THREE-DIMENSIONAL HADAMARD MATRICES OF PALEY TYPE

VEDRAN KRČADINAC[1], MARIO OSVIN PAVČEVIĆ[2], AND KRISTIJAN TABAK[3]

[1]*Faculty of Science, University of Zagreb, Bijenička cesta* 30, *HR*-10000 *Zagreb, Croatia*

[2]*Faculty of Electrical Engineering and Computing, University of Zagreb, Unska* 3, *HR*-10000 *Zagreb, Croatia*

[3]*Rochester Institute of Technology, Zagreb Campus, D. T. Gavrana* 15, *HR*-10000 *Zagreb, Croatia*

Abstract. We describe a construction of three-dimensional Hadamard matrices of even order v such that $v-1$ is a prime power. The construction covers infinitely many orders for which the existence was previously open.

1. Introduction

An n-dimensional matrix of order v over the set S is a function $H : \{1,\ldots,v\}^n \to S$. A k-dimensional *layer* of H is a restriction obtained by fixing $n-k$ coordinates. Two layers are *parallel* if the same coordinates are fixed and the values of the fixed coordinates agree, except (possibly) one. An *n-dimensional Hadamard matrix* is an matrix over $\{-1,1\}$ such that all $(n-1)$-dimensional parallel layers are mutually orthogonal, i.e.

$$\sum_{1\leq i_1,\ldots,\widehat{i_j},\ldots,i_n\leq v} H(i_1,\ldots,a,\ldots,i_n)H(i_1,\ldots,b,\ldots,i_n) = v^{n-1}\delta_{ab}$$

E-mail address: `vedran.krcadinac@math.hr, mario.pavcevic@fer.hr, kristijan.tabak@croatia.rit.edu`.

Date: September 12, 2023.

2020 *Mathematics Subject Classification.* 05B20, 15B34.

Key words and phrases. Hadamard matrix; projective special linear group.

This work has been supported by the Croatian Science Foundation under the project 9752.

holds for all $j \in \{1, \ldots, n\}$ and $a, b \in \{1, \ldots, v\}$. *Proper n-dimensional Hadamard matrices* satisfy the stronger condition that all 2-dimensional layers are Hadamard, i.e. $\{-1, 1\}$ matrices with orthogonal rows and columns.

Higher-dimensional Hadamard matrices were introduced by Paul J. Schlichta [7, 8]. These matrices have been extensively studied and have applications in signal processing, error correction coding and cryptography; see [4, 10]. A central question is determining the orders v for which Hadamard matrices exist. By the famous Hadamard conjecture, 2-dimensional matrices exist for all v divisible by 4. The conjecture remains open with the smallest order for which no example is known currently being $v = 668$. By the following theorem of Yang [9], the existence of proper n-dimensional Hadamard matrices is equivalent to the 2-dimensional case.

Theorem 1.1 (Product construction)**.** *If $h = [h_{ij}]$ is a 2-dimensional Hadamard matrix of order v, then*

$$H(i_1, \ldots, i_n) = \prod_{1 \leq j < k \leq n} h_{i_j i_k}$$

is a proper n-dimensional Hadamard matrix of order v.

On the other hand, orders of improper higher-dimensional Hadamard matrices are not necessarily divisible by 4, but only even. The book [10] contains many constructions for Hadamard matrices of orders $v \equiv 2 \pmod 4$ and dimensions $n \geq 4$. A question whether such matrices exist for all even orders is raised [10, Question 12, p. 419]. There are theorems giving higher-dimensional Hadamard matrices from lower-dimensional ones, for example [10, Theorem 6.1.5]:

Theorem 1.2. *If $h : \{1, \ldots, v\}^n \to \{-1, 1\}$ is an n-dimensional Hadamard matrix, then*

$$H(i_1, \ldots, i_n, i_{n+1}) = h(i_1, \ldots, i_{n-1}, i_n + i_{n+1})$$

is an $(n+1)$-dimensional Hadamard matrix of the same order v. The sum in the last coordinate is taken modulo v.

This construction does not preserve propriety, i.e. H needs not be proper even if h is proper. Less is known about Hadamard matrices of dimension 3. A construction based on perfect binary arrays [10, Theorem 3.2.2] gives examples for orders $v = 2 \cdot 3^k$, $k \geq 0$. The existence of 3-dimensional Hadamard matrices of orders $v \equiv 2 \pmod 4$ that are not of this form has been a long-standing open problem [10, Questions 5 and 6, p. 419]. We give an affirmative answer for all even orders v such that $v - 1$ is a prime power.

In the next section we present a construction based on squares in finite fields of odd orders q similar to Paley's construction of 2-dimensional Hadamard matrices [6]. Our three-dimensional matrices are indexed by points of the projective line $PG(1,q)$ and are invariant under the projective special linear group $PSL(2,q)$. The construction covers infinitely many orders for which three-dimensional Hadamard matrices were not known. We conclude the paper in Section 3 by considering the smallest order not covered by our construction that is still open.

2. The construction

Shlichta suggested to generalise known algebraic constructions of Hadamard matrices to higher dimensions [8, Section VI, Problem (a)]. A famous early construction using finite fields is due to Paley [6]. It can be described as follows. Let q be an odd prime power and $\chi : \mathbb{F}_q^* \to \{1,-1\}$ a function that takes the value 1 for non-zero squares in the field $\mathbb{F}_q$ and -1 for non-squares. Note that χ is a homomorphism from the multiplicative group of $\mathbb{F}_q$ to $\{1,-1\}$. The rows and columns of the matrix h are indexed by the projective line $PG(1,q) = \{\infty\} \cup \mathbb{F}_q$ and the elements are

$$h(x,y) = \begin{cases} -1, & \text{if } x = y = \infty, \\ 1, & \text{if } x = y \neq \infty \text{ or } x = \infty \neq y \\ & \text{ or } y = \infty \neq x, \\ \chi(y-x), & \text{otherwise.} \end{cases} \tag{1}$$

If $q \equiv 3 \pmod 4$, this is a Hadamard matrix of order $q+1$ called the *Paley type I* matrix. For $q \equiv 1 \pmod 4$ there is a similar construction of *Paley type II* Hadamard matrices of orders $2(q+1)$.

Hammer and Seberry [3, Example 2] assume $\chi(0) = -1$ and define the n-dimensional *Paley cube* as

$$H(x_1,\ldots,x_n) = \begin{cases} 1, & \text{if } x_i = \infty \text{ for at least one } i, \\ \chi(x_1 + \ldots + x_n), & \text{otherwise.} \end{cases}$$

For $n = 2$ this matrix is equivalent to the Paley type I matrix, but for $n \geq 3$ the $(n-1)$-dimensional layers are not orthogonal and it is not a higher-dimensional Hadamard matrix. Hammer and Seberry call it "almost Hadamard" because the 2-dimensional layers are either Hadamard matrices or matrices of all ones.

We propose an alternative definition for $n = 3$:

$$H(x,y,z) = \begin{cases} -1, & \text{if } x = y = z, \\ 1, & \text{if } x = y \neq z \\ & \text{ or } x = z \neq y \\ & \text{ or } y = z \neq x, \\ \chi(z-y), & \text{if } x = \infty, \\ \chi(x-z), & \text{if } y = \infty, \\ \chi(y-x), & \text{if } z = \infty, \\ \chi((x-y)(y-z)(z-x)), & \text{otherwise.} \end{cases} \tag{2}$$

In the last four rows the coordinates are assumed to be all distinct. We first describe the symmetries of this three-dimensional matrix.

Lemma 2.1. *The matrix* (2) *is invariant under cyclic shifts of the coordinates, i.e.* $H(x,y,z) = H(y,z,x) = H(z,x,y)$.

Proof. Follows directly from the definition. □

Lemma 2.2. *The matrix* (2) *is invariant under linear fractional transformations of the coordinates with determinant* 1*, i.e. under the action of* $PSL(2,q)$ *on the projective line.*

Proof. Let $f : PG(1,q) \to PG(1,q)$ be defined by $f(x) = \frac{ax+b}{cx+d}$ for $a,b,c,d \in \mathbb{F}_q$, $ad - bc = 1$. If the denominator is zero then $f(x) = \infty$, and $f(\infty) = \frac{a}{c}$. We claim that $H(f(x), f(y), f(z)) = H(x,y,z)$ for all $x,y,z \in PG(1,q)$. Since f is a bijection, this clearly holds if $x = y = z$ or two of the coordinates are equal. Assume that the three coordinates are all distinct and ∞ does not appear among x, y, z, $f(x)$, $f(y)$, $f(z)$. Because $ad - bc = 1$, we have $f(x) - f(y) = \frac{x-y}{(cx+d)(cy+d)}$, so $(f(x) - f(y))(f(y) - f(z))(f(z) - f(x)) = \frac{(x-y)(y-z)(z-x)}{(cx+d)^2(cy-d)^2(cz+d)^2}$. The denominator is a square, hence the χ-value of this expression agrees with $\chi((x-y)(y-z)(z-x))$. Similarly one can check that $H(f(x), f(y), f(z)) = H(x,y,z)$ if x, y, z are distinct and ∞ does appear among x, y, z, $f(x)$, $f(y)$, $f(z)$. □

Theorem 2.3. *For every odd prime power* q*, equation* (2) *defines a three-dimensional Hadamard matrix of order* $q+1$*. If* $q \equiv 3 \pmod 4$*, the matrix is proper with all* 2*-dimensional layers equivalent to the Paley type I matrix* (1).

Proof. Because of Lemma 2.1 we may fix the last coordinate. We claim that for all distinct $a, b \in PG(1,q)$,

$$\sum_{x,y \in PG(1,q)} H(x,y,a)H(x,y,b) = 0.$$

Now, because $PSL(2,q)$ acts 2-transitively on $PG(1,q)$ and Lemma 2.2, we may take $a=0$ and $b=\infty$ without loss of generality. We divide the sum into two parts:

$$\sum_x H(x,x,0)H(x,x,\infty) + \sum_{x\neq y} H(x,y,0)H(x,y,\infty).$$

The first part is readily seen to be $q-3$. For the second part we distinguish whether 0, ∞ are among x, y or not. If $x=0$, $y=\infty$ or $x=\infty$, $y=0$ the summand is 1, so up to now the total is $q-1$. If $x\in\mathbb{F}_q^*$, $y=\infty$, the sum is

$$\sum_{x\in\mathbb{F}_q^*} H(x,\infty,0)H(x,\infty,\infty) = \sum_{x\in\mathbb{F}_q^*} \chi(x) = 0$$

because there are equally many squares and non-squares in $\mathbb{F}_q^*$. Similarly we see that the cases $x\in\mathbb{F}_q^*$, $y=0$; $x=\infty$, $y\in\mathbb{F}_q^*$; and $x=0$, $y\in\mathbb{F}_q^*$ sum up to 0. The final part of the sum is over $x,y\in\mathbb{F}_q^*$, $x\neq y$:

$$\sum H(x,y,0)H(x,y,\infty) = \sum \chi((x-y)(y-0)(0-x))\chi(y-x) =$$

$$= \sum \chi(x)\chi(y) = \sum_x \chi(x) \sum_{y\neq x} \chi(y) = \sum_x \chi(x)(-\chi(x)) = 1-q.$$

The grand total is $q-1+1-q=0$ and the first part of the theorem is proved. For the second part notice that thanks to Lemmas 2.1 and 2.2 we may, without loss of generality, fix the third coordinate to $z=\infty$ and look at the 2-dimensional layer obtained by varying x and y. In this case equation (2) reduces to (1), and this is a Paley type I Hadamard matrix if $q\equiv 3 \pmod 4$. □

3. Concluding remarks

Theorem 2.3 proves the existence of three-dimensional Hadamard matrices of orders $v = 10$, 14, 26, 30, 38, 42, and infinitely many other orders that were previously unknown. The construction is implemented in our GAP [2] package *Prescribed Automorphism Groups* [5]. Examples can be easily obtained by typing `Paley3DMat`(v).

The smallest order $v\equiv 2 \pmod 4$ not covered by Theorem 2.3 is $v=22$. A four-dimensional Hadamard matrix of order 22 can be constructed by [10, Theorem 6.1.4] from a 2-dimensional Hadamard matrix of order $22^2=484$. Theorem 1.2 then covers all dimensions $n>4$. As far as we know, the existence of a three-dimensional Hadamard matrix of order 22 is an open problem. We tried constructing examples by prescribing automorphism groups (see [1] for the relevant definitions) but we did not succeed.

References

[1] W. de Launey, R. M. Stafford, *Automorphisms of higher-dimensional Hadamard matrices*, J. Combin. Des. **16** (2008), no. 6, 507–544.

[2] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.12.2, 2022. `https://www.gap-system.org`

[3] J. Hammer, J. R. Seberry, *Higher-dimensional orthogonal designs and applications*, IEEE Trans. Inform. Theory **27** (1981), no. 6, 772–779.

[4] K. J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, 2007.

[5] V. Krčadinac, *PAG – Prescribed Automorphism Groups*, Version 0.2.2, 2023 (GAP package). `https://vkrcadinac.github.io/PAG/`

[6] R. E. A. C. Paley, *On orthogonal matrices*, Journal of Mathematics and Physics **12** (1933), 311–320.

[7] P. J. Shlichta, *Three- and four-dimensional Hadamard matrices*, Bull. Amer. Phys. Soc. **16 (8)** (1971), 825–826.

[8] P. J. Shlichta, *Higher dimensional Hadamard matrices*, IEEE Trans. Inform. Theory **25** (1979), no. 5, 566–572.

[9] Y. X. Yang, *Proofs of some conjectures about higher-dimensional Hadamard matrices* (Chinese), Kexue Tongbao (Chinese) **31** (1986), no. 2, 85–88.

[10] Y. X. Yang, X. X. Niu, C. Q. Xu, *Theory and applications of higher-dimensional Hadamard matrices, Second edition*, Chapman and Hall/CRC Press, 2010.