2010

# On the Construction of Order Six Multilevel Hadamard Matrices

Keli Parker

*Electronic Proceedings of Undergraduate Mathematics Day*
4 2010 No. **5**, 1–5; **http://academic.udayton.edu/EPUMD/**

# ON THE CONSTRUCTION OF ORDER SIX MULTILEVEL HADAMARD MATRICES[1]

**Keli Parker**

Department of Mathematics and Statistics, Wright State University
Dayton, Ohio 45435 USA
e-mail: parker.132@wright.edu

**Abstract**

The existence of multilevel Hadamard matrices (MHMs) of all orders as well as a construction for full-rate circulant MHMs of all orders $n \neq 4$ is known. We use computer search methods to look for previously unknown full-rate circulant MHMs of orders 5, 6, and 7 and find solutions that potentially do not follow from the known construction. We then give an alternate construction to explain some order six MHMs.

**Key words and phrases:** multilevel Hadamard matrices, full-rate circulant matrix.
**AMS (MOS) Subject Classifications**: 05B20

Multilevel Hadamard matrices were first introduced as an extension of the traditional Hadamard matrices first explored by Sylvester in 1867. Traditional Hadamard matrices are defined as square matrices with elements $\pm 1$ whose columns are mutually orthogonal. Such matrices have typically been found useful as a statistical method to filter interference and have applications in code division multiple access systems and error control coding [2]. Multilevel Hadamard matrices were defined by Trinh et al. in 2006 as square matrices whose elements are real and columns are mutually orthogonal. These were explored as a method of deriving multilevel zero correlation zone sequences and potentially have applications similar to traditional Hadamard matrices [3]. In a 2008 paper, Adams et al. introduced additional restrictions to define a circulant full-rate MHM of order $n$ to be constructed with $n$ integers of distinct absolute value where each subsequent row is a single rotation of the one above [1]. It is of note that while multilevel Hadamard matrices of order four do exist, they cannot be constructed in the full-rate circulant manner. Such a full-rate circulant matrix $H$ is then of the form below [1]:

$$H = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & \cdots & \cdots & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{bmatrix}$$

[1]Dr. K. T. Arasu of Wright State University contributed on an advising capacity for this paper.

The definition of a Hadamard matrix then requires the following to be satisfied:

$$HH^T = H^T H = (a_0^2 + a_1^2 + ... + a_{n-1}^2)I_n.$$

The additional restriction to circulant matrices led Adams et al. [1] to recognize that these matrices could equivalently be defined by $\lfloor \frac{n}{2} \rfloor$ constraining equations for orthogonality. Adams used this to create a construction that proves the existence of full-rate circulant MHMs for all orders $n \neq 4$.

The construction assigns values based upon powers of some number $r$ to each element as follows, possibly multiplying all elements by a scalar to ensure integer entries [1].

$$\begin{aligned} a_0 &= r^0 \\ a_1 &= r^1 \\ a_2 &= r^2 \\ &\cdots \\ a_{n-2} &= r^{n-2} \\ a_{n-1} &= -\frac{(r^{n-1} - r)}{r^2 - 1}. \end{aligned} \tag{1}$$

We pose the question does Adam's construction give a complete listing of MHMs. Using the constraining equations for orthogonality we are able to come up with the requirements for orders five (2) six (3) and seven (4), and use these equations to conduct a computer search for solutions.

$$\begin{aligned} a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_0 = 0, \\ a_0a_2 + a_1a_3 + a_2a_4 + a_3a_0 + a_4a_1 = 0, \end{aligned} \tag{2}$$

$$\begin{aligned} a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_0 = 0, \\ a_0a_2 + a_1a_3 + a_2a_4 + a_3a_5 + a_4a_0 + a_5a_1 = 0, \\ a_0a_3 + a_1a_4 + a_2a_5 = 0, \end{aligned} \tag{3}$$

$$\begin{aligned} a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_6 + a_6a_0 = 0, \\ a_0a_2 + a_1a_3 + a_2a_4 + a_3a_5 + a_4a_6 + a_5a_0 + a_6a_1 = 0, \\ a_0a_3 + a_1a_4 + a_2a_5a_3a_6 + a_4a_0 + a_5a_1 + a_6a_2 = 0. \end{aligned} \tag{4}$$

Searches conducted for integers of unique absolute value $a_i \leq 100$ yield results that do not readily follow from Adam's construction (1) for orders $n = 5, 6, 7$. Some examples of these results include:

| $n = 5$ | $n = 6$ | $n = 7$ |
|---|---|---|
| $6, 17, 14, 26, -22$ | $1, 3, 4, 5, 9, -8$ | $-63, 7, 3, 22, 19, 50, 78$ |
| $6, 18, 26, 54, -33$ | $1, 8, 9, 7, 16, -15$ | $-74, 4, 28, 22, 38, 34, 64$ |
| $4, -24, 43, -56, -68$ | $4, 5, 9, 16, 25, -21$ | $-75, 9, 42, 48, 27, 12, 53$ |
| $11, -12, 26, 62, -16$ | $1, 15, 16, 9, 25, -24$ | |

Order six results show a consistent pattern that we are then able to use to formulate a new order six construction using parameters $a$ and $r$:

$$\begin{aligned} a_0 &= a^2 \\ a_1 &= r^2 - a^2 \\ a_2 &= r^2 \\ a_3 &= 2ar + a^2 \\ a_4 &= (a + r)^2 \\ a_5 &= -2ar - r^2 \end{aligned} \tag{5}$$

Proof: Apply (5) to obtain

$$a^2(r^2 - a^2) + (r^2 - a^2)r^2 + r^2(2ar + a^2) + (2ar + a^2)(a + r)^2$$
$$+(a + r)^2(-2ar - r^2) + (-2ar - r^2)a^2 = 0,$$
$$a^2r^2 + (r^2 - a^2)(2ar + a^2) + r^2(a + r)^2 + (2ar + a^2)(-2ar - r^2)$$
$$+(a + r)^2a^2 + (-2ar - r^2)(r^2 - a^2) = 0,$$
$$a^2(2ar + a^2) + (r^2 - a^2)(a + r)^2 + r^2(-2ar - r^2) = 0,$$

for all $a, r$.

To ensure the resulting MHM is full-rate, it is then necessary to point out that each element must eventually be an integer and apply four additional restrictions:

$$|a| \neq |r| \tag{6}$$

$$a, r \in \mathbb{Q}, \tag{7}$$

$$a \neq 0, \quad \textit{and} \quad r \neq 0, \tag{8}$$

$$r \neq -2a, \quad and \quad a \neq -2r. \tag{9}$$

We can then show that every element of the construction will always be of unique absolute value. It is only necessary to require that $a, r$ be rational since we may multiply all elements by a scalar to ensure the construction is of integers. To confirm unique absolute value of the elements, we check thirty equalities:

Suppose:

$$\begin{aligned}
a^2 = r^2 - a^2 &\Longrightarrow \sqrt{2}a = r && \text{contradiction with (7),}\\
a^2 = a^2 - r^2 &\Longrightarrow r^2 = 0 && \text{contradiction with (8),}\\
a^2 = r^2 &\Longrightarrow |a| = |r| && \text{contradiction with (6),}\\
a^2 = -r^2 &\Longrightarrow a = r\imath && \text{contradiction with (7),}\\
a^2 = 2ar + a^2 &\Longrightarrow 2ar = 0 && \text{contradiction with (8),}\\
a^2 = -2ar - a^2 &\Longrightarrow |a| = |r| && \text{contradiction with (6),}\\
a^2 = (a+r)^2 &\Longrightarrow r = -2a && \text{contradiction with (9),}\\
a^2 = -(a+r)^2 &\Longrightarrow r = a(1+\imath) && \text{contradiction with (7),}\\
a^2 = -2ar - r^2 &\Longrightarrow |a| = |r| && \text{contradiction with (6),}\\
a^2 = 2ar + r^2 &\Longrightarrow r = a(\sqrt{2}-1) && \text{contradiction with (7),}\\
r^2 - a^2 = r^2 &\Longrightarrow a = 0 && \text{contradiction with (8),}\\
r^2 - a^2 = -r^2 &\Longrightarrow a = \sqrt{2}r && \text{contradiction with (7),}\\
r^2 - a^2 = 2ar + a^2 &\Longrightarrow r = a(1+\sqrt{3}) && \text{contradiction with (7),}\\
r^2 - a^2 = -2ar - a^2 &\Longrightarrow r = -2a && \text{contradiction with (9),}\\
r^2 - a^2 = (a+r)^2 &\Longrightarrow |a| = |r| && \text{contradiction with (6),}\\
r^2 - a^2 = -(a+r)^2 &\Longrightarrow |r| = |a| && \text{contradiction with (6),}\\
r^2 - a^2 = -2ar - r^2 &\Longrightarrow a = r(1+\sqrt{3}) && \text{contradiction with (7),}\\
r^2 - a^2 = 2ar + r^2 &\Longrightarrow a = -2r && \text{contradiction with (9),}\\
r^2 = 2ar + a^2 &\Longrightarrow r = a(1+\sqrt{2}) && \text{contradiction with (7),}\\
r^2 = -2ar - a^2 &\Longrightarrow |a| = |r| && \text{contradiction with (6),}\\
r^2 = (a+r)^2 &\Longrightarrow a = -2r && \text{contradiction with (9),}\\
r^2 = -(a+r)^2 &\Longrightarrow a = r(\imath - 1) && \text{contradiction with (7),}\\
r^2 = -2ar - r^2 &\Longrightarrow |r| = |a| && \text{contradiction with (6),}\\
r^2 = 2ar + r^2 &\Longrightarrow 2ar = 0 && \text{contradiction with (8),}\\
2ar + a^2 = (a+r)^2 &\Longrightarrow r = 0 && \text{contradiction with (8),}\\
2ar + a^2 = -(a+r)^2 &\Longrightarrow r = a(\sqrt{2}-2) && \text{contradiction with (7),}
\end{aligned}$$

$$\begin{aligned}
2ar + a^2 = -2ar - r^2 &\Longrightarrow r = a(\sqrt{3} - 2) && \text{contradiction with (7),} \\
2ar + a^2 = 2ar + r^2 &\Longrightarrow |a| = |r| && \text{contradiction with (6),} \\
(a + r)^2 = -2ar - r^2 &\Longrightarrow a = r(\sqrt{2} - 2) && \text{contradiction with (7),} \\
(a + r)^2 = 2ar + r^2 &\Longrightarrow a = 0 && \text{contradiction with (8).}
\end{aligned}$$

Therefore, applying restrictions (6), (7), (8) and (9) ensures the resulting MHM is full rate.

While Adam's construction was effective for proving the existence of order n MHMs for all n, the practical application of such a construction is diminished by the scarcity of desirable results. For order six, the fifth element in an Adam's construction takes the form of $r^4$, a value that rapidly becomes much larger than the rest of the elements in the construction. The new construction defined in this paper helps to fill in some of the gaps, and gives a construction for order six that is practical and easily yields more results with elements of few digits. However, neither construction gives exhaustive solutions, and constructions for other orders must be considered. A more generalized construction that yields usable results is a desirable outcome.

# References

[1] S. S. Adams, M. Crawford, C. Greeley, B. Lee and M. K. Murugan, Multilevel and multidimensional Hadamard matrices, *Des. Codes Cryptogr.* (3) **51** (2009), 245-252.

[2] J. Seberry, B. J. Wysocki and T. A. Wysocki, On some applications of Hadamard matrices, *Metrika* (2-3) **62** (2005), 221-239.

[3] Q. K. Trinh, P. Fan and E. M. Gabidulin, Multilevel Hadamard matrices and zero correlation zone sequences, *Electron. Lett.* (13) **42** (2006), 748-750.