Circulant Hadamard Matrices

R. Stanley

An $n \times n$ matrix H is a *Hadamard matrix* if its entries are ± 1 and its rows are orthogonal. Equivalently, its entries are ± 1 and $HH^t = nI$. In particular,

$$\det H = \pm n^{n/2}. \tag{1}$$

It is easy to see that if H is an $n \times n$ Hadamard matrix then $n = 1$, $n = 2$, or $n = 4m$ for some integer m. It is conjectured that the converse is true, i.e., for every such n there exists an $n \times n$ Hadamard matrix.

An $n \times n$ matrix $A = (b_{ij})$ is a *circulant* if it has the form $b_{ij} = a_{i-j}$ for some $a_0, a_1, \ldots, a_{n-1}$, where the subscript $i - j$ is taken modulo n. For instance,

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

is a circulant. Let $A = (a_{i-j})$ be an $n \times n$ circulant, and let $\zeta = e^{2\pi i/n}$, a primitive nth root of unity. It is straightforward to compute that for $0 \leq j < n$ the column vector $[1, \zeta^j, \zeta^{2j}, \ldots, \zeta^{(n-1)j}]^t$ is an eigenvector of A with eigenvalue $a_0 + \zeta^j a_1 + \zeta^{2j} a_2 + \cdots + \zeta^{(n-1)j} a_{n-1}$. Hence

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

NOTE. The determinant of a circulant matrix is an example of a *group determinant*, where the group is the cyclic group of order n. In 1880 Dedekind suggested generalizing the case of circulants (and more generally group determinants for abelian groups) to arbitrary groups. It was this suggestion that led Frobenius to the creation group of representation theory. See [1] and the references therein.

Note that the matrix

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

is both a Hadamard matrix and a circulant.

Conjecture (source?). Let H be an $n \times n$ circulant Hadamard matrix. Then $n = 1$ or $n = 4$.

The main work on this conjecture is due to Richard Turyn [2]. He showed that there does not exist a circulant Hadamard matrix of order $8m$, and he also excluded certain other orders of the form $4(2m + 1)$. Turyn's proofs use the machinery of algebraic number theory. Here we will give a proof for the special case $n = 2^k$, $k \geq 3$, where the algebraic number theory can be "dumbed down" to elementary commutative algebra and field theory. It would be interesting to find similar proofs for other values of n.

Theorem 1. *There does not exist a circulant Hadamard matrix H of order 2^k, $k \geq 3$.*

From now on we assume $n = 2^k$ and $\zeta = e^{2\pi i/2^k}$. Clearly ζ is a zero of the polynomial $p_k(x) = x^{2^{k-1}} + 1$. We will be working in the ring $\mathbb{Z}[\zeta]$, the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and ζ. Write $\mathbb{Q}(\zeta)$ for the quotient field of $\mathbb{Z}[\zeta]$, i.e., the field obtained by adjoining ζ to $\mathbb{Q}$.

Lemma 2. *The polynomial $p_k(x)$ is irreducible over $\mathbb{Q}$.*

Proof. If $p_k(x)$ is reducible then so is $p_k(x+1)$. Recall that by Gauss' lemma, an integral polynomial that factors over $\mathbb{Q}$ also factors over $\mathbb{Z}$. If $p(x), q(x) \in \mathbb{Z}[x]$, write $p(x) \equiv q(x) \pmod 2$ to mean that the coefficients of $p(x) - q(x)$ are even. Now

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

Hence any factorization of $p_k(x+1)$ over $\mathbb{Z}$ into two factors of degree at least one has the form $p_k(x+1) = (x^r + 2a)(x^s + 2b)$, where $r + s = 2^{k-1}$ and a, b

are polynomial of degrees less than r and s, respectively. Hence the constant term of $p_k(x+1)$ is divisible by 4, a contradiction. $\square$

It follows by elementary field theory that every element $u \in \mathbb{Z}[\zeta]$ can be uniquely written in the form

$$u = b_0 + b_1\zeta + b_2\zeta^2 + \cdots + b_{n/2-1}\zeta^{n/2-1}, \quad b_i \in \mathbb{Z}.$$

The basis for our proof of Theorem 1 is the two different ways to compute $\det H$ given by equations (1) and (2), yielding the formula

$$\prod_{j=0}^{n-1}(a_0 + \zeta^j a_1 + \zeta^{2j}a_2 + \cdots + \zeta^{(n-1)j}a_{n-1}) = \pm n^{n/2} = \pm 2^{2^{k-1}}. \tag{3}$$

Thus we have a factorization in $\mathbb{Z}[\zeta]$ of $2^{2^{k-1}}$. Algebraic number theory is concerned with factorization of algebraic integers (and ideals) in algebraic number fields, so we have a vast amount of machinery available to show that no factorization (3) is possible (under the assumption that each $a_j = \pm 1$). Compare Kummer's famous approach toward Fermat's Last Theorem (which led to his creation of algebraic number theory), in which he considered the equation $x^n + y^n = z^n$ as $\prod_{\tau^n=1}(x + \tau y) = z^n$.

We are continuing to assume that $H = (a_{j-i})$ is an $n \times n$ circulant Hadamard matrix. We will denote the eigenvalues of H by

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

Lemma 3. *For $0 \le j \le n-1$ we have*

$$|\gamma_j| = \sqrt{n}.$$

Thus all the factors appearing on the left-hand side of (3) have absolute value $\sqrt{n}$.

First proof (naive). Let H_i denote the ith row of H, and let $\cdot$ denote the usual dot product. Then

$$\begin{aligned} \gamma_j\bar{\gamma}_j &= (a_0 + a_1\zeta^j + \cdots + a_{n-1}\zeta^{(n-1)j})(a_0 + a_1\zeta^{-j} + \cdots + a_{n-1}\zeta^{-(n-1)j}) \\ &= H_1 \cdot H_1 + (H_1 \cdot H_2)\zeta^j + (H_2 \cdot H_3)\zeta^{2j} + \cdots + (H_1 \cdot H_n)\zeta^{(n-1)j}. \end{aligned}$$

By the Hadamard property we have $H_1 \cdot H_1 = n$, while $H_1 \cdot H_k = 0$ for $2 \le k \le n$, and the proof follows. □

Second proof (algebraic). The matrix $\frac{1}{\sqrt{n}}H$ is a real orthogonal matrix. By linear algebra, all its eigenvalues have absolute value 1. Hence all eigenvalues γ_j of H have absolute value $\sqrt{n}$. □

Lemma 4. *We have*

$$2 = (1-\zeta)^{n/2}u, \tag{4}$$

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

Proof. Put $x = 1$ in

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

to get $2 = \prod_j (1-\zeta^j)$. Since

$$1 - \zeta^j = (1-\zeta)(1 + \zeta + \cdots + \zeta^{j-1}),$$

it suffices to show that $1 + \zeta + \cdots + \zeta^{j-1}$ is a unit when j is odd. Let $j\bar{j} \equiv 1 \pmod{n}$. Then

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

as desired. □

Lemma 5. *We have $\mathbb{Z}[\zeta]/(1-\zeta) \cong \mathbb{F}_2$.*

Proof. Let $R = \mathbb{Z}[\zeta]/(1-\zeta)$. The integer 2 is not a unit in $\mathbb{Z}[\zeta]$, e.g., because $1/2$ is not an algebraic integer. Thus by Lemma 4, $1-\zeta$ is also not a unit. Hence $R \neq 0$.

For all j we have $\zeta^j = 1$ in R since $\zeta^j - 1 = (\zeta - 1)(\zeta^{j-1} + \cdots + 1)$. Hence all elements of R can be written as ordinary integers m. But $0 = 2$ in R by Lemma 4, so the only elements of R are 0 and 1. □

Lemma 6. *For all $0 \le j \le n-1$ there is an integer $h_j \ge 0$ 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. Since 2 is a multiple of $1-\zeta$ by Lemma 4, we have by (3) that

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

in $\mathbb{Z}[\zeta]/(1-\zeta)$. Since $\mathbb{Z}[\zeta]/(1-\zeta)$ is a domain by Lemma 6, some factor $a_0 + a_1\zeta^j + \cdots + a_{n-1}\zeta^{(n-1)j}$ is divisible by $1-\zeta$. Divide this factor and the right-hand side of (4) by $1-\zeta$, and iterate the procedure. We continue to divide a factor of the left-hand side and the right-hand side by $1-\zeta$ until the right-hand side becomes the unit u. Hence each factor of the original product has the form $v(1-\zeta)^h$, where v is a unit. □

Corollary 7. *Either $\gamma_0/\gamma_1 \in \mathbb{Z}[\zeta]$ or $\gamma_1/\gamma_0 \in \mathbb{Z}[\zeta]$. (In fact, both $\gamma_0/\gamma_1 \in \mathbb{Z}[\zeta]$ and $\gamma_1/\gamma_0 \in \mathbb{Z}[\zeta]$, as will soon become apparent, but we don't need this fact here.)*

Proof. By the previous lemma, each γ_j has the form $v_j(1-\zeta)^{h_j}$. If $h_0 \ge h_1$ then $\gamma_0/\gamma_1 \in \mathbb{Z}[\zeta]$; otherwise $\gamma_1/\gamma_0 \in \mathbb{Z}[\zeta]$. □

We now need to appeal to a result of Kronecker on elements of $\mathbb{Z}[\zeta]$ of absolute value one. For completeness we include a proof of this result, beginning with a lemma.

Lemma 8. *Let θ be an algebraic integer such that θ and all its conjugates have absolute value one. Then θ is a root of unity.*

Proof. Suppose the contrary. Let $\deg(\theta) = d$, i.e., $[\mathbb{Q}(\theta) : \mathbb{Q}] = d$. Now θ, θ^2, $\theta^3, \ldots$ are all distinct and hence infinitely many of them have the property that no two are conjugate. Each $\theta^j \in \mathbb{Q}[\theta]$ and so is the root of a monic integral polynomial of degree at most d. If $\theta_1, \theta_2, \ldots, \theta_d$ are the conjugates of θ, then all the conjugates of θ^j are among θ_1^j, $\theta_2^j, \ldots, \theta_d^j$. Hence each θ^j

satisfies the hypothesis that all its conjugates have absolute value 1 (and θ^j is an algebraic integer). Thus the rth elementary symmetric function e_r in θ^j and its conjugates has at most $\binom{d}{r}$ terms, each of absolute value 1, so $|e_r| \leq \binom{d}{r}$. Moreover, $e_r \in \mathbb{Z}$ since θ^j is an algebraic integer. It follows that there are only finitely many possible polynomials that can be the irreducible monic polynomials with roots one of the θ^j's, contradicting the fact that there are infinitely many θ^j's for which no two are conjugate. □

Theorem 9 (Kronecker)**.** *Let τ be any root of unity and $\alpha \in \mathbb{Q}[\tau]$ with $|\alpha| = 1$. Then α is a root of unity.*

Proof. We use the basic fact from Galois theory that the Galois group of the extension field $\mathbb{Q}(\tau)/\mathbb{Q}$ is abelian. Let β be a conjugate of α, so $\beta = w(\alpha)$ for some automorphism w of $\mathbb{Q}(\tau)$. Apply w to the equation $\alpha\bar{\alpha} = 1$. Since complex conjugation is an automorphism of $\mathbb{Q}(\tau)$ it commutes with w, so we obtain $\beta\bar{\beta} = 1$. Hence all the conjugates of α have absolute value one, so α is a root of unity by the previous lemma. □

We now have all the ingredients to complete the proof of Theorem 1. Note that we have yet to use the hypothesis that $a_i = \pm 1$. By Lemma 3 we have

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

Hence by Corollary 7 and Theorem 9 we have $\gamma_0 = \zeta^{-r}\gamma_1$ for some r. Expand γ_0 and $\zeta^{-r}\gamma_1$ uniquely as integer linear combinations of $1, \zeta, \zeta^2, \ldots, \zeta^{\frac{n}{2}-1}$:

$$\begin{aligned} \gamma_0 &= a_0 + a_1 + \cdots + a_{n-1} = \pm n/2 \\ \zeta^{-r}\gamma_1 &= \zeta^{-r}((a_0 - a_{n/2}) + (a_1 - a_{n/2+1})\zeta + \cdots) \\ &= (a_r - a_{n/2+r}) + (a_{r+1} - a_{n/2+r+1})\zeta + \cdots . \end{aligned}$$

Equating coefficients of ζ^0 yields $\pm n/2 = a_r - a_{n/2+r}$. Since each $a_i = \pm 1$, we must have $n \leq 4$, completing the proof. □

References

[1] T. Y. Lam, Representations of finite groups: A hundred years, Part I, *Notices Amer. Math. Soc.* **45** (1998), 361–372; `www.ams.org/notices/199803/lam.pdf`.

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