A PROOF THAT NO CIRCULANT HADAMARD MATRIX HAS SIZE $2^k \times 2^k$ WHEN $k \geq 3$

AASHIR MEHROTRA

Abstract. In this paper, we prove that every circulant Hadamard matrix cannot have size greater than 8, given that the size must be a power of 2. We first give a brief overview of the study of Hadamard matrices. Next, we define circulant matrices, and proceed to give a proof to our claim using algebraic number theory and Galois theory. Specifically, we first prove a lemma that the every Hadamard matrix has size 1, 2, or a multiple of 4, and then create a contradiction that $2^{k2^{k-1}}$ can be factorised using the eigenvalues of the circulant Hadamard matrices.

1. Definitions

We first by the definition of a Hadamard martix.

Definition 1.1. An $n \times n$ matrix A is said to be **Hadamard** if it has orthogonal columns and contains only 1s and -1s.

Note that when we consider orthogonality, we mean in a field of characteristic 0.
As an example: here is a 4×4 Hadamard matrix:

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

The dot product of two distinct columns will always give zero in the above matrix, and is hence Hadamard.
An analogous way of defining Hadamard matrices is by replacing the orthogonality condition with the fact that $A^T A = nI$, where I is the identity matrix. This second fomulation implies that

$$\det A = \pm n^{n/2}$$

I claim that every Hadamard matrix also has orthogonal rows. Let $H' = n^{-1/2}H$ if H is a Hadamard matrix. Then H' has orthonormal columns, which means it's in O_n and hence has orthogonal rows. Hence H, which is a scalar multiple of H', also has orthogonal rows.
It is clear that a permutation of rows or columns of a Hadmard matrix is Hadamard. Also, multiplying any row or column with -1 gives us a Hadamard matrix, as scalar multiplication preserves orthogonality, and since $|-1| = 1$, the norm is also preserved.

Definition 1.2. A Hadamard matrix is said to be **normalized** if it's first row and column consists of all +1s. From the previous paragraph, it is clear that a Hadamard matrix

We now prove a standard fact regarding the size of a Hadamard matrix:

Date: March 11, 2023.

Theorem 1.3. *If H is a Hadamard matrix of size $n \times n$, then $n = 1, 2$ or $4k$ for some $k \in \mathbb{N}$*

Proof. We have $\begin{pmatrix}1\end{pmatrix}$ as a 1×1 Hadamard matrix, and $\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}$ as a 2×2 Hadamard matrix. Now suppose $n \geq 3$. Normalize H and rearrnage the second and third rows in the following way:
$\begin{pmatrix}W & X & Y & Z\end{pmatrix}$,
where W is a $2 \times w$ matrix with all 1s, X is a $2 \times x$ matrix with first row all 1s and second row all -1s, Y is a $2 \times y$ with first row all -1s and second row all 1s, and Z is a $2 \times z$ matrix with all -1s.
We must have $w + x + y + z = n$, and taking the inner product of the rows 1 and 2, 1 and 3, and 2 and 3 gives:

$$\begin{cases} w + x - y - z = 0 \\ w - x + y - z = 0 \\ w - x - y + z = 0 \end{cases}.$$

This system of four linear equations gives the unique solution $w = x = y = z = \frac{n}{4}$, which implies n is a multiple of 4. ∎

The main problem in the study of Hadamard matrices is to prove the converse, that a $4k \times 4k$ Hadamard matrix exists for every k.
We now define circulant matrices.

Definition 1.4. A matrix M is called **circulant** if there exists $a_0, \ldots, a_{n-1}$ with $b_{ij} = a_{i-j}$ where the $i - j$ is taken modulo n.

In simpler terms, every row is a cyclic right shift of the row above it.
For example, the following matrix is circulant (it is also Hadamard):

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

It is an open problem to show the following:

Conjecture 1.5. *A circulant Hadamard matrix only exists for $n = 1$ and 4.*

2. Proof of Main Result

In this paper, we prove that there doesn't exists a circulant Hadamard matrix for all powers of 2 except 1 and 4.
For $n = 2$, a circulant matrix must be of the form

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix}.$$

No combination of x and y being ± 1 will give non-zero determinant, which obviously means the columns cannot be orthogonal.
Let $n = 2^k$ with $k \geq 3$, and $\zeta = e^{\frac{2\pi i}{2^k}}$. Then ζ is a root of the polynomial $p_k(x) = x^{2^{k-1}} + 1$. Let $\mathbb{Z}[\zeta]$ be the smallest subring of $\mathbb{C}$ containing both $\mathbb{Z}$ and ζ. Also, let $\mathbb{Q}(\zeta)$ equal the quotient filed of $\mathbb{Z}[\zeta]$.

Lemma 2.1. *The polynomial $p_k(x)$ is irreducible over $\mathbb{Q}$.*

Proof. Note that it is equivalent to prove this result of $p_k(x+1)$. We use Einstein's criterion; we have
$p_k(x+1) = (x+1)^{2^{k-1}} + 1 = x^{2^{k-1}} + [\sum_{i=1}^{2^{k-1}-1} \binom{2^{k-1}}{i} x^i] + 2$.
If we take $p = 2$, then all coefficients except the leading one are even, and the constant term isn't divisble by 2^2.
Hence the polynomial is irreducible. ■

From this lemma, it follows that every $u \in \mathbb{Z}[\zeta]$ can be uniquely written as

$$u = b_0 + b_1\zeta + b_2\zeta^2 + \ldots + b_{\frac{n}{2}-1}\zeta^{\frac{n}{2}-1}$$

For $b_i \in \mathbb{Z}$
We may write $\det H$ as:

$$\prod_{j=0}^{n-1}(a_0 + \zeta^j a_1 + \zeta^{2j} a_2 + \ldots + \zeta^{(n-1)j} a_{n-1}) = \pm n^{n/2} = \pm 2^{k2^{k-1}} \tag{2.1}$$

Note that $a_i = \pm 1$ since H is Hadamard. So we have a factorisation of $2^{k2^{k-1}}$ in $\mathbb{Z}[\zeta]$ with the form above.
Denote the eigenvalues of H as

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

Lemma 2.2. *We have $|\gamma_j| = \sqrt{n}$ for every $0 \leq j \leq n-1$.*

Proof. Recall $H' = n^{-1/2}H$. This is a real orthogonal matrix, which means it has eigenvalues with absolute value 1, which implies all eigenvalues of H have absolute value $\sqrt{n}$. ■

Lemma 2.3. *$2 = (1-\zeta)^{n/2}u = (1-\zeta)^{2^{k-1}}u$, where $u \in \mathbb{Z}[\zeta]$ is a unit.*

Proof. We have $x^{n/2} + 1 = \prod_{j=0|j=2k+1}^{n-1}(x - \zeta^j)$
$\implies 2 = \prod_{j=0|j=2k+1}^{n-1}(1-\zeta^j)$. If we show that
Since $1 - \zeta^j = (1-\zeta)(1 + \zeta + \ldots + \zeta^{j-1})$, and we have $\frac{n}{2}$ such j, it suffices to show that $(1 + \zeta + \ldots + \zeta^{j-1})$ is a unit when j is odd.
Let $\bar{j}$ be the inverse of j modulo n.
We have $(1 + \zeta + \ldots + \zeta^{j-1})^{-2} = \frac{1-\zeta}{1-\zeta^j} = \frac{1-(\zeta^j)^{\bar{j}}}{1-\zeta^j}$
$= (1 + \zeta^j + \zeta^{2j} + \ldots + \zeta^{(\bar{j}-1)j} \in \mathbb{Z}[\zeta]$, as desired. ■

Lemma 2.4. *We must have $\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{F}_2$.*

Proof. Let $R = \mathbb{Z}[\zeta]/(1-\zeta)$. 2 is not a unit in $\mathbb{Z}[\zeta]$ as $\frac{1}{2}$ is not an algebraic integer. Thus, by the previous lemma, $1-\zeta$ cannot also be a unit, implying $R \neq 0$.
Since ζ is identified with 1 in this quotient ring, we have $\zeta^j = 1$ for all j, and R contains ordinary integers. But since, 2 is not a unit, it must be that $2 = 0$ in R, and that $R = \mathbb{F}_2$ ■

Lemma 2.5. *For all $0 \leq j \leq n-1$, there exists a non-negative integer h_j such that*

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

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

Proof. By Lemma 2.3, 2 is a multiple of $(1-\zeta)^{k2^{(k-1)}}$. By (3.1), we have

$$\prod_{j=0}^{n-1}(a_0 + a_1\zeta^j + a_2\zeta^{2j} + \ldots + a_{n-1}\zeta^{(n-1)j}) = 0 \tag{2.2}$$

in $\mathbb{Z}[\zeta]/(1-\zeta)^{2^{k-1}}$. Since $\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{F}_2$ is an integral domain, there exists some j such that $a_0 + a_1\zeta^j + a_2\zeta^{2j} + \ldots + a_{n-1}\zeta^{(n-1)j}$ is divisible by $1-\zeta$. Divide the LHS of (2.2) and the RHS of (2.1) (which is $\pm 2^{k2^{k-1}}$) by $(1-\zeta)$. We continue to do this until the RHS of (2.1) reaches a unit. Then, each factor (or each eigenvalue of H) has the form $v(1-\zeta)^h$ where v is a unit. ■

Corollary 2.6. *Either* $\frac{\gamma_0}{\gamma_1}$ *or* $\frac{\gamma_1}{\gamma_0}$ *is in* $\mathbb{Z}[\zeta]$

Proof. By the previous lemma, we have $\gamma_j = v_j(1-\zeta)^{h_j}$ for each j If $h_0 \geq h_1$, the $\gamma_0/\gamma_1 \in \mathbb{Z}[\zeta]$. Else, $\gamma_1/\gamma_0 \in \mathbb{Z}[\zeta]$. ■

We know go on a detour in proving Kronecker's theorem , a result in algebraic number theory proved using Galois theory. We first start with the following lemma:

Lemma 2.7. *If* $\theta \in \mathbb{C}$ *is an algebraic number such that it and all of its conjugates have absolute value* 1*, then* θ *is a root of unity.*

Proof. Let $\theta = \theta_1, \theta_2, \ldots, \theta_d$ be the conjugates of θ. Let $f_1(x) = f(x) = \prod_{i=1}^{d}(x-\theta_i)$ be the minimal polynomial for θ.
We now let $f_n = \prod_{i=1}^{d}(x-\theta_i^n)$.
Every polynomial f_n is an integral polynomial. This is because every elementary symmetric polynomial in θ_i^n can be represented as an elementary symmetric polynomial in θ_i, which are integral by definition.
f_n's roots also have absolute value 1. By Vieta's formula, the number of integral polynomials of degree d that have absolute value 1 roots is finite, and hence $\theta^n = \sigma(\theta^m)$ for some natural numbers m and n and for some Galois conjugation σ of f_m. Let t be such that $\sigma^t(\theta^m) = \theta^m$, then $\theta^{n^t} = \theta^m$, or $\theta^{n^t-m} = 1$ (n can be chosen large enough so that $n^t - m$ is guaranteed not to equal 0). ■

Theorem 2.8 (Kronecker)**.** *If* τ *is a root of unity and* $\alpha \in \mathbb{Z}[\tau]$ *with* $|\alpha| = 1$*. Then* α *is a root of unity.*

Proof. Since $\alpha \in \mathbb{Z}[\tau]$, we can conclude that α is an integer. Since the field extension $\mathbb{Q}(\tau)/\mathbb{Q}$ is cyclomatic (due to τ being a root of unity), it implies that the Galois group of the field extension G is abelian.
Let β be a conjugate of α, which means that there exists an automorphism $w \in G$ such that $\beta = w(\alpha)$. Since conjugation is an automorphism in G (as it fixes $\mathbb{Q}$), it commutes with w. Then since $\bar{\alpha}\alpha = 1$, we have
$w(\bar{\alpha}\alpha) = w(1) = 1$
$\implies w(\bar{\alpha})w(\alpha) = 1$
$\implies \bar{w}(\alpha)w(\alpha) = 1$
$\implies \bar{\beta}\beta = 1.$
This implies all conjugates of α have absolute value 1. By using the previous lemma, we must have that α is a root of unity. ■

Lemma 2.9. *If $\tau \in \mathbb{Z}[\zeta]$ is a root of unity, then $\tau = \zeta^r$ for some $r \in \mathbb{Z}$.*

Proof. Suppose not. Then τ must be a 2^mth primitive root of unity for $m > k$, or τ^a is pth root of unity, with p an odd prime and $a \geq 1$. In the former case, we have that

$$[\mathbb{Q}(\tau) : \mathbb{Q}] = \phi(2^m) = 2^{m-1} > 2^{k-1} = \phi(2^k) = [\mathbb{Q}(\zeta) : \mathbb{Q}],$$

which is a contradiction as $\tau \in \mathbb{Z}[\gamma]$. For the latter case, $\tau^a\zeta$ being a primitive pnth root of unity implies

$$[\mathbb{Q}(\tau) : \mathbb{Q}] = \phi(pn) = (p-1)\phi(n) > \phi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}],$$

which is again a contradiction. ■

We now complete the proof of our main result, that there doesn't exist a circulant Hadamard matrix of order 2^k with $k \geq 3$. By Lemma 2.2, we have

$$|\frac{\gamma_0}{\gamma_1}| = |\frac{\gamma_1}{\gamma_0}| = 1$$

. By Corollary 2.6, one of γ_1/γ_0 and γ_0/γ_1 is in $\mathbb{Z}[\zeta]$. This fact along with both of them having absolute value 1 implies that one of them in a root of unity (using Kronecker's theorem). By Lemma 2.9, we get that $\gamma_0 = \zeta^{-r}\gamma_1$ for some integer r. Equating the unique expression of γ_0 and $\zeta^{-r}\gamma_1$ we get

$$\gamma_0 = a_0 + a_1 + \ldots = \pm\sqrt{n}$$

(since γ_0 is real), and

$$\zeta^{-r}\gamma_1 = \zeta^{-r}((a_0 - a_{n/2}) + (a_1 - a_{n/2+1}\zeta + \ldots) = (a_r - a_{n/2+r}) + (a_{r+1} - a_{n/2+r+1})\zeta + \ldots$$

(note that addition in the subscript is modulo n). Equating the constant coefficients, we get that $a_r - a_{n/2+r} = \pm\sqrt{n}$. Since $|a_j| = 1$ for all j, we must have $n \geq 4$, which completes the proof.