A Survey of the Hadamard Conjecture

Eric Tressler

Thesis submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Mark Shimozono, Chair
Gail Letzter
Daniel Farkas

22 April, 2004
Blacksburg, Virginia

Keywords: BIBD, Coding Theory, Clique, Design Theory, Hadamard

A Survey of the Hadamard Conjecture

Eric Tressler

Abstract

Hadamard matrices are defined, and their basic properties outlined. A survey of historical and recent literature follows, in which a number of existence theorems are examined and given context. Finally, a new result for Hadamard matrices over $\mathbb{Z}_2$ is presented and given a graph-theoretic interpretation.

Contents

List of Figures

1 Introduction

1.1 Background

Definition 1.1. An *Hadamard matrix* is an $n \times n$ matrix H with entries in $\{-1, 1\}$ such that any two distinct rows or columns of H have inner product 0.

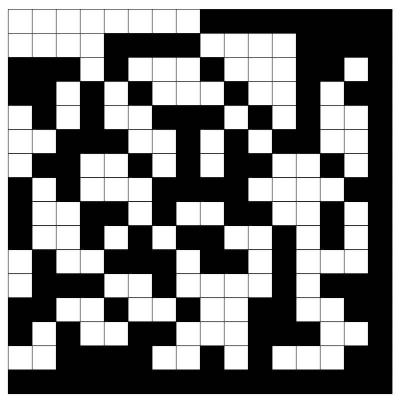

Figure 1: An Hadamard matrix

Hadamard matrices admit several other characterizations; an equivalent definition states that an Hadamard matrix H is an $n \times n$ matrix satisfying the identity

$$HH^T = nI_n.$$

In Figure 1, black squares represent -1s and white squares represent 1s. This convention will be assumed for the rest of the paper.

Definition 1.2. A *binary Hadamard matrix* is an $n \times n$ matrix M (where n is 1 or even) with entries in $\{0, 1\}$ such that any two distinct rows or columns of M have Hamming distance $n/2$.

The *Hamming distance* between two vectors is simply the number of entries at which they differ. Hadamard matrices are clearly in bijection with binary Hadamard matrices; we will therefore work in both settings, with the understanding that results concerning Hadamard matrices have analogues in terms of binary Hadamard matrices, and vice versa.

1.2 Motivation

Coding theory is a relatively new field of mathematics that deals with methods for ensuring reliable information exchange. A *code* is simply a set of words (with elements in some alphabet) to which some meaning has been ascribed. Morse code, for instance, is a set of words in the alphabet $\{\cdot, -\}$ such that words represent various letters and punctuation marks in the English alphabet. Coding theory is concerned primarily with *error-correcting* codes – that is, codes which are correctly translatable given a certain amount of transmission error. This entails first detecting transmission errors (*error detection*) and then correcting them if possible (*error correction*).

If the rows of an Hadamard matrix are taken to be the words of a code, that code will have nice error correcting properties: since any two words will have Hamming distance $n/2$ from each other, as many as $n/2-1$ bits can be transmitted incorrectly and still result in a correct translation. Though many protocols make use of Hadamard matrices, the true reason for the interest in these matrices has less to do with error correction than with a deceptively simple conjecture left by their namesake.

1.3 The Hadamard Conjecture

Conjecture 1.3 (Hadamard). *An $n \times n$ Hadamard matrix exists for $n = 1$, $n = 2$, and $n = 4k$ for any $k \in \mathbb{N}$.*

It is known that a necessary condition for the existence of an $n \times n$ Hadamard matrix is that $n = 1, 2, 4k$ for some k (this is proven below in Proposition 2.6). That this condition is also sufficient is known as the Hadamard conjecture, and has been the subject of a vast amount of literature in recent decades. Before commenting on the state of the conjecture, we will first make note of some basic properties of Hadamard matrices.

2 Basic Properties and Definitions

Many of the following properties of Hadamard matrices are easily established, and are provided without proof. First, a word about notation. In $\mathbb{Z}_2^n$, we will let

$$0^n = (\underbrace{0, \ldots, 0}_{n})$$

and

$$1^n = (\underbrace{1, \ldots, 1}_{n}).$$

If $A \in \mathbb{Z}_2^n$, then let $o(A) = A \cdot 1^n$ denote the number of 1s in A. For $A, B \in \mathbb{Z}_2^n$, let $d(A, B)$ denote the Hamming distance between A and B. Note that Hamming distance is a metric on $\mathbb{Z}_2^n$ and induces a metric on $\{-1, 1\}^n$ via the obvious bijection.

If $A \in \mathbb{Z}_2^n$, let $\overline{A} = 1^n + A \in \mathbb{Z}_2^n$; call $\overline{A}$ the *complement* of A (the analogous operation on $\{-1, 1\}^n$ is simply negation). For a matrix M with entries in $\mathbb{Z}_2$, we may occasionally write $\overline{M}$ to denote the matrix formed by taking the complement of each row of M. For a matrix M, M_i or $M_{i,*}$ will denote the ith row of M, and $M_{*,j}$ will denote the jth column; $M_{i,j}$ will denote the jth entry in the ith row of M.

Proposition 2.1. *If a matrix M' is formed by interchanging two rows or columns of a matrix M, then M' is Hadamard if and only if M is Hadamard.*

Proposition 2.2. *If a matrix M' is formed from a matrix M by replacing some row $M_{i,*}$ by $\overline{M_{i,*}}$ or column $M_{*,i}$ by $\overline{M_{*,i}}$ then M' is Hadamard if and only if M is Hadamard.*

Definition 2.3. Two Hadamard matrices M, M' are said to be *equivalent* if M' can be produced from M by a sequence of swaps and complement operations, applied to both rows and columns.

The above definition defines an equivalence relation on the set of all Hadamard matrices; Thus, we say that there is only one Hadamard matrix of order 2, though it has eight different expressions.

Definition 2.4. A *normalized* Hadamard matrix is an Hadamard matrix whose final row and column consist entirely of 0s.

Since we may replace any row or column of an Hadamard matrix M by its complement and still have an Hadamard matrix, it is often useful to normalize an Hadamard matrix by taking the complement of appropriate columns until the final row consists entirely of 0s and then taking the complement of appropriate rows until the final column consists entirely of 0s.

For our purposes, it will often be sufficient to assume that an Hadamard matrix has final row consisting of 0s; we will call such a matrix *row-normalized.* Thus, we will consider both the second and third matrices in Figure 2 to be row-normalized, though only the third is normalized.

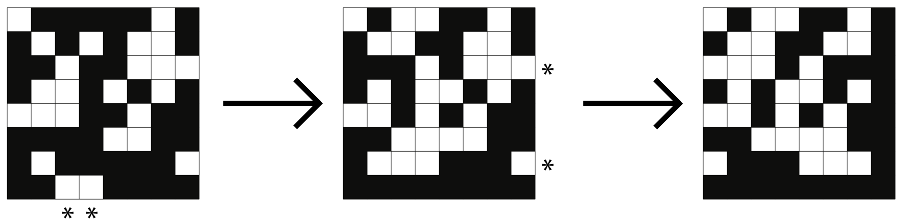

Figure 2: An Hadamard matrix, first row-normalized and then completely normalized. Rows and columns marked by asterisks are those complemented in succeeding figures.

Proposition 2.5. *Any $n \times n$ matrix ($n = 1$ or even) with the property that any two distinct rows are distance $n/2$ from each other is an Hadamard matrix.*

Proof. Let H be an $n \times n$ matrix with entries in $\{-1, 1\}$ with the property that any two distinct rows are distance $n/2$ from each other. Then the rows of H are orthonormal; H is an orthogonal matrix. Therefore, it is automatic that H^T is orthogonal as well, and so we see that the columns of H must also be orthonormal. Thus, any two columns of H are distance $n/2$ from each other, and so H is Hadamard by definition. □

Note that the above property also applies to binary Hadamard matrices; if H is an $n \times n$ binary matrix with the property that any two rows are distance $n/2$ from each other, we may replace all 0s in H by -1s and call the resulting matrix H'. By the above, H' is Hadamard, and so H is therefore Hadamard as well.

Proposition 2.6. *There exist no $n \times n$ Hadamard matrices for $n \notin \{1, 2, 4k : k \in \mathbb{N}\}$.*

Proof. Let M be an $n \times n$ Hadamard matrix, and let M' be its normalization. Suppose M' contains distinct rows A, B, and suppose that neither A nor B is the 0 row. Then $o(A) = o(B) = n/2$, but since M' is Hadamard, $d(A, B) = n/2$. Of the $n/2$ positions at which A has a 1, suppose B has a 1 at k of these. The remaining $n/2 - k$ 1s of B must be distributed among positions at which A has a 0. Thus, A and B differ at $n/2 - k$ positions at which A has a 1, and $n/2 - k$ positions at which A has a 0. This gives us that $d(A, B) = 2(n/2 - k)$, and so $k = n/4$. Since k is an integer, so too must $n/4$ be an integer. □

3 Historical Results

3.1 The Kronecker Product Construction

While proof of the Hadamard conjecture itself remains elusive, there are quite a number of existence results for various subclasses of Hadamard matrices. The first, and simplest, is known as the *Kronecker product* construction [13].

Definition 3.1. If S, T are matrices, their *Kronecker product* $S \otimes T$ is the matrix U constructed by replacing each $S_{i,j}$ in S by $S_{i,j}T$.

If H_n, H_m are Hadamard matrices of orders n and m, respectively, then their Kronecker product $H_n \otimes H_m$ is an Hadamard matrix of order nm. As an immediate corollary, the existence of an Hadamard matrix of order n implies the existence of an Hadamard matrix of order $2n$, via the Kronecker product construction. The Kronecker product of n copies of

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

is said to be an Hadamard matrix of *Sylvester type*. They are so-called because Hadamard matrices were first studied by Sylvester in 1867, under the name "anallagmatic pavement" [14].

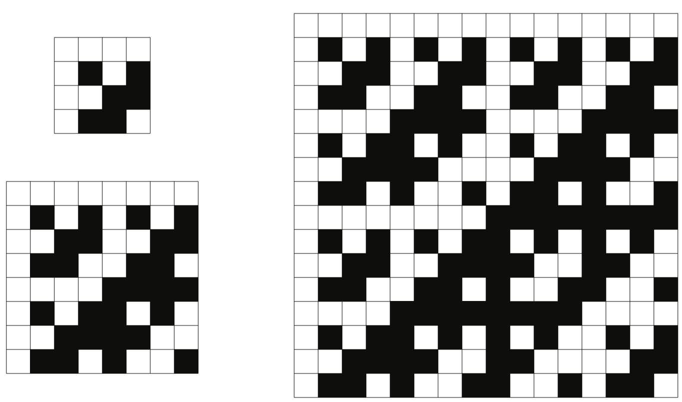

Figure 3: Some Sylvester type Hadamard matrices. White squares represent +1, black squares -1.

If H_n, H_m are binary Hadamard matrices of orders n and m, respectively, then replacing all 0s in H_n by $\overline{H_m}$ and all 1s in H_n by H_m yields an Hadamard matrix of order nm; this operation is analogous to the Kronecker product.

3.2 The Paley Construction

In 1933, Raymond Paley introduced a new family of Hadamard matrices and proved their existence ([11],[1]). He also provided methods for constructing these matrices. Paley's constructions have been generalized; Assmus and Key refer us to chapter 14 of Hall ([9]) for a treatment of these generalizations. The definitions and treatment herein are consistent with (and taken from) those of Assmus and Key [1].

To discuss Paley's work, we will first need the notion of quadratic residues of $\mathbb{F}_q$.

Definition 3.2. An element $s \in \mathbb{F}_q$ is a *quadratic residue* (or *square*) if $s = t^2$ has a solution in $\mathbb{F}_q$.

Lemma 3.3. *If $q = p^r$, where p is an odd prime, the exactly half the nonzero elements of $\mathbb{F}_q$ are squares. Moreover, -1 is a square if and only if $q \equiv 1 \mod 4$.*

Definition 3.4. If q is a power of an odd prime, then χ, the *Legendre symbol*, is the following mapping:

$$\chi : F \to \{0, 1, -1\},$$

where $\chi(0) = 0$ and

$$\chi(x) = \begin{cases} 1 & \text{if x is a non-zero square} \\ -1 & \text{if x is a non-square} \end{cases}$$

Definition 3.5. Using the elements of $\mathbb{F}_q$ as row and column labels, define a $q \times q$ matrix, $\mathbb{Q} = (q_{x,y})$, called a *Jacobsthal matrix*, by

$$q_{x,y} = \chi(y - x).$$

We are now prepared to present Paley's construction of Hadamard matrices.

Theorem 3.6. *If $q \equiv 3 \mod 4$ and Q is a Jacobsthal matrix for $\mathbb{F}_q$, then*

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

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

Proof. See Assmus and Key [1]. □

An Hadamard matrix generated by the above method is known as a *Paley type* Hadamard matrix.

Definition 3.7. An $n \times n$ matrix M is called *circulant* (sometimes *forward circulant*) if $M_{i,j} = M_{i',j'}$ whenever $i - j \equiv i' - j' \bmod n$. Equivalently, M is circulant if the ith row of M is given by the first row of M, rotated to the right $i - 1$ positions.

Example 3.8. Let $q = 23$; the nonzero squares of $\mathbb{F}_{23}$ are 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18. Therefore, the Jacosbsthal matrix Q is the circulant matrix with first row given by

$$Q_{1,*} = (0, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1).$$

Now by Theorem 3.6, we have an Hadamard matrix H (Figure 4) given by

$$\begin{pmatrix} 1 & 1^n \\ (1^n)^T & Q - I \end{pmatrix}.$$

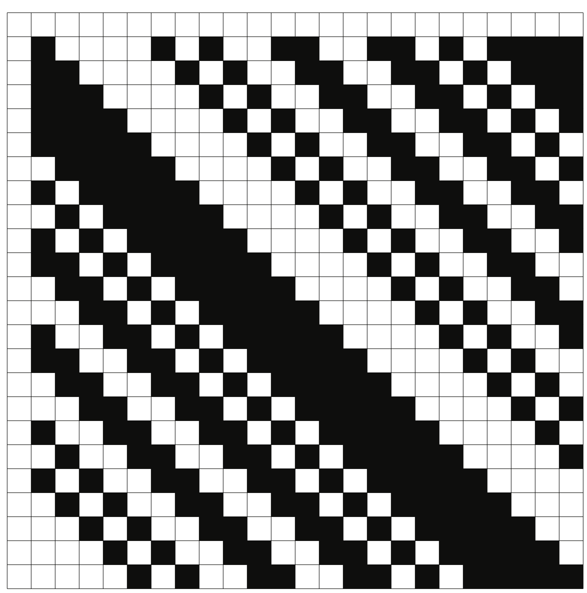

Figure 4: The Paley type Hadamard matrix from Example 3.8.

Paley's original paper [11] gives two other existence theorems, which we will list here:

Theorem 3.9. *Let m be divisible by 4 and of the form $2^k(p^h+1)$, where p is an odd prime. Then we can construct an Hadamard matrix of order m.*

Theorem 3.10. *Let m be divisible by 4 and of the form $2^k p(p+1)$, where $p \equiv 3 \mod 4$ is prime. Then we can construct an Hadamard matrix of order m.*

Proofs of these results can be found in [11]. Observe that Theorem 3.9 is stronger than Theorem 3.6; the former is consistent with the statement in Paley's paper. Paley's theorems, taken together with the Kronecker product construction (which Paley describes in his paper), dispose of an enormous number of cases; the first order (excluding 1 and 2) for which they are not applicable is 92 [11].

3.3 The Williamson Construction

In 1944, Williamson proved the following result ([13],[15]):

Theorem 3.11. *Suppose there exist $n \times n$ matrices A, B, C, and D, that satisfy the following properties:*

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

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

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

Definition 3.12. Call matrices A, B, C, and D satisfying the above properties *Williamson matrices.*

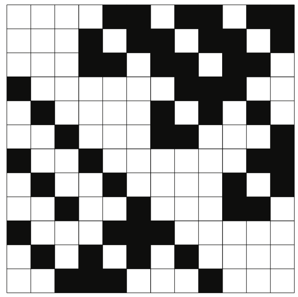

Figure 5: An Hadamard matrix of Williamson type.

In practice, A, B, C, and D are typically taken to be circulant matrices [13]; this ensures that the matrices commute. Satisfaction of the third criterion is nontrivial, and generally requires a computer search. This method was employed by Baumert, Golomb and Hall in 1962 to find an Hadamard matrix of order 92 [2]; the matrices A, B, C, and D below are circulant, and so only their first rows are shown (-1s are represented by 0s):

$$A_{1,*} = (1,1,0,0,0,1,0,0,0,1,0,1,1,0,1,0,0,0,1,0,0,0,1)$$
$$B_{1,*} = (1,0,1,1,0,1,1,0,0,1,1,1,1,1,1,0,0,1,1,0,1,1,0)$$
$$C_{1,*} = (1,1,1,0,0,0,1,1,0,1,0,1,1,0,1,0,1,1,0,0,0,1,1)$$
$$D_{1,*} = (1,1,1,0,1,1,1,0,1,0,0,0,0,0,0,1,0,1,1,1,0,1,1)$$

These are, in fact, the only existing Williamson matrices of order 23 [8]. Williamson's method has been used to find Hadamard matrices of several other orders, including 116 [4], a later result by Baumert. There also exists at least one known infinite family of Williamson-type Hadamard matrices [8]:

Theorem 3.13. *If q is a prime power, $q \equiv 1 \bmod 4$, $q + 1 = 2t$, then there exists a Williamson matrix of order $4t$: $C = D$, and A and B differ only on the main diagonal.*

A more thorough history of various searches and results for Hadamard matrices of Williamson type can be found in Georgiou, Koukouvinos, and Seberry [8]. This source also provides a description of the algorithms used in computer searches for Williamson matrices.

3.4 Baumert-Hall Arrays

In this section, we present the treatment of Baumert-Hall arrays by Geramita and Seberry [8].

Definition 3.14. An *orthogonal design of order* n *and type* $(s_1, \ldots, s_k)$, $s_i \in \mathbb{N}$, is an $n \times n$ matrix X with entries from $\{0, \pm x_1, \ldots, \pm x_k\}$ (the x_i commuting indeterminates) satisfying

$$XX^T = \left(\sum_{i=1}^{k} s_i x_i^2 \right) I_n.$$

Geramita and Seberry [8] offer an equivalent definition: "each row of X has s_i entries of the type $\pm x_i$ and the rows are orthogonal under the Euclidean inner product."

Definition 3.15. An orthogonal design of type (t, t, t, t) and order $4t$ is called a *Baumert-Hall array of order* t.

The reader will recognize Williamson's array (not to be confused with Williamson matrices, which we will make use of shortly),

$$\begin{pmatrix} A & B & C & D \\ -B & A & D & -C \\ -C & -D & A & B \\ -D & C & -B & A \end{pmatrix},$$

as a Baumert-Hall array of order 1. Baumert-Hall arrays admit generalizations of Williamson's theorem, though unfortunately it is very difficult in general to find a Baumert-Hall array of order n, even for small n.

Theorem 3.16 (Baumert-Hall). *If there exists a Baumert-Hall array of order* t *and Williamson matrices of order* n*, then there exists an Hadamard matrix of order* $4nt$.

This theorem is proved simply by replacing the variables in the Baumert-Hall array by the Williamson matrices, also yielding a direct construction. There exist quite a number of further results involving Baumert-Hall arrays; unfortunately, their scarcity limits the usefulness of such results. Several Baumert-Hall arrays can be found in [8]; we will turn our attention now to two vastly different characterizations of Hadamard matrices.

4 Two Characterizations of Hadamard Matrices

4.1 Hadamard Matrices as BIBDs

The following definitions are taken from Stinson [13], and are fairly standard. They are given a different treatment in Assmus and Key [1], which includes a more thorough historical perspective of the following material.

Definition 4.1. A *block design* (sometimes simply *design*) is a pair $(X, \mathcal{A})$ such that

1. X is a set of elements (*points*), and
2. $\mathcal{A}$ is a collection of subsets of X (*blocks*).

The most commonly studied type of block design is known as a balanced incomplete block design (or BIBD).

Definition 4.2. Let $v, k, \lambda \in \mathbb{N}$ with $v > k \geq 2$. A (v, k, λ)-*balanced incomplete block design* ($(v, k, \lambda) - BIBD$) is a design $(X, \mathcal{A})$ such that

1. $|X| = v$,
2. each block contains exactly k points, and
3. every pair of distinct points is contained in exactly λ blocks.

BIBDs are so-called because no block can contain all points (this is easily verified) and because these designs are balanced (that is, property 3 in the above definition holds). BIBDs exhibit many important structural properties; two of these will be useful for us to consider. Here, again, we refer to Stinson [13], though the following properties are widely known.

Theorem 4.3. *In a (v, k, λ)-BIBD, every point occurs in exactly*

$$r = \frac{\lambda(v-1)}{k-1}$$

blocks.

Theorem 4.4. *A (v, k, λ)-BIBD has exactly*

$$b = \frac{vr}{k} = \frac{\lambda(v^2 - v)}{k^2 - k}$$

blocks.

These two theorems indicate that no $(v, k, \lambda) - BIBD$ can exist unless $(k-1) \mid (\lambda(v-1))$ and $(k^2-k) \mid ((\lambda(v^2-v))$. In fact, determining necessary and sufficient conditions for the existence of a $(v, k, \lambda) - BIBD$ is a well-known problem in design theory. We need one more definition before we can establish the relationship between Hadamard matrices and BIBDs:

Definition 4.5. A BIBD in which $b = v$ (or, equivalently, $r = k$ or $\lambda(v-1) = k^2 - k$) is called a *symmetric BIBD*.

Now we present an equivalence between Hadamard matrices and BIBDs, which we attribute to Stinson [13]:

Theorem 4.6. *Let $m > 1$. Then there exists an Hadamard matrix of order $4m$ if and only if there exists a (symmetric) $(4m-1, 2m-1, m-1)$-BIBD.*

Corollary 4.7. *There exists an Hadamard matrix of order $4m$ if $4m - 1$ is a prime power.*

A proof can be found in [13]. Here we will appeal to a standard example to demonstrate this relationship.

Example 4.8. The Fano plane, the projective plane of order two, is a $(7, 3, 1)$-BIBD.

The incidence matrix of the Fano plane is given by

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

The incidence matrix of a BIBD is simply its adjacency matrix when its blocks are considered as edges of a hypergraph (see Bollobás [5] for appropriate definitions). It is easy to verify that if we add a row of 1s and then a column of 1s to this incidence matrix, we have constructed an (binary) Hadamard matrix.

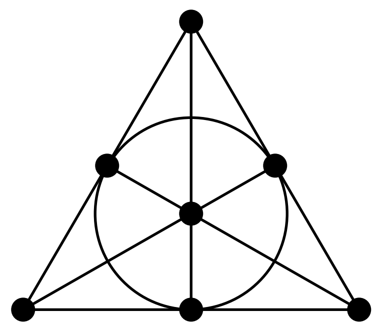

Figure 6: The Fano plane; the lines correspond to blocks.

4.2 Hadamard Matrices as Weighing Matrices

Definition 4.9. A *weighing matrix* of weight k and order n is an $n \times n$ matrix A with entries in $\{-1, 0, 1\}$ such that $AA^T = kI_n$.

An Hadamard matrix of order n, then, is simply a weighing matrix with no entries 0 and with weight n. However, we need only this last condition:

Proposition 4.10. *An $n \times n$ weighing matrix M with weight n must be an Hadamard matrix.*

Proof. Suppose M has weight n (this is clearly the maximal weight for a weighing matrix of order n). $M_{i,i}$ is given by

$$\sum_{j=1}^{n} M_{i,j} M_{j,i}^T = M_{i,*} \cdot M_{i,*} = n.$$

Since $M_{i,j} M_{j,i}^T \in \{-1, 0, 1\}$, we see that $M_{i,*} \cdot M_{i,*} = n$ implies that no element of $M_{i,*}$ can be 0. Thus, M has entries in $\{-1, 1\}$. Now observe that since $M_{s,t} = 0$ for all $i \neq j$, we have that

$$\sum_{k=1}^{n} M_{s,k} M_{k,t}^T = M_{s,*} \cdot M_{t,*} = 0,$$

and so any two rows have inner product 0. By Proposition 2.5, M is an Hadamard matrix. $\square$

In particular, this shows that there exist no weighing matrices of maximal weight for orders $n \notin \{1, 2, 4k : k \in \mathbb{N}\}$. The Hadamard conjecture can be viewed, in this context, as a special case of the more general problem of determining necessary and sufficient conditions for the existence of a weighing matrix of order n and weight k.

5 Recent Results

The constructions given above are frequently cited in the literature, and many recent existence theorems arise from generalizations of these constructions. We will survey a few of these results briefly, and refer the reader to the appropriate literature for proof and context.

Geramita and Seberry [8] present two powerful existence theorems, based partially on a result of Sylvester. First, though, we must define one more class of Hadamard matrices:

Definition 5.1. An Hadamard matrix M is *regular* if the sum of each row over $\mathbb{Z}$ is constant.

Theorem 5.2. *For any $q \in \mathbb{N}$, there exists s dependent on q such that an Hadamard matrix exists of every order $2^t q$ for every $t \geq s$.*

Theorem 5.3.

1. *Given any $q \in \mathbb{N}$, there exists an Hadamard matrix of order $2^s q$ for every $s \geq [2 \log_2(q-3)]$.*
2. *Given any $q \in \mathbb{N}$, there exists a regular symmetric Hadamard matrix with constant diagonal of order $2^{2s} q^2$ for s as before.*

In a sense, this last theorem proves the existence of an Hadamard matrix of "almost all" orders. The Hadamard conjecture itself is equivalent to improving the bound on s from $[2 \log_2(q-3)]$ to 2, though all results of this form to date are dependent on q.

Miyamoto [10] generalizes Paley's construction by way of *C-matrices*, first considered by Paley [11].

Definition 5.4. A C-matrix of order n is an $n \times n$ matrix C with diagonal 0 and all other entries in $\{-1, 1\}$ such that $CC^T = (n-1)I_n$. A C_2-matrix of order $2n$ is a $2n \times 2n$ matrix $D = (d_{i,j})$ such that

1. $d_{i,i} = 0$ for all $i = 1, \ldots, 2n$.
2. $d_{i,n+i} = d_{n+i,i} = 0$ for all $i = 1, \ldots, n$.

3. $DD^T = (2n-2)I_{2n}$.

Theorem 5.5 ([11]). *There exists a C-matrix of order $q+1$ for every odd prime power q.*

We now present a result by Miyamoto [10]:

Theorem 5.6. *Let $q \equiv 1 \mod 4$ be an integer. Suppose there is a C-matrix of order $q+1$ and an Hadamard matrix K of order $q-1$. Then there is an Hadamard matrix H of order $4q$.*

Corollary 5.7. *Let q be a prime power and $q \equiv 1 \mod 4$. If there is an Hadamard matrix of order $q-1$, then there is an Hadamard matrix of order $4q$.*

6 Current State of the Hadamard Conjecture

The Hadamard conjecture has currently been verified for all $n < 428$. The existence theorems above are insufficient to reach this bound, though we will expend some effort in determining which orders we lack.

Paley [11] gives a table of orders $4t$, $1 \leq t \leq 50$, showing which of these orders are disposed of by the results given in his paper (Theorems 3.6 and 3.9, along with the Kronecker product construction – Theorem 3.10 gives no new orders here). We reproduce this information in Table 1, and extend it to include all orders $4t < 428$.

This leaves us with orders 92, 116, 156, 172, 184, 188, 232, 236, 260, 268, 292, 324, 356, 372, 376, 404, and 412 unaccounted for. Baumert, Golomb, and Hall give an Hadamard matrix of order 92 in [2], using Williamson matrices; by the Kronecker product construction, we also get order $92 \cdot 2 = 184$. Baumert and Hall employ Baumert-Hall arrays to give an Hadamard matrix of order 156 in [3]. Baumert gives Hadamard matrices of orders 116 and 232 in [4]. The remaining known orders are typically the result of computer search with Baumert-Hall arrays and Williamson matrices.

The number of inequivalent Hadamard matrices of order n is known only for $n \leq 28$. The number of inequivalent Hadamard matrices of order of order $1, 2, 4, 8, 12, 16, 20, 24, 28$ is, respectively, $1, 1, 1, 1, 1, 5, 3, 60, 487$ [12]. This apparent combinatorial explosion strongly suggests the truth of the Hadamard conjecture.

$4 = 2^2$	$112 = 2^2(3^3+1)$	$220 = 2(109+1)$	$328 = 2(163+1)$
$8 = 2^3$	$116 =$	$224 = 223+1$	$332 = 331+1$
$12 = 11+1$	$120 = 2(59+1)$	$228 = 227+1$	$336 = 2(167+1)$
$16 = 2^4$	$124 = 2(61+1)$	$232 =$	$340 = 2(13^2+1)$
$20 = 19+1$	$128 = 2^7$	$236 =$	$344 = 7^3+1$
$24 = 23+1$	$132 = 131+1$	$240 = 239+1$	$348 = 347+1$
$28 = 3^3+1$	$136 = 2(67+1)$	$244 = 3^5+1$	$352 = 2^3(43+1)$
$32 = 2^5$	$140 = 139+1$	$248 = 2^2(61+1)$	$356 =$
$36 = 2(17+1)$	$144 = 2(71+1)$	$252 = 251+1$	$360 = 359+1$
$40 = 2(19+1)$	$148 = 2(73+1)$	$256 = 2^8$	$364 = 2(181+1)$
$44 = 43+1$	$152 = 151+1$	$260 =$	$368 = 367+1$
$48 = 47+1$	$156 =$	$264 = 263+1$	$372 =$
$52 = 2(5^2+1)$	$160 = 2(79+1)$	$268 =$	$376 =$
$56 = 2(3^3+1)$	$164 = 163+1$	$272 = 271+1$	$380 = 379+1$
$60 = 59+1$	$168 = 167+1$	$276 = 2(137+1)$	$384 = 383+1$
$64 = 2^6$	$172 =$	$280 = 2(139+1)$	$388 = 2(193+1)$
$68 = 67+1$	$176 = 2^2(43+1)$	$284 = 283+1$	$392 = 2^2(97+1)$
$72 = 71+1$	$180 = 179+1$	$288 = 2^2(71+1)$	$396 = 2(197+1)$
$76 = 2(37+1)$	$184 =$	$292 =$	$400 = 2(199+1)$
$80 = 79+1$	$188 =$	$296 = 2^2(73+1)$	$404 =$
$84 = 83+1$	$192 = 191+1$	$300 = 2(149+1)$	$408 = 2^2(101+1)$
$88 = 2(43+1)$	$196 = 2(97+1)$	$304 = 2(151+1)$	$412 =$
$92 =$	$200 = 199+1$	$308 = 307+1$	$416 = 2^2(103+1)$
$96 = 2(47+1)$	$204 = 2(101+1)$	$312 = 311+1$	$420 = 419+1$
$100 = 2(7^2+1)$	$208 = 2(103+1)$	$316 = 2(157+1)$	$424 = 2(211+1)$
$104 = 103+1$	$212 = 211+1$	$320 = 2^2(79+1)$	
$108 = 107+1$	$216 = 2(107+1)$	$324 =$	

Table 1: Table of orders $4t$ for $1 \le t \le 106$.

7 Main Result

The result presented here is new, as far as we have been able to determine. With the many different characterizations of Hadamard matrices, it is entirely possible that the following is more naturally couched in the more general language of design theory or linear algebra; however, we have not been able to find this result in the literature. Note that in the following sections, all Hadamard matrices are taken to be binary Hadamard matrices.

Proposition 7.2 (below) basically states that any $n-2$ nonzero rows of a normalized Hadamard matrix completely determine the other nonzero row (up to complement), and that another such row always exists. To prove this we need the following lemma:

Lemma 7.1. *Let $n, m, k \in \mathbb{Z}$ with $k \le nm$. Suppose we have n identical bins, each with capacity m, and k identical balls to distribute among the bins. Suppose further that a bin with s balls in it has* value *given by $s(m-s)$. Then* *the unique distribution of balls giving the maximum sum of values across all bins is the most even distribution possible.*

Proof. Consider each bin to be initially empty, and hence with value 0. When placing a ball in a bin, we will say that that ball has *worth* given by the change in value it effects when placed in the bin. Thus, a ball placed in an empty bin changes the value of the bin from $0(m)$ to $1(m-1)$, and so has worth $m-1$. Now observe that a ball placed in a bin containing 1 ball already has worth $2(m-2)-1(m-1)=m-3$, a ball placed in a bin containing 2 balls already has worth $3(m-3)-2(m-2)=m-5$, and in general a ball placed in a bin containing s balls already has worth

$$(s+1)(m-s-1)-s(m-s)=m-2s-1.$$

Thus, the sequence given by the worth of successive balls as a bin goes from empty to full is strictly decreasing. It is clear that the maximum sum of values across all bins is given by the placement of balls such that each ball has maximal worth, and that the maximal worth any ball can have results from placing it in the most empty bin available. This results precisely in the most even distribution of all balls among bins, and so we are finished. □

Proposition 7.2. *Let $A_1,\ldots,A_{n-2}\in\mathbb{Z}_2^n$ (n divisible by 4) with $o(A_i)=n/2$ for all i and $d(A_i,A_j)=n/2$ for all $i\neq j$. If $B=\sum_i A_i$, then $o(B)=n/2$ and $d(B,A_i)=n/2$ for all i.*

Proof. Let $A_1,\ldots,A_{n-2}$ be as in the hypothesis. For convenience, we may consider A_i to be the ith row of a matrix, which we will denote by A. For each row $A_{i,*}$, if $A_{i,n}=1$, let $A'_i=\overline{A_i}$; else, let $A'_i=A_i$. We then have an $n-2\times n$ matrix A' with $o(A'_i)=n/2$ for all i and $d(A'_i,A'_j)=n/2$ for all $i\neq j$, with the added restriction that $A'_{*,n}=0$. Let $B'=\sum_i A'_i$.

Let us first establish that $o(B')=n/2$. Define a *row difference* to be a pair $A'_{i,k}\neq A'_{j,k}$. Since $d(A'_i,A'_j)=n/2$ for all $i\neq j$, and there are $\binom{n-2}{2}$ ways to choose rows of A', there are

$$\binom{n-2}{2}\left(\frac{n}{2}\right)=\frac{n(n-2)(n-3)}{4}$$

row differences in A'. Additionally, since $A'_{*,n}=0$, the nth column of A' contributes no row differences. Since $o(A'_i)=n/2$ for all i, there are a total of

$$\left(\frac{n}{2}\right)(n-2)$$

1s distributed among the first $n-1$ columns of A'. Counting row differences columnwise, it is clear that the ith column contributes exactly

$$o(A'_{*,i}) \cdot ((n-2) - o(A'_{*,i}))$$

column differences, the number given by multiplying the number of 1s in the ith column by the number of 0s. It is similarly clear that a column can contain at most

$$\left(\frac{n-2}{2}\right)^2$$

row differences, achieved when the number of 0s is exactly the number of 1s. Suppose $\frac{n}{2}$ columns have $\frac{n-2}{2}$ 1s and $\frac{n}{2}-1$ columns have $\frac{n-2}{2}+1$ 1s. This is the most evenly we can distribute the 1s among the $n-1$ nonzero columns, and this gives us

$$\left(\frac{n}{2}\right)\left(\frac{n-2}{2}\right) + \left(\frac{n}{2}-1\right)\left(\frac{n-2}{2}+1\right) = \frac{n(n-2)}{2}$$

1s, the correct amount. This distribution also gives us the correct number of row differences:

$$\left(\frac{n}{2}\right)\left(\frac{n-2}{2}\right)^2 + \left(\frac{n}{2}-1\right)\left(\frac{n-2}{2}+1\right)\left(\frac{n-2}{2}-1\right) = \frac{n(n-2)(n-3)}{4}.$$

By the lemma above, this is the unique distribution yielding the maximum number of row differences, and so A' must exhibit this distribution. Therefore, $\frac{n}{2}$ columns of A' have an odd number ($\frac{n-2}{2}$) of 1s and $\frac{n}{2}$ have an even number ($\frac{n}{2}-1$ have $\frac{n-2}{2}+1$ and the nth has 0). Thus, B' has $\frac{n}{2}$ 1s and $\frac{n}{2}$ 0s: $o(B') = \frac{n}{2}$.

Now I will show that $d(B', A'_i) = n/2$ for all i. We have established that, of the nonzero columns of A', $\frac{n}{2}$ columns have $\frac{n-2}{2}$ 1s (call these *short* columns) and $\frac{n}{2}-1$ have $\frac{n-2}{2}+1$ 1s (*long* columns). Suppose A'_i has 1s in $n/4+k$ of the short columns. Then since $o(A'_i) = n/2$, A'_i must have 1s in $n/4-k$ of the long columns. Counting the row differences contributed by A'_i, we see that since each short column has $\frac{n-2}{2}$ 1s and $\frac{n-2}{2}$ 0s, A'_i is different from exactly $\frac{n-2}{2}$ other rows at each of its $\frac{n}{2}$ indices corresponding to short columns (this is independent of k and constant across all rows of A'), and so we have $\frac{n(n-2)}{4} = n^2/4 - n/2$ row differences among short columns. There are

$\frac{n}{2} - 1$ long columns; A'_i has 1s on $n/4 - k$ of these and 0s on the remaining $n/4 + k - 1$. Since each long column has $\frac{n-2}{2} + 1$ 1s and $\frac{n-2}{2} - 1$ 0s, we have

$$\begin{aligned}\left(\frac{n}{4} - k\right)\left(\frac{n-2}{2} - 1\right) &= \left(\frac{n}{4} - k\right)\left(\frac{n}{2} - 2\right) \\ &= n^2/8 - kn/2 - n/2 + 2k\end{aligned}$$

row differences on long columns in which A'_i is a 1, and

$$\begin{aligned}\left(\frac{n}{4} + k - 1\right)\left(\frac{n-2}{2} + 1\right) &= \left(\frac{n}{4} + k - 1\right)\left(\frac{n}{2}\right) \\ &= n^2/8 + kn/2 - n/2\end{aligned}$$

row differences on long columns in which A'_i is a 0. Summing these values, we see that A'_i contributes

$$(n^2/4 - n/2) + (n^2/8 - kn/2 - n/2 + 2k) + (n^2/8 + kn/2 - n/2) = n^2/2 - 3n/2 + 2k$$

row differences in total. However, we also know that $d(A'_i, A'_j) = n/2$ for all $i \neq j$, and so A'_i must contribute exactly $n/2$ row differences for each of the remaining $n - 3$ rows. Therefore, A'_i must contribute $(n/2)(n-3) = n^2/2 - 3n/2$ row differences. In other words, $k = 0$, and so A'_i has 1s on exactly $n/4$ of the short columns. However, these are exactly the columns with odd parity, in which B' has 1s, and so on A'_i shares exactly $n/4$ of its $n/2$ 1s with B'. B' has $n/4$ 1s not shared with A'_i, and A'_i has $n/4$ 1s not shared with B': $d(B', A'_i) = n/2$. Since i here is arbitrary, this result holds for each row of A'.

Now note that since $o(B') = n/2$ and $d(B', A'_i) = n/2$ for all i, we have that $d(B', \overline{A'_i}) = n/2$, and so let us invert each row of A' as appropriate to retrieve A. Observe now that if we consider B' as the sum over all of the rows of A', then inverting a row of A' simply changes the parity of each column of A', having the effect of inverting the sum of the rows. Thus, $\sum_i A_i$ is one of $B', \overline{B'}$. But since $d(B', A_i) = n/2$ and $d(\overline{B'}, A_i) = n/2$ for all i, and $o(B') = o(\overline{B'}) = n/2$, we have that in either case $B = \sum_i A_i$ satisfies the hypothesis, and we are finished. □

This result has a particularly natural expression in the form of graph theory.

8 Translation into Graph Theory

Denote the n-cube by γ_n. Suppose n is divisible by 4 (which will be assumed for the rest of the paper), and define δ_n as follows:

$$V(\delta_n) = \{\alpha \in \mathbb{Z}_2^n : o(\alpha) = n/2\},$$

and

$$E(\delta_n) = \{(\alpha, \beta) \in (\mathbb{Z}_2^n)^2 : d(\alpha, \beta) = n/2\}.$$

Since our vertex set is taken from $\mathbb{Z}_2^n$, we will often wish to think of the distance between two vertices s, t as their Hamming distance in $\mathbb{Z}_2^n$, which we will denote by $d(s, t)$; we will denote their distance as vertices in δ_n by $\mathrm{dist}(s, t)$.

It is clear that $|V(\delta_n)| = \binom{n}{n/2}$; this graph also has some other nice properties. For instance, given $x \in \delta_n$, we have that

$$N(x) = \{y \in \delta_n : d(x, y) = n/2\}.$$

Therefore, any $y \in N(x)$ must be obtained by replacing $n/4$ 1s in x by 0s and $n/4$ 0s in x by 1s (else $o(y) \neq n/2$). Since it is evident that any such set of substitutions yields a neighbor of x, we see that

$$|N(x)| = \binom{n/2}{n/4}^2,$$

so δ_n is $\binom{n/2}{n/4}^2$-regular and

$$|E(\delta_n)| = \frac{\binom{n}{n/2}\binom{n/2}{n/4}^2}{2}.$$

For an ordered pair (v, v') of adjacent vertices, define $(v, v')_{11} \in \mathbb{Z}_+^{n/4}$ to be the set of all indices i for which $v_i = v'_i = 1$. Define $(v, v')_{10}$ to be the set of all indices i for which $v_i = 1$ and $v'_i = 0$. Define $(v, v')_{01}$ (resp. $(v, v')_{00}$) to be the set of all indices i for which $v_i = 0$ and $v'_i = 1$ (resp. $v'_i = 0$). Call these sets *regions*; call $(v, v')_i$ *region* i of (v, v'). We will make use of an analogous definition for single vertices (w), with $(w)_1 \in \mathbb{Z}_+^{n/2}$ denoting the set of indices at which w contains a 1, and $(w)_0$ denoting the set of indices at which w contains a 0.

If (x, x') and (y, y') are two pairs of adjacent vertices in δ_n, then there is an automorphism $\varphi \in S_n$ of δ_n with $\varphi(x) = y$ and $\varphi(x') = y'$ defined by $\varphi((x, x')_i) = (y, y')_i$. Since there are $(n/4)!$ ways to fix each of four regions, there are $[(n/4)!]^4$ such automorphisms, each a member of S_n acting on the indices of the elements of the vertex set. These are trivially seen to be bijections, and they clearly preserve distance between vertices, both as elements of $\mathbb{F}_2^n$ and as vertices of δ_n. This means that, without loss of generality, we may take as our representatives $\alpha = 1^{(n/2)}0^{(n/2)}$ and $\beta = 1^{(n/4)}0^{(n/4)}1^{(n/4)}0^{(n/4)}$ whenever we wish to consider two adjacent vertices, as we do now. In fact, we may extend this result to show that there is an isomorphism of δ_n sending any set of k adjacent vertices to any other set of k adjacent vertices, where 2^k is the highest power of 2 dividing n. However, this result is largely uninteresting, as the existence of an Hadamard matrix of order m immediately implies the existence of an Hadamard matrix of order $2m$; therefore, we focus on orders $n = 4q$, q odd.

Let ζ_n denote the subgraph of δ_n induced by $N(\alpha) \cap N(\beta)$. Since α and β are isomorphic to any two adjacent vertices of δ_n, we see that ζ_n depends only upon n, and not upon our choice of vertices (here, α and β). ζ_n has few of the nice properties inherent in γ_n and δ_n, but we will endeavor to uncover some structure.

First, let us classify the vertices in ζ_n. Any neighbor x of α and β in δ_n must satisfy $d(x, \alpha) = d(x, \beta) = n/2$. Thus, x must share $n/4$ 1s with α and $n/4$ with β. Therefore,

$$|(x)_1 \cap ((\alpha, \beta)_{11} \cup (\alpha, \beta)_{10})| = n/4$$

and

$$|(x)_1 \cap ((\alpha, \beta)_{11} \cup (\alpha, \beta)_{01})| = n/4.$$

That is, x must have $n/4$ 1s total in regions 11 and 10, and $n/4$ 1s total in regions 11 and 01. So suppose x has k 1s in region 11. Then x must have $n/4 - k$ in each of regions 10 and 01, and k 1s (those that remain) in region 00. For k fixed, there are exactly

$$\binom{n/4}{k}^4$$

shared neighbors of α and β, since the positions of the 1s within each of the four regions are arbitrary. Thus,

$$|V(\zeta_n)| = \sum_{i=0}^{n/4} \binom{n/4}{i}^4.$$

We now apply Proposition 7.2 to ζ_n:

Proposition 8.1. *There exists an Hadamard matrix of order n (n divisible by 4) if and only if ζ_n contains an $(n-4)$-clique.*

Proof. If there exists an Hadamard matrix H of order n, then there exists a normalized Hadamard matrix H' of order n; there exists some permutation of the columns of H' yielding a matrix H^* such that the first row of H^* is $\alpha = 1^{(n/2)}0^{(n/2)}$ and the second row of H^* is $\beta = 1^{(n/4)}0^{(n/4)}1^{(n/4)}0^{(n/4)}$. The remaining nonzero rows of H^* then give an $(n-3)$-clique of ζ_n.

Given an $(n-4)$-clique of ζ_n, take the members of the clique to be the rows of an $(n-4) \times n$ matrix M. If we add rows α and β to M, yielding an $(n-2) \times n$ matrix M', Proposition 7.2 gives us that the sum of the rows of M' gives another row $B \in \mathbb{Z}_2^n$ whose distance in $\mathbb{Z}_2^n$ from the existing rows is $n/2$ and whose distance from 0^n is $n/2$. Adding rows B and 0^n to M' gives a matrix M^*, which is an Hadamard matrix by Proposition 2.5. □

Corollary 8.2. *ζ_n contains an $(n-4)$-clique if and only if it contains an $(n-3)$-clique.*

Proof. This follows directly from the proof of Proposition 8.1. □

9 Conclusion

The search for a proof of the Hadamard conjecture has spurred many recent advancements in the fields of design theory and combinatorics. We have outlined several of the more prominent theorems associated with the conjecture, though a complete listing of these accomplishments would be impossible. We have also given the current state of the theorem and used known results to partially re-establish this bound. Finally, we have given a purely combinatorial proof of a basic property of Hadamard matrices, and briefly examined its implications in graph-theoretic terms.

10 Acknowledgements

I would like to thank Mark Shimozono for his guidance and suggestions, as well as my thesis committee (Mark Shimozono, Gail Letzter, and Daniel Farkas) for their careful consideration of my work.

References

[1] E. F. Assmus Jr. and J. D. Key, *Designs and Their Codes*. Cambridge University Press, Cambridge, Great Britain, 1992.

[2] L. D. Baumert, S. W. Golomb, M. Hall Jr., "Discovery of an Hadamard Matrix of Order 92." *Bull. Amer. Math. Soc.*, vol. 68, pp. 237-238, 1962.

[3] L. D. Baumert and M. Hall, Jr., "A New Construction for Hadamard Matrices." *Bull. Amer. Math. Soc.*, vol. 71, pp. 169-170, 1965.

[4] L. D. Baumert, "Hadamard Matrices of Orders 116 and 232." *Bull. Amer. Math. Soc.*, vol. 72, pp. 237, 1966.

[5] Bollobás, Béla. *Modern Graph Theory*. Springer-Verlag New York, Inc., New York, NY, 1998.

[6] Anthony Bonato, W. H. Holzmann, Hadi Kharaghani, "Hadamard Matrices and Strongly Regular Graphs with the 3-e.c. Adjacency Property." *The Electronic Journal of Combinatorics*, vol. 8, r1, 2001.

[7] S. Georgiou, C. Koukouvinos, Jennifer Seberry, "Hadamard Matrices, Orthogonal Designs and Construction Algorithms." http://citeseer.ist.psu.edu/467688.html

[8] Anthony V. Geramita, Jennifer Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, chapters 4,7. Marcel Dekker, Inc., New York, NY, 1979.

[9] M. Hall, Jr., *Combinatorial Theory*. New York: Wiley, second edition, 1986.

[10] Masahiko Miyamoto, "A Construction of Hadamard Matrices." *Journal of Comb. Theory*, Series A, vol. 57, pp. 86-108, 1991.

[11] Raymond E.A.C. Paley, "On Orthogonal Matrices." *Journal of Mathematics and Physics*, vol. 12, pp. 311-320, 1933.

[12] Sloane, N. J. A. Sequence A007299, "The On-Line Encyclopedia of Integer Sequences." http://www.research.att.com/∼njas/sequences/

[13] Douglas R. Stinson, *Combinatorial Designs: Constructions and Analysis*, chapters 1 and 4. Springer-Verlag New York, Inc., New York, NY, 2004.

[14] J. J. Sylvester, "Thoughts on Orthogonal Matrices, Simultaneous Sign-Successions, and Tessellated Pavements in Two or More Colours, with Applications to Newton's Rule, Ornamental Tile-Work, and the Theory of Numbers." *Phil. Mag.* 34, pp. 461-475, 1867.

[15] J. Williamson, "Hadamard's Determinant Theorem and the Sum of Four Squares." *Duke Math. J.*, vol. 11, pp. 65-81, 1944.