant. Notice that for an $n \times n$ circulant matrix $A = (a_{i-j})$, with $\zeta = e^{2\pi i/n}$ a nth root of unity, we see that for $0 \leq j < n$ the column vector $[1, \zeta^j, \zeta^{2j}, \cdots, \zeta^{(n-1)j}]^T$ is an eigenvector of A with eigenvalue $a_0 + \zeta^j a_1 + \zeta^{2j} a_2 + \cdots + \zeta^{(n-1)j} a_{n-1}$. Thus we have that

$$\det(A) = \prod_{j=0}^{n-1} (a_0 + \zeta^j a_1 + \zeta^{2j} a_2 + \cdots + \zeta^{(n-1)j} a_{n-1}).$$

Example 2.1.2 The matrix $M = \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$ is both a circulant matrix and Hadamard.

The following is a foamous open problem in the theory of real Hadamad matrices.

Conjecture: There does not exist a real circulant Hadamard matrix for $n \neq 1, 4$. Richard Turyn (See [8] showed using modern algebraic number theory, that there is no circulant Hadamard matrix of order $8m$. He also eliminated for certain m, orders of the form $4(2m+1)$. We provide proof of the special case $n = 2^k$, which can also be found in Stanley's book. For the remainder of this section, we will assume that n is an integer that can be written as a power of 2. In this section, we will show that no circulant Hadamard matrix exist for such an n when $n > 4$.

Recall that $n = 2^k$ and write $\zeta = e^{2\pi i/2^k}$. Let $\mathbb{Q}(\zeta)$ denote the quotient field of $\mathbb{Z}[\zeta]$. Notice that in $\mathbb{Q}(\zeta)$, the polynomial $p_k(x) = x^{2^{k-1}} + 1$ is zero at ζ as $\zeta^{2k} - 1 = 0 \rightarrow (\zeta^{2k-1} + 1)(\zeta^{2k-1} - 1) = 0 \rightarrow \zeta^{2k-1} + 1 = 0$.

The proof of theorem 2.1.11 is due to Stanley (see [5]) and will make use of the fact that for any Hadamard matrix H, $\det(H) = \pm n^{n/2}$ and that any circulant matrix A has the property $\det(A) = \prod_{j=0}^{n-1}(a_0 + \zeta^j a_1 + \zeta^{2j} a_2, \cdots, \zeta^{(n-1)j} a_{n-1})$, which together give us that

$$\det(A) = \pm n^{n/2} = \pm (2^k)^{2^{k-1}}. \qquad (1)$$

i.e. there is such a factorization of $(2^k)^{2^{k-1}}$ in $\mathbb{Z}[\zeta]$. Using the properties of algebraic number fields, we will show that no such factorization is possible with each $a_j = \pm 1$ and $n = 2^k$. We proceed by providing the necessary background to complete the proof.

Lemma 2.2.3 The polynomial $p_k(x)$ is irreducible over $\mathbb{Q}$.

Proof. Suppose in order to reach a contradiction, that $p_x(x)$ is reducible over $\mathbb{Q}$. Then $p_k(x+1)$ is reducible over $\mathbb{Q}$ as well. By Gauss' lemma, we know that an integral polynomial that factors over $\mathbb{Q}$ also factors over $\mathbb{Z}$. For $p(x), q(x) \in \mathbb{Z}[x]$, let $p(x) \equiv q(x) \mod 2$ mean

that the coefficients of $p(x) - q(x)$ are divisible by 2. But,

$$p_k(x+1) \equiv (x+1)^{2^{k-1}} + 1 \equiv x^{2^{k-1}} \mod 2.$$

It follows that $p_k(x+1) = (x^r + 2a)(x^s + 2b)$ is the only factorization of $p_k(x+1)$ over $\mathbb{Z}$ into two factors of degree greater than or equal to one. Here we require that $r + s = 2^{k-1}$ with a, b polynomials of degree less than r and s, respectively. We thus have that the constant term of $p_k(x+1)$ is a multiple of 4, which is clearly false. □

Let $H = (a_{i-j})$ be an $n \times n$ circulant Hadamard matrix and denote the eigenvalues of H as

$$\gamma_j = a_0 + a_1 zeta^j + a_2\zeta^{2j} + \cdots + a_{n-1}\zeta^{(n-1)j}.$$

We provide the following lemma:

Lemma 2.2.4 For $H = (a_{i-j})$ an $n \times n$ circulant Hadamard matrix with eigenvalues γ_j, $1 \leq j \leq n$, we have that $|\gamma_j| = \sqrt{n}$.

Proof. Consider the matrix $\frac{1}{\sqrt{n}}H$, which is a real orthogonal matrix. So its eigenvalues have absolute value 1 and it follows that $|\gamma_j| = \sqrt{n}$ for $1 \leq j \leq n$ □

Lemma 2.2.5 There exists a unit u in $\mathbb{Z}[\zeta]$ such that $2 = (1-\zeta)^{n/2}u$. (2)

Proof. Write

$$x^{n/2} + 1 = \prod_{j=0 \ j \ odd}^{n-1} (x - \zeta^j).$$

Letting $x = 1$, we have that

$$2 = \prod_{j \ odd} (1 - \zeta^j).$$

But $1 - \zeta^j = (1-\zeta)(1 + \zeta + \cdots + \zeta^{j-1})$, and so if we can show that $(1 + \zeta + \cdots + \zeta^{j-1})$ is a unit in $\mathbb{Z}[\zeta]$ when j is odd, we are done. Letting $j\bar{j} \equiv 1(\mod n)$, then $\zeta^{j\bar{j}} = \zeta^1$ and so we have that

$$\begin{aligned}(1 + \zeta + \cdots + \zeta^{j-1})^{-1} &= \tfrac{1-\zeta}{1-\zeta^j} \\ &= \tfrac{1-(\zeta^j)^{\bar{j}}}{1-\zeta^j} \in \mathbb{Z}[\zeta],\end{aligned}$$

as was to be shown. □

Lemma 2.2.6 We have that $\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{F}_2$.

Proof. Write $R = \mathbb{Z}[\zeta]/(1-\zeta)$. We first note that 2 is not a unit in $\mathbb{Z}[\zeta]$ since $1/2$ is not an algebraic integer as the only rationals which are algebraic integers are the integers. It follows from lemma 2.2.4 that $(1-\zeta)$ is also not a unit in $\mathbb{Z}[\zeta]$. Indeed, if $(1-\zeta)$ were a unit then $2 = (1-\zeta)^{n/2}u$ would be a unit, which is a contradiction.Thus, we have that $r \neq 0$. But $\zeta^j - 1 = (\zeta - 1)(\zeta^{j-1} + \cdots + 1)$ for all j,and so $\zeta^j = 1$. From the previous lemma we have that $0 = 2$ in R and since all elements of R can be exprssed as some $m \in \mathbb{Z}$, it follows that R has only two elements, namely 0 and 1. Thus, $R \cong \mathbb{F}_2$ as was to be shown. □

Lemma 2.2.7 For all $0 \leq j \leq n-1$ there is an integer h_j such that

$$a_0 + a_1\zeta^j + a_2\zeta^{2j} + \cdots + a_{n-1}\zeta^{(n-1)j} = v_j(1-\zeta)^{h_j},$$

where v_j is a unit in $\mathbb{Z}[\zeta]$.

Proof. From Lemma 2.2.5, we have that 2 is a multiple of $1-\zeta$. This together with (1) tells us that

$$\prod_{j \ odd} = 0^{n-1}(a_0 + a_1\zeta^j + a_2\zeta^{2j} + \cdots + a_{n-1}\zeta^{(n-1)j} = 0$$

in $\mathbb{Z}[\zeta]$. We showed in Lemma 2.2.6 that $\mathbb{Z}[\zeta]/(1-\gamma)$ is isomorphic to $\mathbb{F}_2$, which is an integral domain, and so it follows that $1-\gamma$ divides some factor of $(a_0+a_1\zeta^j+a_2\zeta^{2j}+\cdots+a_{n-1}\zeta^{(n-1)j}$. We can thus divide this factors well as the right-hand side of (2) by $1-\zeta$. We can continue this process until the right-hand side becomes the unit u. We have thus demonstrated that each factor of the original product has the form $v(1-\zeta)^h$, with v a unit, as was to be shown. □

Recalling that for $0 \leq j \leq n-1$, γ_j denotes the eigenvalues of H, we have the following corollary.

Corollary 2.2.8 For γ_0 and γ_1, we have that $\gamma_0/\gamma_1 \in \mathbb{Z}[\zeta]$ or $\gamma_1/\gamma_2 \in \mathbb{Z}[\zeta]$.

Proof. We first note that Lemma 2.2.7 guarantees that each γ_j is of the form $v_j(1-\zeta)^{h_j}$. When $h_0 \geq h_1$, we have that $\gamma_0/\gamma_1 \in \mathbb{Z}[\zeta]$; If $h_0 < h_1$, we have that $\gamma_1/\gamma_0 \in \mathbb{Z}[\zeta]$. □

Lemma 2.2.9 If α is an algebraic integer such that α and all of its conjugates have absolute value 1, then α is a root of unity.

Proof. Since α is an algebraic integer, it is a root of some monic polynomial over $\mathbb{Z}$, say $\mathbb{Z}$ is $\prod_{i=1}^{d}(x-\alpha_i)$. Thus, α^n is a root to the polynomial $\prod_{i=1}^{d}(x-\alpha_i^n)$ over $\mathbb{Z}$, which is also of degree d, with all of its roots having absolute value equal to 1. Since there can only be finitely many such polynomials, we have that $\alpha^n = \sigma(\alpha) = \alpha_j$ for some j and for some Galois conjugation of σ. Therefore, α^n is a root of $\prod_{i=1}^{d}(x-\alpha_i)$, for any n. Whence, $\sigma^m(\alpha) = \alpha$ implies that $\alpha^{n^m} = \alpha$ and so $\alpha_j^m = \alpha$, from which it follows that $\alpha^{n^m-1} = 1$. □

Lemma 2.2.10 (Kronecker) Let ζ be a root of unity and $\alpha \in \mathbb{Q}[\zeta]$ with $|\alpha| = 1$. Then α is a root of unity.

Proof. Recall that the Galois group of the field extension $\mathbb{Q}(\tau)/\mathbb{Q}$ is abelian. Take β to be a conjugate of α, so that $\beta = \omega(\alpha)$, where ω is some automorphism of $\mathbb{Q}(\zeta)$. Consider the equation $\alpha\bar{\alpha} = 1$. Complex conjugation is an automorphism of $\mathbb{Q}(\zeta)$, and so it commutes with ω. Thus applying ω to both sides of $\alpha\bar{\alpha} = 1$ yields the equation $\beta\bar{\beta} = 1$. We have thus established that all of the conjugates of α are of absolute value one. It follows from Lemma 2.2.9 that α is a root of unity as well. □

We know proceed to the main theorem of this chapter.

Theorem 2.2.11 There does not exist a (real) circulant Hadamard matrix H of order 2^k, $k \geq 3$.

Proof. We first note that from Lemma 2.2.4 we have that

$$\gamma_1/\gamma_0| = |\gamma_0/\gamma_1| = 1$$

Thus, Corollary 2.2.8 and Lemma 2.2.10 provide that $\gamma_0 = \zeta^{-r}\gamma_1$ for some $r \in \mathbb{Z}$. We can thus expand γ_0 and $\zeta^{-r}\gamma_1$ as integer combinations of $1, \zeta, \zeta^2, \cdots, \zeta^{n/2-1}$ uniquely as follows:

$$\gamma_0 = a_0 + a_1 + a_1 + \cdots + a_{n-1} = \pm n/2$$

$$\begin{aligned}\zeta^{-r}\gamma_1 &= \zeta^{-r}((a_0 - a_{n/2}) + (a_1 - a_{n/2-1})\zeta + \cdots) \\ &= (a_{r-a} - a_{n/2+r}) + (a_{r+1} - a_{n/2+r+1})\zeta + \cdots\end{aligned}$$

We can thus equate the coefficients of ζ^0 to get $\pm n/2 = a_r - a_{n/2+r}$. But each a_i has absolute value equal to one, and so it follows that n must be less than or equal to 4. $\square$

Chapter 3

Butson Type Matrices

3.1 Butson type Hadamard matrices

Definition 3.1.1 Let $n, k \in \mathbb{Z}_+$. Then, $BH(n,k)$ is defined to be the set of all Hadamard matrices of dimension n with entries, k-th roots of unity, i.e., if $H \in BH(n,k)$, 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. We immediately note that $F_n \in BH(n,n)$ and in our next theorem provide as an example due to Petrescu, which is also a Butson Type matrix.

Theorem 3.1.2 (*Petrescu*) The matrix

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

is Hadamard where $\epsilon = e^{2\pi i/6}$. Petrescu's matrix has had considerable impact on the theory of Hadamard matrices. His method for discovering this matrix involved the use of a computer to minimize a set of equations, which governed a six dimensional Hadamard matrix. This

method has been successfully employed by several other researchers in the field in search for additional Hadamard matrices. We can also extend Petrescu's matrix to a one dimensional affine family of Hadamard matrices given by

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

where $|a| = 1$.

Petrescu's research has also been generalized to create infinite parametric families of Hadamard matrices for dimensions $p = 13, 19$ and 31. The interested reader is referred to [6]. Notice that Petrescu's example has also provided a non-trivial example of an Butson type Hadamard matrices, as $P_7 \in BH(7, 6)$.

Finding Hadamard matrices with arbitrary unimodular entries can be extremely difficult, which is why Butson type Hadamard matrices are so important. The further restrictions imposed on the entries of a Butson type matrix make the task of discovering new Hadamard matrices less daunting, as one can restrict the search to matrices that are of Butson type.
Several questions arise concerning Butson type matrices, $BH(n, k)$. For example, when is $BH(n, k) = \emptyset$? We know that both $BH(n, n)$ and $BH(7, 6)$ are non-empty. We are naturally prompted to consider for which $n, k \in \mathbb{Z}$ is $BH(n, k) = \emptyset$.
Below we present two theorems concerning obstructions on the existence of Butson type matrices.

Theorem 3.2.2 Let p, q be distinct primes and $0 < l, m \in \mathbb{Z}$ Then we have $BH(p^l, q^m) = \emptyset$.

Proof. In order to reach a contradiction, suppose that there exists a $H = (a_{i,j}) \in BH(p^l, q^m)$. We may assume that H is dephased. By letting $\epsilon = e^{2\pi i/q^m}$, we have $k_1, k_2, \cdots, k_{p^l-1}$ such that $(a_{1,j}) = \epsilon^{k_j}$, for $1 \leq j \leq p^l - 1$. We thus have that $1 + \epsilon^{k_1} + \cdots + \epsilon^{k_{p^l-1}} = 0$. Set

$g(x) = 1 + x^{k_1} + \cdots + x^{k_{p^l-1}}$. But then $g(\epsilon) = 0$ and so it follows that $\Phi_{q^m}(x)$ divides $g(x)$, i.e. $g(x) = \Phi_{q^m}(x) \cdot \alpha(x)$. We can evaluate g at $x = 1$ to obtain that $p^l = q \cdot \alpha(1)$. Thus we have shown that q divides p^l, which is clearly false. □

The next result is due to Winterhof.

Theorem 3.2.3 Winterhof Let n be odd. If the square free part of n is divisible by a prime of the form $6k + 5$, then $BH(n, 6) = \emptyset$. Note that the square of the determinant of a matrix $H \in BH(n, 6)$ must be of the form $A^2 + 3B^2$ since for $H \in BH(n, 6)$ we have entries based on $\epsilon = \frac{-1+i\sqrt{3}}{2}$ and so $det(H) = a + i\sqrt{3}b$ (entries in the ring $\mathbb{Z}$ implies the determinant will also be in the same ring). Thus it follows that $|det(H)|^2 = a^2 + b^2$. We will use this fact as well as the following lemma in our proof of theorem 3.2.3.

Lemma 3.2.4 Let A and B be integral numbers such that $A^2 + 3B^2 = n$. Then every prime divisor p of the square free part of n is of the form $6k + 3$ or $6k + 1$.

Proof. That every prime number p of the form $6k+1$ also has the form x^2+3y^2 is well known and the reader is referred to [6]. We also note that $3 = 0^2 + 3 \cdot 1^2$ and $q^2 = q^2 + 3 \cdot 0^2$, for any integer q. Furthermore, if two integers, say n_1 and n_2 have this form, then so to does there product, as $n_1 n_2 = (x_1 + 3y_1^2)(x_2 + 3y_2^2) = (x_1x_2 + 3y_1y_2)^2 + 3(x_1y_2 - x_2y_1)^2$. We continue by demonstrating that numbers other than perfect square, primes of the form $6k + 1$, and 3, cannot have the form $x^2 + 3y^2$.

In order to reach a contradiction, suppose that

$$A^2 + 3B^2 = p^2 r, \qquad (3)$$

where r is square free. Without loss of generality, we may assume A, B and r are all pairwise relatively prime, as we can always divide A, B and r by their greatest common divisor.

Notice that if r is even, then A and B must both be odd, and so the left hand side of (3) must be divisible by 4 but not 8. But this is a contradiction, as the right hand side of (3) is divisible by 8.

If $p > 3$ and p divided r, then we have that $A^2 \equiv -3B^2 (\mod p)$. But A and B are nonzero modulo p and so -3 is a quadratic residue modulo p. Since p is also of the form $6k + 5$, we notice that

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = (-1)^{p-1} \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

which shows -3 is not a quadratic residue modulo p. □

We now complete the proof of theorem 3.3.

Proof. For any $H \in BH(n, 6)$, we have that

$$|det(H)| = |A + B\zeta| = n^{n/2},$$

which in turn gives us that $(2A - B)^2 + 3B^2 = 4n^n$. We now are in a position to apply Lemma 3.4. Since n is odd, the square free part of $4n^n$ is simply the square free part of n. But the square free part of n cannot have a prime divisor of the form $6k + 5$. The result follows. □

Chapter 4

Conclusions

Hadamard matrices have a simple but elagant structure. They have been studied for over 150 years, yet there is still much to learn about there characterization, existence, as well as their interplay with other modern areas of mathematics and fields of science at large. In 1983 Popa [4] noticed the connection between Hadamard matrices and von Neumann algebras, which characterized under what conditions a unitarty matrix U is of the form $\frac{1}{\sqrt{n}}H$, where H is Hadamard. In this sense, Hadamard matrices appear in the study of subfactor theorty and statistical mechanics.

Bibliography

[1] Assmus, E. F. and Key, J. D. (1992). *Designs and their Codes*. Number 103. Cambridge University Press. 5

[2] Draghici, T. (2007). MS Windows NT hadamard's maximum determinant problem. v

[3] Hadamard, J. (1893). Résolution dune question relative aux déterminants. *Bull. sci. math*, 17(1):240–246. v, 1

[4] Popa, S. (1983). Orthogonal pairs of*-subalgebras in finite von neumann algebras. *Journal of Operator Theory*, pages 253–268. 22

[5] Stanley, R. P. (2012). Topics in algebraic combinatorics. *Course notes for Mathematics*, 192. 13

[6] Szöllősi, F. (2011). Construction, classification and parametrization of complex hadamard matrices. *arXiv preprint arXiv:1110.5590*. 19

[7] Tadej, W. and Życzkowski, K. (2006). A concise guide to complex hadamard matrices. *Open Systems & Information Dynamics*, 13(02):133–177. 10

[8] Turyn, R. J. (1965). Character sums and difference sets. *Pacific J. Math.*, 15:319–346. 5, 13

[9] Wallis, W. D. and Wallis, J. (1969). Equivalence of hadamard matrices. *Israel Journal of Mathematics*, 7(2):122–128. 10

[10] Williamson, J. (1944). Hadamard's determinant theorem and the sum of four squares. *Duke Math. J.*, 11:65–81. 4, 5

Vita

Gregory Allen Schmidt was born in the twentieth century outside of the U.S.A. He dropped out of high school in the ninth grade and later went on to get a G.E.D. He susequently enrolled in the University of Georgia, where he recieved a B.S. in Mathematics. After graduation he traveled throughout much of Asia and South America. Upon returning to the United States he began his career as a Georgia 6-12 mathematics teacher, which also lead to his enrollment and completion of an M.A. in Mathematics from the University of Georgia. After teaching all grades 8-12 he accepted a graduate teaching assistantship at The University of Tennessee, Knoxville, where he completed a M.S. in Mathematics with a thesis on the classification of Hadamard matrices.