Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 41, pp. 480-483, September 2025.

THE SMITH NORMAL FORM OF HADAMARD MATRICES FROM PALEY'S SECOND CONSTRUCTION*

PETER SIN†

Abstract. The Smith normal forms of the Hadamard matrices arising from Paley's second construction are computed and found to be of the standard type.

Key words. Hadamard matrix, Paley construction, Smith normal form.

AMS subject classification. 05B20.

1. Introduction.

A Hadamard matrix of order n is an $n \times n$ matrix H whose entries are either $+1$ or -1 and whose rows are mutually orthogonal. The last condition can be expressed by the equation $HH^T = nI$. It is well known that the only possible values for the order n are 1, 2, and multiples of 4. We shall assume that $n = 4m$ is a multiple of 4. The famous, unsolved Hadamard Conjecture asserts the existence of Hadamard matrices of order equal to any multiple of 4. Starting from the equation above, and standard properties of the invariant factors s_i, $i = 1,\ldots, n$ of H, an easy and well-known argument (cf. [5, p.127]) shows that we must have $s_1 = 1$, $s_2 = 2$ and $s_i s_{n-i+1} = n$ for all i. In many cases, such as when m is square-free, it has been shown in [5], and earlier in [7] when m is odd, that $s_2 = \cdots = s_{2m} = 2$, and $s_{2m+1} = \cdots = s_{4m-1} = 2m$. This is called the *standard type* of Smith normal form for a Hadamard matrix. Of course, plenty of examples are known of Hadamard matrices whose Smith normal forms are not of standard type. For example, since the SNF of a Kronecker product of two matrices is equivalent to the Kronecker product of their SNFs, most Sylvester Hadamard matrices and others obtained by Kronecker product will not be of standard type.

Paley gave two constructions of Hadamard matrices in [6], starting from finite fields $\mathbb{F}_q$. For $q \equiv 3 \pmod 4$, the Hadamard matrix given by Paley's first construction is of order $q+1$ and is a *skew Hadamard* matrix, meaning that $H - I$ is skew-symmetric. The Smith normal form of any skew Hadamard matrix has been computed by Michael and Wallis [4] and found to be of standard type. For $q \equiv 1 \pmod 4$, Paley's second construction produces a symmetric Hadamard matrix of order $2(q+1)$. The purpose of this note is to show that its Smith normal form is also of standard type.

2. Statement and proof.

THEOREM 2.1. *The Smith normal form of the Hadamard matrix arising from Paley's second construction starting with $\mathbb{F}_q$, $q \equiv 1 \pmod 4$ is of standard type. Namely, the invariants are $s_1 = 1$, $s_2 = \cdots = s_{q+1} = 2$, $s_{q+2} = \cdots = s_{2q+1} = q+1$, $s_{2(q+1)} = 2(q+1)$.*

Proof. Let q be a power of a prime p with $q \equiv 1 \pmod 4$. The Paley graph on $\mathbb{F}_q$ is the graph with vertex set $\mathbb{F}_q$, with two vertices x and y on an edge if and only if $x - y$ is a nonzero square in $\mathbb{F}_q$. We fix an arbitrary ordering on the set $\mathbb{F}_q$ and let A be the $q \times q$ $(0,1)$-adjacency matrix of the Paley graph

*Received by the editors on June 3, 2025. Accepted for publication on August 25, 2025. Handling Editor: Froilán Dopico. Corresponding Author: Peter Sin.

Funding: Research partially supported by a grant from the Simons Foundation #633214.

†Department of Mathematics, University of Florida, PO Box 118105, Gainesville, FL 32611–8105, USA (sin@ufl.edu).

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 41, pp. 480-483, September 2025.

with respect to this ordering. In [1], the Smith normal form of A was determined, using the fact that the diagonalization of A obtained by conjugating by the character table of $(\mathbb{F}_q, +)$ is an integral equivalence in the sense of Smith normal forms, except that we must work over a local ring of algebraic integers in which q is invertible. As we shall see, when the same trick is applied to the matrices arising from A in Paley's construction, the Hadamard matrix is reduced to a simple form which is not diagonal but, nevertheless, allows one to deduce the Smith normal easily.

The *Jacobsthal matrix* B is the $q \times q$ matrix with rows and columns indexed by $\mathbb{F}_q$ (in the same order), with (x, y) entry equal to $\chi(x - y)$, where χ is the quadratic character. Thus, we have

$$B = A - A^c = 2A - J + I, \tag{2.1}$$

where A^c is the adjacency matrix of the complementary graph and J is the matrix with all entries equal to 1. Let $\mathbf{j}$ be the column vector of length q, all of whose entries are 1. Then

$$C = \left[\begin{array}{c|c} 0 & \mathbf{j}^T \\ \hline \mathbf{j} & B \end{array}\right], \tag{2.2}$$

is called the *conference matrix* obtained by bordering B.

Finally, the Hadamard matrix from Paley's construction is

$$H = \left[\begin{array}{c|c} C + I & C - I \\ \hline C - I & -C - I \end{array}\right]. \tag{2.3}$$

Since the order of H is $2(q + 1)$, it follows that the invariant factors of H are coprime to p, so finding them is equivalent to finding the ℓ-elementary divisors of H for all primes $\ell \neq p$. Let R be the cyclotomic ring $\mathbb{Z}[\xi]$, where ξ is a p-th primitive root of unity. Every rational prime $\ell \neq p$ is unramified in R. (See [2, Theorems 44 and 46].) We denote by $R_{(\ell)}$ the localization of R at the prime ideal ℓR. Then if we view H as a matrix over the PID $R_{(\ell)}$, the multiplicity of ℓ^i as an elementary divisor over $R_{(\ell)}$ is exactly the same as its multiplicity over $\mathbb{Z}$.

Let X be the character table of the additive group $(\mathbb{F}_q, +)$, with columns ordered by our fixed ordering of $\mathbb{F}_q$ and, for the moment, any order of rows. Thus for an additive character ψ of $\mathbb{F}_q$ and an element $x \in \mathbb{F}_q$, the (ψ, x) entry of X is $\psi(x)$. Let $\overline{X}$ be the matrix whose (ψ, x) entry is $\psi(-x)$. Then the character orthogonality relation is $\frac{1}{q} X \overline{X}^t = I$ so $\frac{1}{q} \overline{X}^t = X^{-1}$.

Also we have

$$XAX^{-1} = \frac{1}{q} XA\overline{X}^t = \operatorname{diag}(\psi(S))_\psi, \tag{2.4}$$

where ψ runs over the additive characters of $\mathbb{F}_q$ and $\psi(S) = \sum_{y \in S} \psi(y)$. Thus, the $\psi(S)$ are the eigenvalues of A. (This idea goes back to [3], where it was applied to difference sets.) Now the eigenvalues of A are $\frac{q-1}{2}$ (once), $\alpha := \frac{-1+\sqrt{q}}{2}$ ($\frac{q-1}{2}$ times), and $\beta := \frac{-1-\sqrt{q}}{2}$ ($\frac{q-1}{2}$ times). We may assume that the rows of X are ordered so that

$$\operatorname{diag}(\psi(S))_\psi = \operatorname{diag}\left(\frac{q-1}{2}, \alpha, \ldots, \alpha, \beta, \ldots, \beta\right). \tag{2.5}$$

Here, we also make the observation that the matrices X and $X^{-1} = \frac{1}{q}\overline{X}^t$ have entries in $R_{(\ell)}$, which will be crucial to our proof.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 41, pp. 480-483, September 2025.

Next consider the Jacobsthal matrix $B = 2A - J + I$. Now A and J are both diagonalized by X, and a short computation yields

$$XBX^{-1} = \mathrm{diag}(0, \sqrt{q}, \ldots, \sqrt{q}, -\sqrt{q}, \ldots, -\sqrt{q}). \tag{2.6}$$

Now consider the conference matrix C (2.2).

We shall conjugate $C + I$ and $C - I$ by the $(q+1) \times (q+1)$ matrix

$$Y = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & X \end{array}\right]. \tag{2.7}$$

Using (2.6), we find that

$$Y(C+I)Y^{-1} = \left[\begin{array}{cc|c} 1 & 1 & 0 \\ q & 1 & 0 \\ \hline 0 & 0 & D_1 \end{array}\right], \tag{2.8}$$

where $D_1 = \mathrm{diag}(1 + \sqrt{q}, \ldots, 1 + \sqrt{q}, 1 - \sqrt{q}, \ldots, 1 - \sqrt{q})$, and

$$Y(C-I)Y^{-1} = \left[\begin{array}{cc|c} -1 & 1 & 0 \\ q & -1 & 0 \\ \hline 0 & 0 & D_2 \end{array}\right], \tag{2.9}$$

where $D_2 = \mathrm{diag}(-1 + \sqrt{q}, \ldots, -1 + \sqrt{q}, -1 - \sqrt{q}, \ldots, -1 - \sqrt{q})$. Next, if we set

$$E = \left[\begin{array}{c|c} Y & 0 \\ \hline 0 & Y \end{array}\right]. \tag{2.10}$$

then from the definition (2.3) of H, (2.8) and (2.9) we obtain

$$EHE^{-1} = \left[\begin{array}{cc|c|cc|c} 1 & 1 & 0 & -1 & 1 & 0 \\ q & 1 & 0 & q & -1 & 0 \\ \hline 0 & 0 & D_1 & 0 & 0 & D_2 \\ \hline -1 & 1 & 0 & -1 & -1 & 0 \\ q & -1 & 0 & -q & -1 & 0 \\ \hline 0 & 0 & D_2 & 0 & 0 & -D_1 \end{array}\right]. \tag{2.11}$$

By permuting rows and columns of the matrix (2.11), we obtain the diagonal block sum of the two matrices

$$\left[\begin{array}{cc|cc} 1 & 1 & -1 & 1 \\ q & 1 & q & -1 \\ \hline -1 & 1 & -1 & -1 \\ q & -1 & -q & -1 \end{array}\right] \quad \text{and} \quad \left[\begin{array}{c|c} D_1 & D_2 \\ \hline D_2 & -D_1 \end{array}\right]. \tag{2.12}$$

By elementary R-integral row and column operations, it is easy to reduce the first matrix in (2.12) to $\mathrm{diag}(1, 2, q+1, 2(q+1))$. By further permuting the rows and columns of the second matrix in (2.12), we can obtain the diagonal block matrix with each of the $(q-1)/2$ blocks on the diagonal identically equal to

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 41, pp. 480-483, September 2025.

$$\left[\begin{array}{cc:cc} -2\alpha & 0 & 2\beta & 0 \\ 0 & -2\beta & 0 & 2\alpha \\ \hdashline 2\beta & 0 & 2\alpha & 0 \\ 0 & 2\alpha & 0 & 2\beta \end{array}\right]. \tag{2.13}$$

By elementary R-integral row and column operations, we can reduce this matrix to $\mathrm{diag}(2, 2, q+1, q+1)$.

As noted earlier, X is an invertible matrix over the PID $R_{(\ell)}$, and it follows that the matrices Y and E are also invertible matrices over $R_{(\ell)}$. The above computations therefore show that H is $R_{(\ell)}$-equivalent to the standard Smith normal form. Thus, the ℓ-elementary divisors of H are the same, counting multiplicites, as those in the standard Smith normal form. Since this holds for any $\ell \neq p$, and since the elementary divisors of H must be prime to p, as they must divide $4(q+1)$, we conclude that the Smith normal form of H is of standard type. □

REFERENCES

[1] D.B. Chandler, P. Sin, and Q. Xiang. The Smith and critical groups of the Paley graphs. *J. Algebr. Comb.*, 41(4):1013–1022, 2015.
[2] A. Frölich and M.J. Taylor. *Algebraic Number Theory*. Cambridge Studies in Advanced Mathematics, vol. 27. Cambridge University Press, Cambridge, 1991.
[3] F.J. MacWilliams and H.B. Mann. On the p-rank of the design matrix of a difference set. *Inform. Control*, 12:474–488, 1968.
[4] T.S. Michael and W.D. Wallis. Skew-Hadamard matrices and the Smith normal form. *Des. Codes Cryptogr.* 13(2):173–176, 1998.
[5] M. Newman. Invariant factors of combinatorial matrices. *Isr. J. Math.* 10:126–130, 1971.
[6] R.E.A.C. Paley. On orthogonal matrices. *J. Math. Phys.*, 12:311–320, 1933.
[7] W.D. Wallis and J. Wallis. Equivalence of Hadamard matrices. *Isr. J. Math.* 7:122–128, 1969.