18.304 Final Project
Hadamard Matrices

Nicolas Bravo
nbravo@mit.edu

May 2015

1 Abstract

2 Introduction

Definition 2.1. A Hadamard matrix is a square matrix whose entries are either +1 or -1 and whose rows are mutually orthogonal.

3 Construction

There are several ways to construct Hadamard matrices. For example, James Joseph Sylvester proposed the following: Let H be a Hadamard matrix of order n. Then

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

is a Hadamard matrix of order $2n$. This construction could lead to the following sequence of Hadamard matrices: $H_1 = \begin{bmatrix} 1 \end{bmatrix}$, $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & H_{2^{k-1}} \end{bmatrix}$

4 Equality of Hadamard Matrices

From the definition of Hadamard matrices we can see that, given a Hadamard matrix H, we can perform a number of interesting operations on H and still end up with a Hadamard matrix. In particular, we can perform any of the following operations any number of times:

- Interchange any two rows or any two columns
- Multiply any row or any column by -1

- Transpose

and the result will still be Hadamard. If we can transform H into H' through a sequence of the above operations then we say that H and H' are equivalent. The problem of determining whether two Hadamard matrices are equivalent turns out to be very difficult; the interested reader is highly encouraged to look into the topic on his own.

For a given order n there may be only one distinct (i.e. non-equivalent) Hadamard matrix or there may be several. The table below gives the number of distict Hadamard matrices for various orders.

5 Results

Theorem 5.1. *Let A be an $n \times n$ real matrix whose entries satisfy $|a_{ij}| \leq 1$ for all i, j. Then $|det(A)| \leq n^{\frac{n}{2}}$. Equality holds if and only if A is a Hadamard matrix.*

Proof. We'll take a geometric approach to this proof. Let the rows of A be $a_1, a_2, \ldots, a_n$. Then we can interpret $|det(A)|$ as the volume of a parallelipiped with sides $a_1, \ldots, a_n$. Therefore,

$$|det(A)| \leq |a_1||a_2| \ldots |a_n|$$

where equality holds only if and only if all sides (rows of A are perpendicular). We also know that

$$\begin{aligned} |a_i| &= \left(\sum_{j=1}^{n} a_{ij}^2 \right)^{\frac{1}{2}} \\ &\leq \sqrt{n} \end{aligned}$$

where equality in this case holds if and only if $|x_{ij}| = 1$ for all j. Therefore $|det(A)| = n^{\frac{n}{2}}$ if and only if A is a matrix with entries ± 1 and all rows mutually orthogonal, which makes A a Hadamard matrix. □

Theorem 5.2. *Let H be a Hadamard matrix of order n. Then $HH^T = nI_n$.*

Proof. Since each entry in H is ± 1, we know that the length of each row vector is $\sqrt{n}$. Further, we know from the definition of Hadamard matricecs that each row is orthogonal to each other row, so if we divide H by $\sqrt{n}$ we obtain an orthognal matrix $Q = \frac{1}{\sqrt{n}} H$. We then see that

$$\begin{aligned} QQ^T &= I_n \\ \left(\frac{1}{\sqrt{n}} H \right) \left(\frac{1}{\sqrt{n}} H^T \right) &= I_n \\ HH^T &= nI_n \end{aligned}$$

□

Theorem 5.3. *Let H be a Hadamard matrix of order n. Then $|det(H)| = n^{\frac{n}{2}}$*

Proof.

$$\begin{aligned} HH^T &= nI_n \\ det(H) * det(H^T) &= det(nI_n) \\ det(H)^2 &= n^n \\ |det(H)| &= n^{\frac{n}{2}} \end{aligned}$$

□

Theorem 5.4. *If H is an $n \times n$ Hadamard matrix, then $n = 1$ or $n = 2$ or $n \equiv 0 \mod 4$.*

Proof. We know that Hadamard matrices exist for $n = 1$ and $n = 2$ by construction. We also know that n must be even because the orthogonality of the rows implies that there are exactly as many $+1$ entries as there are -1 entries in each row. All that remains is to show that for $n > 3$, $4|n$.

First, we know that we can negate an entire column in a Hadamard matrix and the result will also be Hadamard. Therefore we can selectively multiply columns in H until the first row consists entirely of 1's. If we look at the next 2 rows of H, in each column there are 4 possibilities for the next two entries in those rows: $++, +-, -+$, or $--$. Let's say that each possibility occurs a, b, c, and d times respectively. If we take advantage of the orthogonality relations on these first three rows we obtain the following set of equations:

$$\begin{aligned} a + b + c + d &= n \\ a + b - c - d &= 0 \\ a - b + c - d &= 0 \\ a - b - c + d &= 0 \end{aligned}$$

If we add all of these equations we obtain $4a = n$, thus proving that n must be a multiple of 4. □

Theorem 5.5. *There exists an $n \times n$ matrix with entries ± 1 whose determinant is greater than $\sqrt{n!}$*

Proof. We begin by considering the root mean square of all 2^{n^2} matrices with ± 1 entries. Then we have

$$D_n = \frac{\sqrt{\sum_A (\det\ A)^2}}{2^{n^2}}$$

and it should be clear that

$$\max_A \det A \geq D_n$$

so our goal is to obtain a bound on D_n.

The idea will be to use the definition of the determinant to write out the sum $\sum_A (\det A)^2$ and interchange the appropriate summations in such a way that the terms simplify nicely.

Recall that we define the determinant of a matrix A as

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma_i}$$

where σ is a permutation of the set $\{1, 2, \ldots, n\}$ and $\text{sign}(\sigma)$ takes a value of ± 1 depending on the permutation σ. We can the write

$$\begin{aligned} D_n^2 &= \frac{1}{2^{n^2}} \sum_A \left(\sum_\pi \text{sign}(\pi) \prod_{i=1}^{n} a_{i,\pi_i} \right)^2 \\ &= \frac{1}{2^{n^2}} \sum_A \sum_\sigma \sum_\tau \text{sign}(\sigma)\text{sign}(\tau) \prod_{i=1}^{n} a_{i,\sigma_i} \prod_{j=1}^{m} a_{j,\tau_j} \end{aligned}$$

In this last expression, the inner two sums compute the square of the determinant for each matrix while the outer sum sums over all matrices. We will exchange the order of summations so that instead, we consider pairs of permutations σ and τ in the outer sum and for each pair we sum over each matrix A in the inner sum. In other words, we rewrite as

$$D_n^2 = \frac{1}{2^{n^2}} \sum_{\sigma,\tau} \text{sign}(\sigma)\text{sign}(\tau) \left(\sum_A \prod_{i=1}^{n} a_{i,\sigma_i} \prod_{j=1}^{m} a_{j,\tau_j} \right)$$

Now we will rewrite the inner sum once more. Specifically, note that since we are considering all matrices A with entries ± 1, summing over all A is equivalent to summing over $\sum_{a_{11}=\pm 1} \sum_{a_{12}=\pm 1} \cdots \sum_{a_{nn}=\pm 1}$

So we rewrite the inner sum as $\sum_{a_{11}=\pm 1} \sum_{a_{12}=\pm 1} \cdots \sum_{a_{nn}=\pm 1} \prod_{i=1}^{n} a_{i,\sigma_i} \prod_{j=1}^{m} a_{j,\tau_j}$.

The most important thing about this sum is that it is 0 when $\sigma \neq \tau$. When $\sigma = \tau$, however, the inner product evaluates to 1 and so we have

$$\sum_{a_{11}=\pm 1} \sum_{a_{12}=\pm 1} \cdots \sum_{a_{nn}=\pm 1} 1 = 2^{n^2}$$

So we can finally rewrite our original expression as

$$\begin{aligned} D_n^2 &= \frac{1}{2^{n^2}} \sum_\sigma 2^{n^2} \\ &= n! \\ D_n &= \sqrt{n!} \end{aligned}$$

And we conclude that $\max_A \det A \geq \sqrt{n!}$ □

6 Hadamard Conjecture

The most important open question in the theory of Hadamard matrices is that of existence. The Hadamard conjecture proposes that a Hadamard matrix of order 4k exists for every positive integer k. The Hadamard conjecture has also been attributed to Paley, although it was considered implicitly by others prior to Paley's work.[2]

A generalization of Sylvester's construction proves that if H_n and H_m are Hadamard matrices of orders n and m respectively, then $H\_n \otimes H\_m$ is a Hadamard matrix of order nm. This result is used to produce Hadamard matrices of higher order once those of smaller orders are known.

Sylvester's 1867 construction yields Hadamard matrices of order 1, 2, 4, 8, 16, 32, etc. Hadamard matrices of orders 12 and 20 were subsequently constructed by Hadamard (in 1893).[3] In 1933, Raymond Paley discovered the Paley construction, which produces a Hadamard matrix of order $q+1$ when q is any prime power that is congruent to 3 modulo 4 and that produces a Hadamard matrix of order $2(q+1)$ when q is a prime power that is congruent to 1 modulo 4.[4] His method uses finite fields.

The smallest order that cannot be constructed by a combination of Sylvester's and Paley's methods is 92. A Hadamard matrix of this order was found using a computer by Baumert, Golomb, and Hall in 1962 at JPL.[5] They used a construction, due to Williamson,[6] that has yielded many additional orders. Many other methods for constructing Hadamard matrices are now known.

In 2005, Hadi Kharaghani and Behruz Tayfeh-Rezaie published their construction of a Hadamard matrix of order 428.[7] As a result, the smallest order for which no Hadamard matrix is presently known is 668.

As of 2008, there are 13 multiples of 4 less than or equal to 2000 for which no Hadamard matrix of that order is known.[8] They are: 668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, and 1964.

7 Conclusion