2011

Multilevel Hadamard Matrices

Keli Siqueiros Parker
Wright State University

MULTILEVEL HADAMARD MATRICES

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science

By

KELI SIQUEIROS PARKER
B.S. University of California Davis, 2009

2011
Wright State University

WRIGHT STATE UNIVERSITY
SCHOOL OF GRADUATE STUDIES

May 23, 2011

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY Keli Siqueiros Parker ENTITLED Multilevel Hadamard Matrices BE ACCEPTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF Master of Science.

K.T. Arasu, Ph.D.
Thesis Director

Weifu Fang, Ph.D.,
Chair
Department of
Mathematics and Statistics
College of Science and Mathematics

Committee on
Final Examination

K.T. Arasu, Ph.D.

Yuqing Chen, Ph.D.

Xiaoyu Liu, Ph.D.

Andrew Hsu, Ph.D.
Dean, School of
Graduate Studies

ABSTRACT

Parker, Keli Siqueiros. M.S., Department of Mathematics and Statistics, Wright State University, 2011. Multilevel Hadamard Matrices.

Multilevel Hadamard Matrices (MHMs) have been examined by Trihn, Fan, and Gabidulin for constructions of multilevel zero-correlation zone sequences, which in turn have useful application in quasi-synchronous code division multiple access (CDMA) systems. Subsequently, Adams, Crawford, Greeley, Lee and Murugan introduced a construction of full-rate circulant MHMs and proved the existence of an order n MHM with n elements of distinct absolute value for all n, thus determining the maximum number of distinct elements permissible in an order n MHM to be the greatest possible. We give a survey of MHMs, in particular examining the circulant case and the methods for studying such objects. We provide several observations regarding Adams' construction, discuss the characterization of circulant matrices H satisfying $HH^T = wI$ for orders 3 and 4, and give new constructions for other orders of MHMs.

CONTENTS

LIST OF TABLES

1. Introduction

A Hadamard matrix of order n is defined as a square matrix H with entries of ± 1 such that

$$HH^T = nI_n.$$

Equivalently, a Hadamard matrix may be defined as a ± 1 matrix, with the restriction that the rows are mutually orthogonal. Clearly columns must also be mutually orthogonal, and

$$H^T H = nI$$

also holds [9].

It is well known that a necessary condition for the existence of a Hadamard matrix of order n is $n = 1, 2$ or $n \equiv 0 \pmod 4$. The Hadamard matrix conjecture speculates that this condition is sufficient for existence, but the question remains open, with the smallest unknown case currently of order 668. Hadamard matrices have significant applications for error correcting codes, optimal weighing designs, and CDMA spreading codes [22].

There are many generalizations of Hadamard matrices that have been studied for their potential use in similar applications. Multilevel Hadamard matrices (MHMs) in particular were proposed by Trinh et al. as an extension of Hadamard matrices for use in the construction of multilevel zero-correlation zone sequences. MHMs are $n \times n$ matrices with nonzero integer entries whose columns are mutually orthogonal. Specifically, an MHM of order n, weight w, referred to as $MHM(n, w)$ is an $n \times n$

matrix M with nonzero integer entries $\pm a_1, \pm a_2, \ldots, \pm a_n$ satisfying

$$MM^T = M^T M = wI,$$

where

$$w = \sum_{i=0}^{n} a_i^2.$$

The latter condition pertaining to the weight w as the sum of the squares of the elements is readily seen to be a result of the mutual orthogonality of the column vectors (and hence row vectors as well). The matrix product MM^T takes on nonzero values only along the main diagonal, at which point entries are simply the inner product of said column vector with itself [1]. While we suspect that MHMs may have applications similar to those of traditional Hadamard matrices (see section Applications), the issue of how to best incorporate such a non-binary object into existing and developing systems is yet unresolved. However, for this thesis we primarily are concerned with investigating the combinatorial properties and constructions of MHMs, and it is our hope that future work may prove these objects to be valuable in application.

Motivated by Adams et al. we refer to order n MHMs with n elements of distinct absolute value as full rate MHMs (FMHMHs), from the terminology of generalized orthogonal designs. Orthogonal designs have been a topic of research in combinatorics for some time, and it can be seen that if we replace the integer entries of an MHM with commuting indeterminates we obtain an orthogonal design. For an original treatment of the subject we refer the reader to [10]. In this thesis we are most concerned with circulant (CMHMs) and full rate circulant MHMs (FCMHMs) as investigated by

Adams et al. A CMHM M of order n takes the form of

$$M = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_2 & \cdots & a_{n-1} & a_0 & a_1 \\ a_1 & \cdots & a_{n-2} & a_{n-1} & a_0 \end{bmatrix},$$

where each row consists of a right cyclic shift of the previous row and of course the conditions of an MHM are satisfied [1]. In this way it becomes clear that a CMHM is completely determined by its first row, and we may use notation to take advantage of this fact. When referring to group invariant MHMs we will make use of the group ring notation (see section: Preliminaries).

Theorem 1. *(Adams et al.* [1]*) For all positive integers $n \neq 4$, there exists an FCMHM with n entries of distinct absolute value.*

Example 1. The following example of a previously unknown order 5 FCMHM of weight 1681 is

$$M = \begin{bmatrix} 6 & 17 & 14 & 26 & -22 \\ -22 & 6 & 17 & 14 & 26 \\ 26 & -22 & 6 & 17 & 14 \\ 14 & 26 & -22 & 6 & 17 \\ 17 & 14 & 26 & -22 & 6 \end{bmatrix}.$$

Related to Hadamard matrices and MHMs are weighing matrices, denoted $W(n, k)$, square $n \times n$ matrices of weight k with entries in {-1,0,1} whose columns are mutually orthogonal. A more generalized design would be an integer weighing matrix (IW, or ICW if circulant), defined as a square matrix W with integer entries (possibly including 0) satisfying

$$WW^T = kI$$

for some weight k. In this thesis we will consider IWs as the most general family of integer entry objects which Hadamard matrices, MHMs, FCMHMs and ICWs all belong to.

2. Preliminaries

Let R be a commutative ring with identity and G a multiplicatively written group. Then the group ring $R[G]$ is defined as the set of formal sums

$$A = \sum_{g \in G} a_g g,$$

with $a_g \in R$.

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g$$

and

$$(\sum_{g \in G} a_g g)(\sum_{h \in G} b_h h) = \sum_{g,h \in G} (a_g b_h) gh$$

define addition and multiplication, respectively, for $R[G]$ [19]. Earlier we noted that any CMHM is completely determined by its first row, and we would take advantage of this by using the group ring notation. In actuality, we will use group ring notation for any group invariant matrix, not just cyclic matrices. That is, let M be any matrix of order n and S_n denote the symmetric group of order n. M is group invariant given the existence of a subgroup G of S_n for which a group action is defined on the set $\{1, 2, \ldots, n\}$ such that for $M = [m_{i,j}]$, $m_{g(i),g(j)} = m_{i,j}$. It can be seen that the set of group invariant matrices over a ring R is isomorphic to the group ring $R[G]$ via the isomorphism

$$\Psi(M) = \sum_{g \in G} m_{g(1),1} g,$$

as given in [3].

Hence the $MHM(n,w)$ M with entries $a_0, a_1, \ldots, a_{n-1}$ may be represented as $A \in \mathbb{Z}[G]$, where G is a group of order n and

$$A = \sum_{g \in G} a_g g.$$

Equivalently, if we let g be a generator of C_n, the cyclic group of order n, and the entries $a_0, a_1, \ldots, a_{n-1}$ are of distinct moduli, A represents a FCMHM and we may write A in polynomial notation as

$$A = \sum_{i=0}^{n-1} a_i g^i = a_0 + a_1 g + \cdots + a_{n-1} g^{n-1},$$

highlighting the circulant nature of the object. At this point it is convenient to mention that $w = v^2$, where $v = \sum_{i=0}^{n-1} a_i$. For the remainder of this thesis we will refer to such v as the *sum weight* of an FCMHM. The following are notations commonly used in the study of group ring objects that are useful for the remainder of the thesis. See [9].

Definition 1. *Let $A \in Z[G]$ be a group ring element and t an integer. Then we define*

$$A^{(t)} = \sum_{g \in G} a_g g^t \quad for \quad A = \sum_{g \in G} a_g g.$$

Similarly, if $\alpha : G \to H$ is a mapping from the group G into a group H, then we extend this map linearly as a mapping from $\mathbb{Z}[G]$ into $\mathbb{Z}[H]$ and denote this as

$$A^{\alpha} = \sum_{g \in G} a_g g^{\alpha} \quad for \quad A = \sum_{g \in G} a_g g.$$

Definition 2. *For $A \in R[G]$, the support of A is defined as*

$$supp(A) = \{g \in G : a_g \neq 0\},$$

hence for MHM $M \in \mathbb{Z}[G]$, $supp(M) = G$.

Most of our interest for this thesis is directed at circulant examples and as such, group ring representations are created using cyclic groups. However, it seems that it would be of interest for the future study of such objects to consider MHMs constructed with abelian groups in general. We thus borrow some ideas from the study of difference sets to obtain generalized conditions for an object to be an MHM.

Using our group ring notation as described above, we may now see that the transpose of a matrix A is $A^{(-1)} \in \mathbb{Z}[G]$. Hence for an abelian group G, $A \in \mathbb{Z}[G]$ represents an MHM of weight w if and only if the support of A is G and

$$AA^{(-1)} = w.$$

A represents an FMHM if and only if in addition to the above condition, the coefficients of A are of distinct moduli. We introduce some common definitions, see [20].

2.1. **Characters.** Let G be an abelian group and $\mathbb{C}^*$ denote the multiplicative group of all the nonzero elements of the field of complex numbers. Then we call a homomorphism χ from G into $\mathbb{C}^*$ a complex character of G and denote the set of all such characters by $\widehat{G}$. It is easy to see that $\widehat{G}$ forms a group under point-wise multiplication that is in fact isomorphic to G itself. Characters map elements of G to roots of unity, specifically, if g is an element of order v in G then $\chi(g)$ is a v-th root of unity

for any character χ. Additionally, for g an element of order v in G, if ξ is a v-th root of unity in $\mathbb{C}^*$, then there exists χ in $\widehat{G}$ such that $\chi(g) = \xi$. The principal character is the identity element of $\widehat{G}$ that maps all $g \in G$ to the identity of $\mathbb{C}^*$. We will use characters in our notation by extending them linearly as

$$\chi(A) = \sum_{g \in G} a_g \chi(g) \quad for \quad A = \sum_{g \in G} a_g g.$$

Thus $\chi(A) \in \mathbb{C}$ for our purposes. The following are well known regarding characters.

Orthogonality Relations:

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{for } g = 1 \\ 0 & \text{for } g \neq 1 \end{cases}$$

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{for } \chi = \chi_0 \\ 0 & \text{for } \chi \neq \chi_0 \end{cases},$$

where χ_0 is the principal character.

Inversion Formula:

$$a_g = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(A)\chi(g^{-1}) \quad for \quad A = \sum_{g \in G} a_g g \in \mathbb{Z}[G].$$

Hence for $A, B \in \mathbb{Z}[G]$, if $\chi(A) = \chi(B)$ for all $\chi \in \widehat{G}$, then A = B. Now we have the following generalized result for MHMs.

Lemma 1. *An element A of a group ring $\mathbb{Z}[G]$, where the order of G is n and $supp(A) = G$ is an $MHM(n, w)$ if and only if for every character $\chi \in \widehat{G}$,*

$$|\chi(A)| = \sqrt{w}.$$

Proof. We apply any character χ to our equation $AA^{(-1)} = w$ to get

$$\chi(AA^{(-1)}) = w\chi(1).$$

Since we are considering complex characters, it is clear that $\chi(g^{-1}) = (\chi(g))^{-1} = \overline{\chi(g)}$ for all $g \in G$, so

$$\chi(AA^{(-1)}) = \chi(A)\chi(A^{(-1)}) = \chi(A)\overline{\chi(A)} = |\chi(A)|^2.$$

Furthermore, $w\chi(1) = w$ and we have the identity. Finally, inversion formula completes the proof. □

It is a simple observation to note that $\chi(A)$ is an eigenvalue of the matrix representation of A for any character $\chi \in \widehat{G}$, and $\{\chi(A) : \chi \in \widehat{G}\}$ gives all eigenvalues of A.

2.2. **Similarity of MHMs.** A notable issue with FCMHMs is determining when two such objects are equivalent. It becomes necessary to consider the possible redundancy of considering $A = \sum_{h \in G} a_h h$ and $gA = \sum_{h \in G} a_h gh$ as distinct FCMHMs when clearly gA is simply a cyclic shift of A for g a nonidentity element of G.

Definition 3. *Let A be an IW of order n weight w. We define an IW B as a permutation of A if there exists a bijection σ from G to itself such that $B = A^\sigma$.*

It is immediate that for any MHM A, we may easily generate an MHM that is a permutation of A by letting σ be an automorphism. In general if σ not an automorphism, A^σ will not be an MHM, with the exception that any translate of A clearly will be. FCMHMs that are permutations of each other have the same order, the same weight, and contain the same n coefficients. However we may have MHMs that are related to one another in far more subtle ways. In fact we can see that the space of IWs is closed under matrix multiplication, as is the space of all ICWs, and that MHMs and FCMHMs are closed under scalar multiplication. Let M be an $FCMHM(n, w)$ and $\alpha \in \mathbb{Z} \setminus \{0\}$. Then we have that

$$MM^T = wI_n \Longrightarrow (\alpha M)(\alpha M^T) = \alpha^2 w I_n.$$

Now α is an integer, so clearly αM contains n elements of distinct absolute value provided that M does, and αM is an FCMHM with weight $\alpha^2 w$.

Definition 4. *We define a reduced MHM M with integer coefficients $a_0, a_1, \ldots, a_{n-1}$ as an MHM such that $gcd(a_0, a_1, \ldots, a_{n-1}) = 1$. By the reduced form of an MHM M, we mean sM, where s is an appropriate scalar such that sM is a reduced MHM.*

Definition 5. *Two MHMs are defined to be similar if their reduced forms are permutations of each other.*

Let A, B be examples of an $MHM(n,w)$ and $MHM(n,v)$, respectively. It is clear that AB and BA are $IW(n,wv)$, and with the proper restrictions, $MHM(n,wv)$.

$$AB(AB)^T = ABB^TA^T = AvI_nA^T = wvI_n.$$

Hence it would seem useful to provide yet another definition for MHMS.

Definition 6. *An MHM M is said to be irreducible if M is not the product of at least one MHM with a nonidentity IW of the same order. Hence an $MHM(n,w)$ is always irreducible if $w = p^2$, p a prime.*

In our investigation of the existence of MHMs, an important question for classification purposes arose. Can we find n, w such that there exist M_1, M_2 both $MHM(n,w)$s such that M_1 is not similar to M_2? Unfortunately for the complexity of the problem we are able to answer an even stronger question with the following irreducible $FCMHM(5,71^2)$s, which are clearly not similar.

$$6 + 18g + 26g^2 + 54g^3 - 33g^4,$$

$$62 + 11g + 26g^2 - 16g^3 - 12g^4.$$

3. Known Constructions

MHMs were originally conceived by Trihn, Fan, and Gabidulin as a method for the construction of multilevel zero correlation zone sequences and they considered examples of MHMs constructed with an alphabet of 2 elements. We include some particular construction results here from [22].

3.1. **Kronecker product and two element circulant constructions.** Let M_1 and M_2 be $MHM(n, w)$ and $MHM(m, v)$, respectively. Then $M_1 \otimes M_2$, where $\otimes$ is the Kronecker product is an $MHM(nm, wv)$.

$$(M_1 \otimes M_2)(M_1 \otimes M_2)^T = \begin{bmatrix} m^1_{(1,1)}M_2 & \cdots & m^1_{(1,n)}M_2 \\ m^1_{(2,1)}M_2 & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ m^1_{(n,1)}M_2 & \cdots & m^1_{(n,n)}M_2 \end{bmatrix} \begin{bmatrix} m^1_{(1,1)}M_2^T & \cdots & m^1_{(n,1)}M_2^T \\ m^1_{(1,2)}M_2^T & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ m^1_{(1,n)}M_2^T & \cdots & m^1_{(n,n)}M_2^T \end{bmatrix}$$

$$= wvI_{nm}.$$

If we consider the Kronecker product of a binary Hadamard matrix and an MHM it becomes quite easy to build MHMs of larger orders that have a clear block structure. Trihn et al. include such a construction in their work, along with a two element circulant construction that generates a CMHM for all $n > 1$. They note that if we generate an $n \times n$ circulant matrix with first row $[abb \cdots b]$, then the matrix will be an MHM if we subject the elements to the restriction that $2ab - (n-2)b^2 = 0$. This restriction satisfies the same constraining equations that the Adams construction arises from (see 3.2), and provides a simple method for generating a circulant $MHM(n, n^2)$ for any $n > 2$. Simply let $b = 2$ and $a = 2 - n$ and this is easily achieved.

3.2. **Adams construction.** [1] If an order n matrix is group invariant, as are most MHMs we consider, then it may be constructed with a potential maximum of n elements. Adams et al. proved that an MHM of order n with n elements of distinct absolute value exists for all n, and it was the construction Adams gave as proof that provided the motivation for this thesis.

Adams examined the equations that arise from the condition that an MHM has mutually orthogonal columns, and considered the circulant case as follows. Let

$$A = \sum_{i=0}^{n-1} a_i g^i \in \mathbb{Z}[C_n]$$

be a circulant MHM of order n with weight w. Then it may be observed that in order for $AA^{(-1)} = wI_n$ to hold, the equations

$$\sum_{i=0}^{n-1} a_i a_{i+j(mod\ n)} = 0$$

must be satisfied for $j = 1, \ldots, \lfloor \frac{n}{2} \rfloor$. In fact, any integers satisfying the above equations will generate a circulant MHM. The $\lfloor \frac{n}{2} \rfloor$ equations are simpler to deal with than the general case, which would involve $\binom{n}{2}$ such equations. We will later see that a $\lfloor \frac{n}{2} \rfloor$ condition on the number of equations necessary to express mutual orthogonality can be exploited for non-circulant group invariant matrices as well. Adams et al. then took the equation with general j and manipulated in the following way. Let r be an integer greater than 1 and let $a_i = r^i$ for $i = 0, 1, \ldots, n-2$. We may then solve for a_{n-1} to achieve

$$a_{n-1} = -\frac{r^{n-1} - r}{r^2 - 1}.$$

Since r was selected to be an integer, a_i is an integer for $i = 1, \ldots, n-2$. a_{n-1} is potentially not an integer, but by selecting s an appropriate scalar, for instance $s = r^2 - 1$, we may ensure all entries are integers by replacing a_i with sa_i for $i = 1 \ldots, n-1$ if need be. We also note that the use of a scalar makes the restriction of r to an integer unnecessary, and the construction holds for $r \in \mathbb{Q}$ not equal to ± 1 or 0, appropriate scalar $s \in \mathbb{Z}$.

We thus refer to Adams' construction as

$$A = s[(\sum_{i=0}^{n-2} r^i g^i) - (\frac{r^{n-1} - r}{r^2 - 1})g^{n-1}].$$

Since Adams' construction is clearly circulant we will have an FCMHM for the cases when $r^{n-1} - r \neq (r^2 - 1)r^i$ for $i = 1, \ldots, n-2$. Thus Adams' construction gives an FCMHM for all $n \neq 4$. Concerning the $n = 4$ case, Adams showed that no FCMHM of order 4 exists, although CMHMs and non-circulant FMHMs do [1]. The circulant binary Hadamard matrix $H = 1 + g + g^2 - g^3$ is a particularly interesting case of an order 4 MHM, and it is conjectured to be the only order greater than 1 for which a circulant binary Hadamard matrix exists [20]. This open conjecture has seen many failed attempts at a proof.

At this point we were motivated to investigate the existence of other examples of MHMs. As with weighing matrices and difference sets, the question existence for particular orders n and weights w is a topic of research interest. Clearly the work of Adams et al. answered an important question as to the orders n for which an MHM exists and in the process also answered for which n an FCMHM exists. However, a complete classification of MHMs is still unknown, and it was unclear if the examples

from the construction created by Adams et al. would cover the set of all FCMHMs. We thus focused on FCMHMs and initially used a brute force approach to the problem.

The key observation that led to the derivation of Adams' construction was the $\lfloor \frac{n}{2} \rfloor$ constraining equations mentioned above, and this suggested an elementary computer algorithm to search for explicit examples. While not elegant, it was effective for small n to write a code implementing nested for loops that would step the elements $a_i,\ i = 0, 1, \ldots, n-1$, through integers in a given range and test the satisfaction of the $\lfloor \frac{n}{2} \rfloor$ constraining equations while also ensuring full rate. Clearly large n prohibits such a method due to the high number of operations such an algorithm requires, and the nesting of the for loops ensures that an increase in n increases the computing time exponentially. However even using consumer level computers, this algorithm yielded FCMHMs of orders $3, 5, 6, 7, 8$, though the number of examples was greatly reduced for the later two cases. Examples which are not full-rate are also easily found and will be discussed later in the thesis. Every order 3 example found fit the Adam's construction and led to the following observation.

3.3. **Characterization of order 3.**

Remark 1. *Adams' construction gives a complete characterization of the family of order* 3 *group invariant MHMs, up to similarity .*

We may see this through the following arguments. Suppose M is an order 3 group invariant MHM. Hence we may write

$$M = \sum_{g \in C_3} a_g g.$$

We have that M is a circulant MHM and, denoting $C_3 = \langle g \rangle$, as such satisfies

$$MM^{(-1)} = (a_0 + a_1 g + a_2 g^2)(a_0 + a_1 g^2 + a_2 g) = a_0^2 + a_1^2 + a_2^2.$$

We thus are able to derive the following:

$$a_0 a_1 + a_1 a_2 + a_0 a_2 = 0$$

$$a_2 = -\frac{a_0 a_1}{a_1 + a_0}$$

$$\frac{a_2}{a_0} = -\frac{a_1}{a_1 + a_0} = -\frac{\frac{a_1}{a_0}}{\frac{a_1}{a_0} + 1}$$

Set $r = \frac{a_1}{a_0}$, select scalar s for integer entries, and M is similar to

$$\frac{s}{a_0} M = s(1 + rg - \frac{r}{r+1} g^2),$$

which is precisely Adams' construction for order 3. Note that the above arguments are valid even for non-integer valued M, and Adams construction completely characterizes order 3 group invariant matrices A satisfying $AA^T = wI$. Similarly the following general observation covers the order 3 case.

Remark 2. *The roots $a,\ b,\ c$ of any polynomial of the form $x^3 + wx^2 + \alpha$ form a circulant matrix represented by $A = a + bg + cg^2$ that satisfies $AA^{(-1)} = w$.*

This is easily seen to be true when we recall that the x coefficient of such a polynomial $(x - a)(x - b)(x - c)$ is necessarily $ab + bc + ac$. Hence if the x coefficient is zero, then $ab + bc + ac = 0$ and the only constraining equation on the elements of

an order three group invariant matrix with mutually orthogonal columns is satisfied. This gives a complete classification of the family of order 3 complex group invariant matrices A satisfying $AA^{(T)} = wI$ for some w.

4. Circulant Order 6 MHMs and the Doubling Theorem

To us a result from a computer search is not interesting in and of itself beyond the potential for application, so we set about investigating results that were not obviously of the family described by Adams. In particular, orders 5 and 6 yielded several results that failed to arise from any known r, s used in Adams' construction. However, there was a structure to a subset of the order 6 results that satisfied a new construction. It was through this observation that we were able to generate the order 6 construction as follows.

4.1. **Order 6 construction.**

Lemma 2. *Let $p, q \in \mathbb{Q} \setminus \{0\}$. Then*

$$M = s[p^2 + (q^2 - p^2)g + q^2g^2 + (2pq + p^2)g^3 + (p + q)^2g^4 - (2pq + q^2)g^5] \in \mathbb{Z}[C_6]$$

is MHM of order n for (if needed) appropriate scalar $s \in \mathbb{Z}$, and is FCMHM for $|p| \neq |q|$, $p \neq -2q$, $q \neq -2p$.

Proof. Since $M = \sum_{i=0}^{n-1} a_i g^i \in \mathbb{Z}[C_6]$, the entries of M must satisfy the $\lfloor \frac{n}{2} \rfloor = 3$ constraining equations

$$a_0a_1 + a_1a_2 + a_2a_3 + a_3a_4 + a_4a_5 + a_5a_0 = 0,$$

$$a_0a_2 + a_1a_3 + a_2a_4 + a_3a_5 + a_4a_0 + a_5a_1 = 0,$$

$$a_0a_3 + a_1a_4 + a_2a_5 = 0.$$

A simple exercise in arithmetic shows that the coefficients of M satisfy the constraining equations, and that all entries are nonzero. Thus M is MHM. The additional restrictions $|p| \neq |q|$, $p \neq -2q$, $q \neq -2p$ are sufficient for FCMHM (see [18]). $\square$

Example 2. The following is an example of a previously unknown $FCMHM(6, 14^2)$ constructed using the previous theorem with $p = 1, q = 2$.

$$M = 1 + 3g + 4g^2 + 5g^3 + 9g^4 - 8g^5.$$

Some examples resulting from the lemma are well known, however, we may show that the example above is not similar to any Adam's construction.

The sum weight of M is $k = 14$. Suppose there exists an Adams' construction FCMHM A that is similar to M. M is a reduced MHM, hence in reduced form, A must also be of sum weight 14. Now we consider Adams' construction for order 6 FCMHMs. For rational r, integer scalar s, we have that

$$A = s[(\sum_{i=0}^{4} r^i g^i) - (\frac{r^5 - r}{r^2 - 1})g^5].$$

The last coefficient is equivalent to $-(r^3 + r)$ and hence for any order 6 Adams' construction, the sum weight will be

$$v = s(r^4 + r^2 + 1).$$

We are now ready to use some well-known notions regarding polynomials to show that no order 6 Adams' construction can be similar to an FCMHM of sum weight 14.

If A were similar to M above, then there would exist integer scalar s and rational $r = \frac{p}{q}$ such that $v = 14$. Thus

$$sr^4 + sr^2 + s - 14 = 0$$

may be considered as a polynomial in r. By Descartes rule of signs, for r to be real s must be positive and $s - 14$ negative. Hence we impose the restriction $0 < s < 14$. Applying $r = \frac{p}{q}$, $gcd(p, q) = 1$, we see that

$$s\frac{p^4}{q^4} + s\frac{p^2}{q^2} + s - 14 = 0,$$

$$sp^4 + sp^2q^2 + q^4(s - 14) = 0,$$

so $p^2|(s - 14)$ and $q^2|s$. We now show that no such p, q and s exist.

$$\begin{aligned}
s = 1 \quad &\Longrightarrow q = 1, \quad p = 1 \quad v = 3, \\
s = 2 \quad &\Longrightarrow q = 1 \quad p = \begin{cases} 1 & v = 6, \\ 2 & v = 42, \end{cases} \\
s = 3 \quad &\Longrightarrow q = 1 \quad p = 1 \quad v = 9, \\
s = 4 \quad &\Longrightarrow p = 1 \quad q = \begin{cases} 1 & v = 12, \\ 2 & v = \frac{21}{4}, \end{cases} \\
s = 5 \quad &\Longrightarrow q = 1 \quad p = \begin{cases} 1 & v = 15, \\ 3 & v = 455, \end{cases} \\
s = 6 \quad &\Longrightarrow q = 1 \quad p = \begin{cases} 1 & v = 18, \\ 2 & v = 126, \end{cases}
\end{aligned}$$

$$
\begin{aligned}
s = 7 \quad &\Longrightarrow q = 1 \quad p = 1 \quad v = 21, \\
s = 8 \quad &\Longrightarrow p = 1 \quad q = \begin{cases} 1 & v = 24, \\ 2 & v = \frac{21}{2}, \end{cases} \\
s = 9 \quad &\Longrightarrow p = 1 \quad q = \begin{cases} 1 & v = 27, \\ 3 & v = \frac{91}{9}, \end{cases} \\
s = 10 \quad &\Longrightarrow q = 1 \quad p = \begin{cases} 1 & v = 30, \\ 2 & v = 210, \end{cases} \\
s = 11 \quad &\Longrightarrow q = 1 \quad p = 1 \quad v = 33, \\
s = 12 \quad &\Longrightarrow p = 1 \quad q = \begin{cases} 1 & v = 36, \\ 2 & v = \frac{63}{4}, \end{cases} \\
s = 13 \quad &\Longrightarrow q = 1 \quad p = 1 \quad v = 39.
\end{aligned}
$$

Thus no such p, q and s exist for which A has sum weight $v = 14$.

4.2. **The doubling theorem.** We later found that Lemma 2 was a specific case of a more general construction for MHMs that also gives results not of Adams construction. Several theorems on weighing matrices are easily adapted to give construction results for MHMs. See [3], [7], [5] for the inspiration to the following theorems.

Theorem 2. *Let $A, B \in \mathbb{Z}[G]$ be MHMs of the same weight w for an abelian group G of order n. Let $\langle t \rangle = C_2$. Note $t^2 = 1$. Then $M \in \mathbb{Z}[G \times \langle t \rangle]$,*

$$M = (1 - t)A + (1 + t)B$$

is an IW of order $2n$, weight $4w$.

Proof. Observe that

$$MM^{(-1)} = (1-t)^2 AA^{(-1)} + (1+t)^2 BB^{(-1)}$$

$$= 4w$$

Since entries of M must be integers, the proof is complete. □

Clearly the way we have stated theorem two we cannot guarantee that the constructed object M will have support $G \times \langle t \rangle$, so we do not have an MHM. A trivial example of when this might happen would include constructing

$$M = (1-t)A + (1+t)A,$$

in which case $supp(M) = G$. To overcome this, we give another result.

Theorem 3. The Doubling Theorem: *Let $A \in \mathbb{Z}[C_n]$ be an FCMHM of weight w. Let $g \in C_n \setminus \{1\}$, $\langle t \rangle = C_2$. Then $M \in \mathbb{Z}[C_n \times \langle t \rangle]$,*

$$M = (1-t)A + (1+t)gA$$

is an MHM of order $2n$, weight $4w$. If n is odd, them M above is a circulant MHM of order $2n$.

Proof. As before,

$$\begin{aligned} MM^{(-1)} &= (1-t)^2 AA^{(-1)} + (1+t)^2 (gA)(gA)^{(-1)} \\ &= 4w. \end{aligned}$$

Since A is FCMHM and $g \neq 1$,

$$\begin{aligned} A &= \sum_{h \in C_n} a_h h, \quad gA = \sum_{h \in C_n} a_{g^{-1}h} h, \\ M &= \sum_{h \in C_n} (a_h + a_{g^{-1}h}) h + (a_h - a_{g^{-1}h}) th, \\ &= \sum_{g \in C_n \times C_2} m_g g, \end{aligned}$$

and $|a_h| \neq |a_{g^{-1}h}|$ for any $h \in C_n$. Thus, $m_g = a_h + a_{g^{-1}h}$ or $m_g = a_h - a_{g^{-1}h}$ and $m_g \neq 0$ for any $g \in C_n \times C_2$. □

Example 3. The doubling theorem provides a construction for order $2n$ MHMs. Clearly if n is even or the resulting MHM is not full rate, then these constructions provide results unique from Adams construction by structure. However, if n is odd, the resulting MHM is circulant and still many of these do not follow Adams' construction. In addition, under certain conditions we may achieve an order $2n$ FCMHM from two odd order n FCMHMs. In the following we will use a non-Adams $FCMHM(5, 11^2)$ H and an Adams' construction $FCMHM(7, 127^2)$ A to construct an order 10 circulant

MHM and order 14 FCMHM, respectively. Following the theorem let

$$H = 6 + 2g + 8g^2 - g^3 - 4g^4,$$

$$gH = -4 + 6g + 2g^2 + 8g^3 - g^4,$$

$$A = 3 + 6g + 12g^2 + 24g^3 + 48g^4 + 96g^5 - 62g^6,$$

$$gA = -62 + 3g + 6g^2 + 12g^3 + 24g^4 + 48g^5 + 96g^6.$$

Then

$$\begin{aligned} M &= (1-t)H + (1+t)gH \\ &= 2 + 8g + 10g^2 + 7g^3 - 5g^4 - 10t + 4tg - 6tg^2 + 9tg^3 + 3tg^4, \\ &= 2 + 4tg + 10g^2 + 9tg^3 - 5g^4 - 10t + 8g - 6tg^2 + 7g^3 + 3tg^4 \end{aligned}$$

is a circulant $MHM(10, 22^2)$, and

$$\begin{aligned} N &= (1-t)A + (1+t)gA \\ &= -59 + 9g + 18g^2 + 36g^3 + 72g^4 + 144g^5 + 34g^6 \\ &\quad - 65t - 3tg - 6tg^2 - 12tg^3 - 24tg^4 - 48tg^5 + 158tg^6, \\ &= -59 - 3tg + 18g^2 - 12tg^3 + 72g^4 - 48tg^5 + 34g^6 \\ &\quad - 65t + 9g - 6tg^2 + 36g^3 - 24tg^4 + 144g^5 + 158tg^6 \end{aligned}$$

is an $FCMHM(14, 254^2)$.

It is easy to see that the doubling theorem may also be represented by a block matrix construction. Let A, gA be as above. Then

$$M = \begin{bmatrix} A + gA & gA - A \\ gA - A & A + gA \end{bmatrix}$$

is an equivalent representation of the construction.

From a combinatorial perspective, one could argue that a full rate result is more interesting due to the inherent structure and various properties that hold for distinct elements. As we will see in the applications section this requires closer examination to determine if a full rate MHM is of more than just theoretical interest. However, we note here that we may use the doubling theorem in a manner to guarantee a full rate result. Let A be an Adam's construction MHM. Then we may use A and gA as in the theorem in the following way. Assume

$$A = \sum_{i=0}^{n-1} a_i g^i \ , \quad \text{so}$$

$$gA = \sum_{i=0}^{n-1} a_{i-1(mod\ n)} g^i.$$

Since we have added the restriction that A is an Adams construction, we are able to specify A and gA even further. We note that an MHM is full rate iff any similar MHM is also full rate, hence we may scale A however we wish. For simplicity, we let our scalar $s = r^2 - 1$, the denominator of the last element in the general Adams construction, and assume r is an integer. Now consider $M = A - tA + gA + tgA$.

With the mentioned scaling, coefficients of M consist of:

$$\begin{aligned}
r^{i+3} + r^{i+2} - r^{i+1} - r^i \qquad & i = 0, \ldots, n-3, \\
-r^{i+3} + r^{i+2} + r^{i+1} - r^i \qquad & i = 0, \ldots, n-3, \\
-r^{n-1} + r^2 + r - 1, & \\
-r^{n-1} - r^2 + r + 1, & \\
r^n - r^{n-1} - r^{n-2} + r, & \\
r^n + r^{n-1} - r^{n-2} - r. &
\end{aligned}$$

The only further restriction then required then is that $r \notin \{\pm 1\}$, and M will be full rate.

As noted previously, we realized that the order 6 construction is actually a doubling theorem construction from a rational formulation of an order three Adams construction. Observe that Adams order three construction may be rewritten with rational $r = \frac{p}{q}$ as

$$A = s(1 + \frac{p}{q}g - \frac{p}{p+q}g^2).$$

Scale this minimally by $s = q(p+q)$ to achieve

$$A = (pq + q^2) + (p^2 + pq)g - (pq)g^2,$$

$$gA = -(pq) + (pq + q^2)g + (p^2 + pq)g^2.$$

Now by the doubling theorem,

$$\begin{aligned} N =&(1-t)A + (1+t)gA, \\ =&q^2 + (p+q)^2 g + p^2 g^2 - (2pq+q^2)t + (q^2-p^2)tg + (2pq+p^2)tg^2, \\ =&p^2 g^2 + (q^2-p^2)tg + q^2 + (2pq+p^2)tg^2 + (p+q)^2 g - (2pq+q^2)t. \end{aligned}$$

We may then easily multiply N by g and still have an MHM. Finally, replace tg^2, which is a generator of the cyclic group C_6, with $\dot{g}$ and we see the order six construction clearly.

$$\begin{aligned} Ng =&p^2 + (q^2-p^2)tg^2 + q^2 g + (2pq+p^2)t + (p+q)^2 g^2 - (2pq+q^2)tg, \\ =&p^2 + (q^2-p^2)\dot{g} + q^2\dot{g}^2 + (2pq+p^2)\dot{g}^3 + (p+q)^2\dot{g}^4 - (2pq+q^2)\dot{g}^5. \end{aligned}$$

5. Folding

Very early on in our investigation of MHMs, it was noted that for any $MHM(n, w)$ achieved through a computer search, we could find another $MHM(n, w)$ whose coefficients were a simple permutation of the those of the previous object. As noted in the preliminaries section, we decided to denote two such MHMs as permutations of each other, and to classify them as similar MHMs. Also noted was that for A an $MHM(n, w)$, σ an automorphism of the generating group G, A^σ is a similar $MHM(n, w)$. However, the restriction of σ to an automorphism on G need not be so strong to ensure that A^σ is an MHM in general. Consider instead $\varphi : G \to H$ any group homomorphism. We can easily extend this homomorphism linearly to $\varphi : \mathbb{Z}[G] \to \mathbb{Z}[H]$, as mentioned in the preliminaries section. The following is adapted from [4], [5].

Theorem 4. Folding Theorem: *Let M be any $MHM(n, w)$ for some abelian group G of order n. Let φ be a group homomorphism from G to some group H. Extend φ linearly to a group ring homomorphism and denote $\varphi(A)$ as A^φ for $A \in \mathbb{Z}[G]$. That is*

$$A^\alpha = \sum_{g \in G} a_g g^\varphi \in \mathbb{Z}[H] \quad for \quad A = \sum_{g \in G} a_g g \in \mathbb{Z}[G].$$

Then M^φ is an $IW(v, w)$, where v is the order of H.

Proof. It is immediate that the coefficients of M^φ will be integers. We thus need only verify that $(M^\varphi)(M^{\varphi(-1)}) = w$. Let $M = \sum_{g \in G} a_g g$ be an $MHM(n, w)$. Then

$$
\begin{aligned}
(M^{\varphi})(M^{\varphi(-1)}) =& (\sum_{g\in G} a_g g^{\varphi})(\sum_{f\in G} a_f f^{\varphi(-1)}),\\
&= \sum_{g,f\in G} (a_g a_f) g^{\varphi} f^{\varphi(-1)},\\
&= \sum_{h\in G^{\varphi}} \left(\sum_{(gf^{-1})^{\varphi}=h} (a_g a_f) h \right).
\end{aligned}
$$

Now we know that

$$
\begin{aligned}
\sum_{gf^{-1}=\upsilon} a_g a_f =& 0 \qquad \text{for } \upsilon \in G \text{ not the identity of } G, \text{ and}\\
\sum_{gf^{-1}=\upsilon} a_g a_f =& w \qquad \text{for } \upsilon \in G \text{ the identity.}
\end{aligned}
$$

Hence

$$
\sum_{(gf^{-1})^{\varphi}=h} (a_g a_f) h = 0 \qquad \text{for } h \text{ a nonidentity element of H}
$$

and we have the above sum evaluate to

$$
(M^{\varphi})(M^{\varphi(-1)}) = w
$$

as required. □

Theorem 4 is a well known result that we have adapted for MHMs, and has been used for some time in the study of weighing matrices. It is used extensively to show some results in the recent work on Strassler's table in [4] and [5]. However one may

note that the folding theorem does not in fact guarantee that the homomorphic image of an MHM is necessarily MHM. For such a result to hold we must apply more restrictions to the original MHM, and the homomorphism φ. The most obvious preliminary requirement is that we require $\varphi : G \to H$ to be a surjective homomorphism, otherwise $supp(M^{\varphi}) \neq H$ trivially. Then we must apply additional restrictions to the coefficients of M such that the sum

$$\sum_{g \in G : g^{\varphi} = h} a_g \neq 0 \quad \text{for } h \in H.$$

Clearly many restrictions could be imposed, but for the sake of practicality, we include only a canonical result here.

Corollary 1. *Let M be a $FMHM(n, w)$ for some abelian group G of order n, n even. Let N be a normal subgroup of G of order 2. Then for $\varphi : G \to G/N$ given by $\varphi : g \mapsto Ng$, M^{φ} is an $MHM(\frac{n}{2}, w)$.*

Proof. All we need to verify is that M^{φ} will have support of order $\frac{n}{2}$. Since the coefficients of M are of distinct modulus, the sum of any two will be nonzero. Furthermore, since every coefficient of M^{φ} is the sum of two coefficients of M,

$$supp(M^{\varphi}) = G/N.$$

□

The folding theorem implies one possible application of MHMs in the search of weighing matrices. A common technique for shrinking the search parameters of a

potential weighing matrix is to consider the possible lower order matrices that the weighing matrix in question could fold down to. A particular MHM might be the result of just such a folding. It is notable that in practice it is generally easy to attain an MHM from the folding of a higher order MHM for an arbitrary subgroup.

5.1. **Non-circulant group invariant MHMs.** It is well known that non-circulant examples of MHMs exist, and we have discussed some ways to construct such objects, such as with a Kronecker product or the doubling theorem. There are also the obvious examples of any binary Hadamard matrix as a special case of an MHM. However, as with the circulant case, there do exist non-circulant MHMs that defy any known construction. One such example is the reduced form $FMHM(9, 21^2)$

$$A = 1 + 8g + 9g^2 + 11h + 3hg - 5hg^2 + 6h^2 - 2h^2g - 10h^2g^2.$$

It is unknown if this object is an irreducible example, especially since its sum weight is 21. However by inspection four coefficients are of prime modulus, suggesting that this is not the result of a Kronecker product between two order 3 MHMs. A and other non-circulant examples were found using a computer search algorithm very similar to the one used for the circulant case. The success of this algorithm relies once again on the fact that the condition of mutual orthogonality still gives $\lfloor \frac{n}{2} \rfloor$ equations, even when the group G is $\mathbb{Z}_3 \times \mathbb{Z}_3$. It is clear that the non-circulant case is not well understood and requires some inspection for a complete understanding to be realized.

Definition 7. *Let G be a group of order n and $A \in \mathbb{Z}[G]$. Any integer t with $(n,t)=1$ is called a multiplier of A if $A^{(t)} = Ag$ for some $g \in G$.*

This definition is actually specifying what has been referred to as a numerical multiplier in the literature, but we do not concern ourselves with multipliers that are non-numerical. Multipliers have been studied intensively for their usefulness in the construction of difference sets. In the following we include some results that may prove useful for the classification of MHMs. For a further discussion of multipliers see [9], [11], [12], [14], [16], [17], and in particular for a treatment of their use with the existence problem for circulant weighing matrices, see [4], [5]. The following is a well known result concerning multipliers originally from McFarland [16].

Theorem 5. The Multiplier Theorem *Let G be a finite abelian group or order n. Let A be an element of G such that $AA^{(-1)} = w^2$ for some integer w relatively prime to n. Let*

$$w = p_1^{\alpha_1} \dots p_s^{\alpha_s}$$

where the p_i's are distinct primes. Suppose there are integers $t, f_1, \dots, f_s$ such that

$$t \equiv p_1^{f_1} \equiv \dots \equiv p_s^{f_s} (mod n).$$

Then t is a multiplier of A.

Unfortunately for our problem we have not found a way to use multipliers for construction purposes as they are typically used for weighing matrices, an issue that

stems from the fact that for any group G generating an $MHM(n,w)$ A, $supp(A) = G$, and coefficients of A are not restricted to $\{\pm 1, 0\}$. However we are able to use multipliers in a fashion that gives certain restrictions to the possible weights of MHMs, a particularly useful result for the classification of the full rate case. The following notions have been noted by various authors throughout the years and are often used, we refer in particular to [2], [17], [8] and include an alternate proof here.

Lemma 3. *Let G be a multiplicatively written abelian group of order n, and let $A = \sum_{g\in G} a_g g$ be an element of the group ring $\mathbb{Z}[G]$ such that $\sum_{g\in G} a_g = k$. We define the stamina of A by*

$$St(A) = \prod_{g\in G} g^{a_g} \in G.$$

If $(n,k) = 1$, then there exists a unique translate of A, say $B = Ab$ for some $b \in G$, whose stamina is the identity of G.

Proof. Let $G = \{g_i\}_{i=0}^{n-1}$ be the desired abelian group as above and let A be an element of the group ring $\mathbb{Z}[G]$. Then

$$St(A) = \prod_{g\in G} g^{a_g} = g_0^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} \in G.$$

Now $(k,n) = 1$, so $\varphi : x \mapsto x^k$ is an automorphism on G. Hence there exists a unique $b \in G$ such that $g_0^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} b^k = e$. The result can now be made clear by observing

that

$$\begin{aligned} e = g_0^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} b^k =& (g_0 b)^{a_0} (g_1 b)^{a_1} \cdots (g_{n-1} b)^{a_{n-1}}, \\ =& \prod_{g \in G} (gb)^{a_g}, \\ =& St(B), \end{aligned}$$

where $B = Ab = \{gb : g \in A\}$. Hence B is the required translate. □

Lemma 4. *Let G be a multiplicatively written group of order n, $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$ such that $\sum_{g \in G} a_g = k$, $(k, n) = 1$. Then there exists a translate of A that is fixed by all multipliers of A.*

Proof. Let t be any multiplier of A. Note that t a multiplier of A implies t is a multiplier of any translate of A. Let $B = Ab$ be the unique translate of A whose stamina is identity, as in Lemma 3. Let $(Ab)^{(t)} = Ac$. We make the following observations.

$$\begin{aligned} e = e^t =& g_0^{ta_0} g_1^{ta_1} \cdots g_{n-1}^{ta_{n-1}} b^{tk}, \\ =& (g_0 b)^{ta_0} (g_1 b)^{ta_1} \cdots (g_{n-1} b)^{ta_{n-1}}, \\ =& (g_0 c)^{a_0} (g_1 c)^{a_1} \cdots (g_{n-1} c)^{a_{n-1}}, \\ =& g_0^{a_0} g_1^{a_1} \cdots g_{n-1}^{a_{n-1}} c^k. \end{aligned}$$

It must be that $b^k = c^k$. Furthermore, since $(k, n) = 1$ implies that $\varphi : x \mapsto x^k$ is an automorphism, $b = c$. Therefore $(Ab)^{(t)} = Ab$ □

These lemmas give a proof for the following well known result, as used in [2].

Corollary 2. *Let G be an abelian group of order n and let p be a prime relatively prime to n. If $A \in \mathbb{Z}[G]$ is such that $AA^{(-1)} = p^{2r}$, then there exists $g \in G$ such that $(gA)^{(p)} = gA$.*

Proof. Since $AA^{(-1)} = p^{2r}$ implies that $\sum_{g \in G} a_g = p^r$, and $(p^r, n) = 1$, all we need to do is verify that p is a multiplier of A and apply lemma 4. Of course, the multiplier theorem guarantees that such a prime p will indeed be a multiplier, and we have the required condition. □

The following is an adapted result of [2], which we include to explain a restriction on the possible weights of MHMs.

Theorem 6. *Let G be an abelian group of order n and let p be a prime relatively prime to n. Let $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$, where the a_g are distinct nonzero integers such that $AA^{(-1)} = p^{2r}$. That is let A be an MHM of order n and weight p^2. Then $p \equiv 1 (mod\ d)$ for d the exponent of G. If G is cyclic, then $p \equiv 1 (mod\ n)$.*

Proof. By Corollary 2, there exists an element $g \in G$ such that $(gA)^{(p)} = gA$. Since A is MHM, $supp(A) = G$, and hence $h \in G \Rightarrow h \in supp(A)$. Thus any $h \in G$ has the property of being fixed by p since the coefficients of A are distinct, that is, $h^p = h$ for all $h \in G$. Therefore, $o(h) | p - 1$ for all $h \in G$. Since d is the exponent of G, there exists an h such that $o(h) = d$ and thus $d | p - 1$. Clearly $d = n$ for cyclic groups G and the result holds. □

Although the previous prime weight theorem follows from a well known result, it has interesting implications for MHMs and their classification. In particular we would like to note that if p is a prime congruent to one modulo the order n of the MHM, then $\mathbb{Z}_p$ is a finite field that contains n^{th} roots of unity. Most of the research that we have conducted here was motivated by results of the previously mentioned computer search algorithm, and the motivation to consider the prime weight theorem was driven directly by a strong observation among the results. These observations seem to suggest the possibility of a specific structure to these MHMs, particularly in the circulant case. Obviously Adams construction results in MHMs that fit a specific cyclic form, and in the following we make some observations on the structure of this form. Later in the thesis, we include some conjecture and the evidence we have seen in the search results to support the idea of a connection between finite fields and MHMs.

7. On Adams Construction and Roots of Unity of a finite field

MHMs may be thought of in many different ways. In this thesis we have already used a group ring representation of the matrices, and included conditions for existence defined in terms of complex characters. Obviously MHMs are but one example of many generalized forms of $n \times n$ matrices that satisfy an $HH^T = wI_n$ condition. It is quite easy to find an MHM with entries that come from some ring other than the integers, we could for instance consider instead all real numbers in $\mathbb{R}$ and achieve scaled orthogonal matrices, or the field $\mathbb{C}$ of complex numbers and deal with unitary matrices, or even use entries from $\mathbb{Z}_k$ the ring of integers modulo some number k. We will discuss for now a simple observation pertaining to Adams construction MHMs.

Theorem 7. *Let $A \in \mathbb{Z}[G]$ be a reduced Adams' construction of order n, weight $w = v^2$ generated by an integer q and scaled minimally by s to ensure integer entries. Then the coefficients a_i of $A = \sum_{i=0}^{n-1} a_i g^i$ are the roots of $x^n - s^n$ in $\mathbb{Z}_v[x]$. That is,*

$$A = \sum_{i=0}^{n-1} sq^i g^i \in \mathbb{Z}_v[G],$$

and q is a primitive n^{th} root of unity in $\mathbb{Z}_v$.

Proof. We begin by examining Adams' construction for odd order $n = 2k+1$. Without scaling, we have

$$\sum_{i=0}^{2k-1} r^i g^i - (\frac{r^{2k} - r}{r^2 - 1}) g^{2k}$$

The last term is easily expanded to

$$-r\frac{r^{2k-2}+r^{2k-3}+\cdots+r+1}{r+1}$$

Thus A may be scaled minimally by $r+1$ to ensure integer entries. We therefore have a form of any odd order Adam's construction as

$$A=\sum_{i=0}^{2k-1} r^i(r+1)g^i-\left(r\sum_{i=0}^{2k-2} r^i\right)g^{2k}.$$

From here it is immediate that the sum weight of A is

$$v=\sum_{i=0}^{2k} r^i=\frac{r^{2k+1}-1}{r-1}.$$

Let $r=q$ be an integer of modulus greater than 1 and let $s=q+1$. Now the g^{n-1} coefficient of A satisfies

$$-q\sum_{i=0}^{2k-2} q^i\equiv sq^{2k}(mod\ v), \qquad \text{and}$$

$$A=\sum_{i=0}^{n-1} sq^ig^i\in\mathbb{Z}_v[G].$$

Clearly s is a particular root of x^n-s^n in $\mathbb{Z}_v[x]$, so we need only verify the claim that q is a primitive n^{th} root of unity in $\mathbb{Z}_v$. Since $q\neq\pm1$ it is clear that q^i is a distinct element of Z_v for $i=1,\ldots,n-1$. Finally, $q^n=(q-1)v+1$ and $q^n=1\in\mathbb{Z}_v$.

For even order $n=2k$, the last term is seen to be an integer since

$$\frac{r^{2k-1}-r}{r^2-1}=r^{2k-3}+\cdots+r^3+r,$$

so the sum weight becomes

$$v = \sum_{i=0}^{2k-2} r^i - \sum_{i=0}^{k-2} r^{2i+1} = \sum_{i=0}^{k-1} r^{2i}.$$

Now for $r = q$ as before, q is a primative n^{th} root of unity in $\mathbb{Z}_v$ and we again achieve

$$A = \sum_{i=0}^{n-1} q^i g^i \in \mathbb{Z}_v[G].$$

□

7.1. **The orders 4 and 5 cases.** The original motivation for this thesis was to determine if Adams construction provided for the complete family of full rate circulant MHMs and to explore other possible constructions of MHMs, including non-circulant and non-full rate examples. It was immediately clear from the computer search results that Adams construction is not in fact the complete family of FCMHMs. Through the manipulation of a construction technique for weighing matrices we were able to provide the doubling theorem, which extended an explanation for the existence of many even order MHMs, but unexplained examples in prime orders such as $n = 5$ and $n = 7$ continue to abound. It was in our search of an explanation for the existence results we have found that we first noticed the presence of a large family of MHMs that fit a specific form. As we have shown with Adams construction above, the coefficients of many full rate circulant results generate a polynomial with n^{th} roots when considered modulo the weight of the FCMHM. The following observations and conjecture could be a topic of further research on these objects, possibly leading to a new construction.

To begin, consider the circulant order 4 matrices with complex entries satisfying $HH^T = wI$, and let $A = a_0 + a_1 g + a_2 g^2 + a_3 g^3$ be such a generalized object. As noted by Adams et al. in [1], there are two constraining equations that A must satisfy to have mutually orthogonal columns:

$$a_0 a_1 + a_1 a_2 + a_2 a_3 + a_0 a_3 = 0$$

$$a_0 a_2 + a_1 a_3 = 0.$$

Without loss of generality, we may state that the former of the two conditions requires $a_1 = -a_3$, and note that given this condition the first equation is always satisfied. Then the remaining constraint is that

$$a_0 a_2 = -a_1^2,$$

and the sum weight of A will be $a_0 + a_2$. Hence we may construct a complex order 4 circulant matrix satisfying the general condition $HH^T = wI$ simply by taking any two numbers a_0 and a_1 that sum to w, and take the other two elements to be $\pm\sqrt{a_0 a_1}$. Clearly this implies that to attain such a matrix with integer entries, $a_0 a_1$ must be a perfect square, which leads to the following fact.

Remark 3. *Let p be a prime, $p \equiv 1 (mod\ 4)$. Then there exists a $CMHM(4, p^2)$, and similar to the observations regarding Adams construction, when the elements of the $CMHM(4, p^2)$ are taken to be roots of a polynomial in $\mathbb{Z}_p[x]$, this polynomial takes the form of $x^4 - \alpha \in \mathbb{Z}_p[x]$.*

The above can be shown to be true by construction. Consider the well-known theorem of Fermat from number theory that any prime congruent to one modulo four may be written as the sum of two squares. Then for any prime $p \equiv 1(mod\ 4)$, let $a^2 + b^2 = p$. It is trivial to verify that

$$A = a^2 + abg + b^2g^2 - abg^3$$

is a $CMHM(4, p^2)$. Observe also that

$$(x - a^2)(x - ab)(x - b^2)(x + ab) = x^4 - a^2b^2 \in \mathbb{Z}_p x.$$

The observations regarding these types of circulant MHMs may be able to give future construction results. Computer results support the possibility of a general construction for $CMHM(n, w)s$ whose elements are integer representatives of the roots of $x^n - \alpha \in \mathbb{Z}_w[x]$. In particular, the following has been verified for primes less than 10^4.

Conjecture 1. *There exists a $CMHM(5, p^2)$ for any prime $p \equiv 1\ (mod\ 5)$, and in particular there exists such of a form that its elements are integer representatives of the roots of $x^5 - \alpha \in \mathbb{Z}_p[x]$.*

Of course we should include that even this conjecture is not powerful enough to classify all prime weight circulant examples of order 5. While we have confirmed the existence of an $FCMHM(5, p^2)$ satisfying the conjecture for appropriate p up to the practical limits of computation, there are also examples of $FCMHM$s that occur with prime weights but are not the roots of such a polynomial. For example

we consider the $FCMHM(5, 71^2)$

$$M = 6 + 18g + 26g^2 + 54g^3 - 33g^4.$$

M is not an example that arises from the conjecture as we can see from the fact that

$$(x-6)(x-18)(x-26)(x-54)(x+33) = x^5 + 62x^2 + 26x + 60 \in \mathbb{Z}_{71}[x].$$

8. Applications

Hadamard matrices have had extensive applications in communications, error correcting codes, digital signal processing, and code division multiple access (CDMA) spreading systems [1], [15], [22]. While more research is required to determine the usefulness of multilevel Hadamard matrices in these areas, some work has already been done to apply these objects in an interesting way. The canonical application of an MHM involves considering an MHM as a particular type of multilevel sequence. We require some definitions, as seen in [13] and [10].

Definition 8. *The periodic autocorrelation function (PACF) of an integer valued sequence* $a = (a_0, a_1, \ldots, a_{n-1})$ *of length* n *is defined as*

$$R_a(T) = \sum_{i=0}^{n-1} a_i a_{i+T(mod\ n)}, \quad T = 0, 1, \ldots, n-1.$$

The periodic cross-correlation function (PCCF) of a *and another sequence* $b = (b_0, b_1, \ldots, b_{n-1})$ *of the same length is given by*

$$R_{ab}(T) = \sum_{i=0}^{n-1} a_i b_{i+T(mod\ n)}, \quad T = 0, 1, \ldots, n-1.$$

Finally, we define a perfect sequence as one for which its PACF is zero except for $T = 0$*, at which point* $R_a(0)$ *is called the energy of the sequence* a*. That is,*

$$R_a(T) = \begin{cases} E_a, & T = 0 \\ 0, & T \neq 0, \end{cases}$$

and $E_a = a_1^2 + a_2^2 + \cdots + a_{n-1}^2$*, what we have referred to as the weight for an MHM.*

It is quite trivial to see that the first row (or column) of any circulant MHM, when considered as a sequence, is in fact a perfect sequence. The advantage here is that using our knowledge of MHMs , we may generate multilevel perfect sequences for arbitrary n. However, it is desirable to have a restricted alphabet in application, and the energy of a sequence generated in this way could grow rapidly with increased n. It is relevant to note that MHMs may be easily converted into other types of matrices with similar properties, and these matrices in turn correspond to other types of perfect sequences.

For instance, let A be an $MHM(n, w^2)$. Simply scale by $\frac{1}{w}$ and $\frac{1}{w}A$ becomes a rational orthogonal matrix, from which we may generate a rational perfect sequence. Of course, the orthogonal matrices are simply real examples of unitary matrices. We include another definition, as given in [21].

Definition 9. *A complex Hadamard matrix* $H = [h_{i,j}]$ *is a square* $n \times n$ *matrix with complex entries satisfying* $|h_{i,j}| = 1$ *for* $i, j = 0, 1, \ldots n-1$*, and the property that*

$$HH^* = H^*H = nI_n,$$

*where * denotes the conjugate transpose of a complex matrix.*

Take any MHM, and let A be the corresponding orthogonal matrix. Then for any complex Hadamard matrix H, AH and HA are also complex Hadamard matrices. Complex Hadamard matrices are a topic of great study for their combinatorial interest and potential applications to many physical problems including quantum computing

and quantum information theory [21]. Of course as before we could easily use such a matrix to generate a complex perfect sequence.

The work of Trihn et al. in [22] used MHMs to build multilevel (specifically ternary) zero correlation zone (ZCZ) sequence sets, which have been useful in CDMA systems. We include their particular construction here and include a multilevel ZCZ sequence set achieved from their construction using some MHMs of our results.

Definition 10. *A multilevel zero correlation zone (ZCZ) sequence set is a set of multilevel sequences whose $PACF$ and $PCCF$ take on a value of 0 over a range of T. Such a family of sequences is denoted as $ZCZ(N, M, Z_{CZ})$ for N the size of each sequence in the set, M the number of sequences in the family, and Z_{CZ} the size of the zone for which the correlation functions are zero.*

The construction in [22] is as follows. Let n be fixed and $A = [a_{i,j}], B = [b_{i,j}]$ be two MHMs of order n. We will construct sets of sequences $\{u_r^{(m)}\}_{r=0}^{2n-1}$ for $2n$ sequences for $m \geq 0$. Define $I(a_r, b_s) = [a_{r,0}, b_{s,0}, \ldots, a_{r,n-1}, b_{s,n-1}]$, and for $m = 0, 0 \leq r \leq n-1$, let

$$u_{2r}^{(0)} = I([-a_r, a_r], [b_r, b_r]) \quad \text{and} \quad u_{2r+1}^{(0)} = I([a_r, -a_r], [b_r, b_r]).$$

Assume $\{u_r^{(m-1)}\}_{r=0}^{2n-1}$ has been constructed, then for $0 \leq r \leq n-1$,

$$u_{2r}^{(m)} = I([u_{2r}^{(m-1)}, u_{2r+1}^{(m-1)}]) \quad \text{and} \quad u_{2r+1}^{(m)} = I([u_{2r}^{(m-1)}, -u_{2r+1}^{(m-1)}]).$$

Then the sequence set $\{u_r^{(m)}\}_{r=0}^{2n-1}$ is a $ZCZ(n2^{m+2}, 2n, 2^m)$.

For example we will select $m = 3$, $n = 6$. Let

$$A = \begin{bmatrix} 1 & -8 & 9 & 5 & 4 & 3 \\ 3 & 1 & -8 & 9 & 5 & 4 \\ 4 & 3 & 1 & -8 & 9 & 5 \\ 5 & 4 & 3 & 1 & -8 & 9 \\ 9 & 5 & 4 & 3 & 1 & -8 \\ -8 & 9 & 5 & 4 & 3 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & -3 & 4 & -5 & 9 & 8 \\ 8 & 1 & -3 & 4 & -5 & 9 \\ 9 & 8 & 1 & -3 & 4 & -5 \\ -5 & 9 & 8 & 1 & -3 & 4 \\ 4 & -5 & 9 & 8 & 1 & -3 \\ -3 & 4 & -5 & 9 & 8 & 1 \end{bmatrix}.$$

The result of this construction is the multilevel $ZCZ(96, 12, 4)$ sequence set seen in Table 1. Included in the table are the autocorrelation $R_{0,0}(T)$ of $u_0^{(2)}$ and cross correlation $R_{0,i}(T)$ of $u_0^{(2)}$ with $u_i^{(2)}$.

9. Acknowledgements

I would like to thank the entire WSU Department of Mathematics and Statistics for their unbelievable support in the last two years, and my instructors for being so inspiringly passionate about what they do. Special gratitude is owed to Dr. Chen and Dr. Liu for participating in this committee, and for the support they have given me in my time here. I thank Dr. Dombrowski for every opportunity and honor that has been bestowed upon me, and for all the work she has done to ensure I meet the requirements of this program. I especially thank Dr. Arasu for his friendship, advice, and the passion with which he teaches. I am honored to have had him as an advisor, and feel incredibly lucky to have had the opportunity to work with such an amazing mentor.

I would also like to thank my family for their continued support and love, and my father for instilling a passion for knowledge and science in me many years ago, and for continuing to do so today.

I owe all of my success to the love of my life, Jessica, who has given me the confidence to pursue my dreams and the courage to challenge myself to be the best that I can be.

TABLE 1. Multilevel $ZCZ(96, 12, 4)$ sequence set

$u_0^{(2)} =$	(-1, -1, 1, -1, 1, 1, 1, -1, 8, 8, -8, 8, -3, -3, -3, 3, -9, -9, 9, -9, 4, 4, 4, -4, -5, -5, 5, -5, -5, -5, -5, 5, -4, -4, 4, -4, 9, 9, 9, -9, -3, -3, 3, -3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 5, 4, 4, -4, 4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8)
$u_1^{(2)} =$	(-1, 1, 1, 1, 1, -1, 1, 1, 8, -8, -8, -8, -3, 3, -3, -3, -9, 9, 9, 9, 4, -4, 4, 4, -5, 5, 5, 5, -5, 5, -5, -5, -4, 4, 4, 4, 9, -9, 9, 9, -3, 3, 3, 3, 8, -8, 8, 8, 1, -1, -1, -1, 1, -1, 1, 1, -8, 8, 8, 8, -3, 3, -3, -3, 9, -9, -9, -9, 4, -4, 4, 4, 5, -5, -5, -5, -5, 5, -5, -5, 4, -4, -4, -4, 9, -9, 9, 9, 3, -3, -3, -3, 8, -8, 8, 8)
$u_2^{(2)} =$	(-3, 3, -3, 8, 8, 8, -8, -1, -1, 1, -1, 1, 1, 1, -1, 8, 8, -8, 8, -3, -3, -3, 3, -9, -9, 9, -9, 4, 4, 4, -4, -5, -5, 5, -5, -5, -5, 5, -4, -4, 4, -4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 4, 4, -4, 4, 9, 9, 9, -9)
$u_3^{(2)} =$	(-3, 3, 3, 3, 8, -8, 8, 8, -1, 1, 1, 1, -1, 1, 1, 8, -8, -8, -8, -3, 3, -3, -3, -9, 9, 9, 9, 4, -4, 4, 4, -5, 5, 5, 5, -5, 5, -5, -5, -4, 4, 4, 4, 9, -9, 9, 9, 3, -3, -3, -3, 8, -8, 8, 8, 1, -1, -1, -1, 1, -1, 1, 1, -8, 8, 8, 8, -3, 3, -3, -3, 9, -9, -9, -9, 4, -4, 4, 4, 5, -5, -5, -5, -5, 5, -5, -5, 4, -4, -4, -4, 9, -9, 9, 9)
$u_4^{(2)} =$	(-4, -4, 4, -4, 9, 9, 9, -9, -3, -3, 3, -3, 8, 8, 8, -8, -1, -1, 1, -1, 1, 1, 1, -1, 8, 8, -8, 8, -3, -3, -3, 3, -9, -9, 9, -9, 4, 4, 4, -4, -5, -5, 5, -5, -5, -5, -5, 5, 4, 4, -4, 4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 5)
$u_5^{(2)} =$	(4, 4, 4, 9, -9, 9, 9, -3, 3, 3, 3, 8, -8, 8, 8, -1, 1, 1, 1, 1, -1, 1, 1, 8, -8, -8, -8, -3, 3, -3, -3, -9, 9, 9, 9, 4, -4, 4, 4, -5, 5, 5, 5, -5, 5, -5, -5, 4, -4, -4, -4, 9, -9, 9, 9, 3, -3, -3, -3, 8, -8, 8, 8, 1, -1, -1, -1, 1, -1, 1, 1, -8, 8, 8, 8, -3, 3, -3, -3, 9, -9, -9, -9, 4, -4, 4, 4, 5, -5, -5, -5, -5, 5, -5, -5)
$u_6^{(2)} =$	(-5, -5, 5, -5, -5, -5, -5, 5, -4, -4, 4, -4, 9, 9, 9, -9, -3, -3, 3, -3, 8, 8, 8, -8, -1, -1, 1, -1, 1, 1, -1, 8, 8, -8, 8, -3, -3, -3, 3, -9, -9, 9, -9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 5, 4, 4, -4, 4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4)
$u_7^{(2)} =$	(-5, -5, 5, -5, -5, -5, -5, 5, -4, -4, 4, -4, 9, 9, 9, -9, -3, -3, 3, -3, 8, 8, 8, -8, -1, -1, 1, -1, 1, 1, -1, 8, 8, -8, 8, -3, -3, -3, 3, -9, -9, 9, -9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 5, 4, 4, -4, 4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4)
$u_8^{(2)} =$	(5, 5, 5, -5, 5, -5, -5, -4, 4, 4, 4, 9, -9, 9, 9, -3, 3, 3, 3, 8, -8, 8, 8, -1, 1, 1, 1, 1, -1, 1, 1, 8, -8, -8, -8, -3, 3, -3, -3, -9, 9, 9, 9, 4, -4, 4, 4, 5, -5, -5, -5, -5, 5, -5, -5, 4, -4, -4, -4, 9, -9, 9, 9, 3, -3, -3, -3, 8, -8, 8, 8, 1, -1, -1, -1, 1, -1, 1, 1, -8, 8, 8, 8, -3, 3, -3, -3, 9, -9, -9, -9, 4, -4, 4, 4)
$u_9^{(2)} =$	(-9, -9, 9, -9, 4, 4, 4, -4, -5, -5, 5, -5, -5, -5, -5, 5, -4, -4, 4, -4, 9, 9, 9, -9, -3, -3, 3, -3, 8, 8, 8, -8, -1, -1, 1, -1, 1, 1, 1, -1, 8, 8, -8, 8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 5, 4, 4, -4, 4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3)
$u_{10}^{(2)} =$	(-9, 9, 9, 9, 4, -4, 4, 4, -5, 5, 5, 5, -5, 5, -5, -5, -4, 4, 4, 4, 9, -9, 9, 9, -3, 3, 3, 3, 8, -8, 8, 8, -1, 1, 1, 1, 1, -1, 1, 1, 8, -8, -8, -8, -3, 3, -3, -3, 9, -9, -9, -9, 4, -4, 4, 4, 5, -5, -5, -5, -5, 5, -5, -5, 4, -4, -4, -4, 9, -9, 9, 9, 3, -3, -3, -3, 8, -8, 8, 8, 1, -1, -1, -1, 1, -1, 1, 1, -8, 8, 8, 8, -3, 3, -3, -3)
$u_{11}^{(2)} =$	(8, 8, -8, 8, -3, -3, -3, 3, -9, -9, 9, -9, 4, 4, 4, -4, -5, -5, 5, -5, -5, -5, -5, 5, -4, -4, 4, -4, 9, 9, 9, -9, -3, -3, 3, -3, 8, 8, 8, -8, -1, -1, 1, -1, 1, 1, 1, -1, -8, -8, 8, -8, -3, -3, -3, 3, 9, 9, -9, 9, 4, 4, 4, -4, 5, 5, -5, 5, -5, -5, -5, 5, 4, 4, -4, 4, 9, 9, 9, -9, 3, 3, -3, 3, 8, 8, 8, -8, 1, 1, -1, 1, 1, 1, 1, -1)
$R_{0,0}(T) =$	(3136, 0, 0, 0, 0, -12, 0, 12, -48, 12, 0, -12, 0, 80, 0, -80, 320, -80, 0, 80, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, -80, 0, 80, -320, 80, 0, -80, 0, 12, 0, -12, 48, -12, 0, 12, 0, -784, 0, 784, 0, 784, 0, -784, 0, 12, 0, -12, 48, -12, 0, 12, 0, -80, 0, 80, -320, 80, 0, -80, 0, 0, 0, 0, 0, 0, 0, 0, 0, 80, 0, -80, 320, -80, 0, 80, 0, -12, 0, 12, -48, 12, 0, -12, 0, 0, 0, 0)
$R_{0,i}(T) =$	(0, 0, 0, 0, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, x, x, x, x, x, x, x, 0, 0, 0, 0)

TABLE 2. Adams construction examples

Order	First row	r	s	sumweight
3	(28, 21, -12)	3/4	28	w=37
	(10, 15, -6)	3/2	10	w=19
	(3, 6, -2)	2	3	w=7
	(14, 35, -10)	5/2	14	w=39
	(4, 12, -3)	3	4	w=13
	(18, 63, -14)	7/2	18	w=67
	(5, 20, -4)	4	5	w=21
	(6, 30, -5)	5	6	w=31
4	(16, 12, 9, -12)	3/4	16	w=25
	(4, 6, 9, -6)	3/2	4	w=13
	(1, 2, 4, -2)	2	1	w=5
	(4, 10, 25, -10)	5/2	4	w=29
	(1, 3, 9, -3)	3	1	w=10
	(4, 14, 49, -14)	7/2	4	w=53
	(1, 4, 16, -4)	4	1	w=17
	(1, 5, 25, -5)	5	1	w=26
5	(448, 336, 252, 189, -444)	3/4	448	w=781
	(40, 60, 90, 135, -114)	3/2	40	w=211
	(3, 6, 12, 24, -14)	2	3	w=31
	(56, 140, 350, 875, -390)	5/2	56	w=1031
	(4, 12, 36, 108, -39)	3	4	w=121
	(72, 252, 882, 3087, -938)	7/2	72	w=3355
	(5, 20, 80, 320, -84)	4	5	w=341
	(6, 30, 150, 750, -155)	5	6	w=781
6	(256, 192, 144, 108, 81, -300)	3/4	256	w=481
	(16, 24, 36, 54, 81, -78)	3/2	16	w=133
	(1, 2, 4, 8, 16, -10)	2	1	w=21
	(16, 40, 100, 250, 625, -290)	5/2	16	w=741
	(1, 3, 9, 27, 81, -30)	3	1	w=91
	(16, 56, 196, 686, 2401, -742)	7/2	16	w=2613
	(1, 4, 16, 64, 256, -68)	4	1	w=273
	(1, 5, 25, 125, 625, -130)	5	1	w=651

TABLE 3. $x^5 - \alpha \in \mathbb{Z}_p$ circulant MHMs for primes p less than 1000

First row	a primitive 5^{th} root	α	prime sumweight
(-4 -1 8 2 6)	3	10	11
(-14 24 12 6 3)	2	26	31
(-22 26 14 17 6)	10	27	41
(-18 -2 54 6 21)	9	29	61
(-12 -16 26 11 62)	5	23	71
(-43 -4 56 24 68)	36	87	101
(-64 68 26 87 14)	53	69	131
(-69 52 114 6 48)	8	75	151
(-27 -48 156 36 64)	42	49	181
(-48 -46 131 38 116)	39	155	191
(-114 60 135 40 90)	55	12	211
(-42 -39 222 34 66)	87	176	241
(-49 -22 236 24 62)	20	151	251
(-156 147 96 118 66)	10	113	271
(-94 -30 110 65 230)	86	37	281
(-178 116 176 74 123)	6	165	311
(-144 52 18 159 246)	64	220	331
(-156 -4 113 116 332)	39	179	401
(-150 -54 250 90 285)	252	310	421
(-4 -118 398 104 51)	95	269	431
(-64 -100 420 80 125)	88	14	461
(-106 -124 383 96 242)	101	288	491
(-100 -4 500 20 105)	25	18	521
(-312 264 276 141 172)	48	316	541
(-306 132 111 288 346)	106	401	571
(-191 -102 342 126 426)	32	97	601
(-66 -197 282 96 516)	228	504	631
(-34 -106 122 41 618)	357	579	641
(-374 333 186 354 162)	197	77	661
(-345 160 66 390 420)	89	108	691
(-274 -58 438 149 446)	89	47	701
(-333 526 396 24 138)	80	522	751
(-4 -268 308 89 636)	67	498	761
(-321 316 78 666 72)	212	581	811
(-58 -307 654 206 326)	51	713	821
(-30 -295 770 230 206)	268	623	881
(-412 371 672 14 266)	19	334	911
(-228 -184 776 164 413)	349	739	941
(-208 -12 74 191 926)	65	715	971
(-125 -180 930 150 216)	160	296	991

References

[1] Adams, Sarah Spence; Crawford, Matthew; Greeley, Caitlin; Lee, Bryce; Murugan, Mathav Kishore *Multilevel and multidimensional Hadamard matrices*. Des. Codes and Cryptogr. 51 (2009), no. 3, 245 - 252.

[2] Ang, Miin Huey; Arasu, K. T.; Lun Ma, Siu; Strassler, Yoseph *Study of proper circulant weighing matrices with weight 9*. Discrete Math. 308 (2008), no. 13, 2802-2809.

[3] Arasu, K. T.; Dillon, J. F.; Jungnickel, Dieter; Pott, Alexander *The Solution of the Waterloo Problem*. J. Combin. Theory Ser. A 71 (1995), no. 2, 316 - 33.

[4] Arasu, K. T.; Gutman, Alex J. *Circulant weighing matrices*. Cryptogr. Commun. 2 (2010), no. 2, 155-171.

[5] Arasu, K. T.; Hollon, J.R. *Group weighing matrices* (2010), Preprint.

[6] Arasu, K.T.; Kotsireas, I. S.; Koukouvinos, C.; Seberry, Jennifer *On circulant and two-circulant weighing matrices*. Australas. J. Combin. 48 (2010), 43-51.

[7] Arasu, K. T.; Leung, Ka Hin; Ma, Siu Lun; Nabavi, Ali; Ray-Chaudhuri, D. K. *Circulant matrices of weight* 2^{2t}. Des. Codes Cryptogr. 41 (2006), no. 1, 111-123.

[8] Arasu, K. T.; Ray-Chaudhuri, D. K. *Multiplier theorem for a difference list*. Ars Combin. 22 (1986), 119-137.

[9] Beth, Thomas; Jungnickel, Dieter; Lenz, Hanfried *Design Theory*. Vol. I, Second edition. Encyclopedia of Mathematics and its Applications, 69. Combridge University Press, Cambridge, 1999.

[10] Geramita, Anthony V.; Seberry, Jennifer *Orthogonal Designs. Quadratic forms and Hadamard matrices*. Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York, 1979.

[11] Hall, Marsharl, Jr. *Combinatorial theory*. Second edition. Wiley-Interscience series in Discrete Mathematics. A Wiley-Interscience Publication. John Wiley and Sons, Inc. NewYork, 1986.

[12] Lander, Eric S. *Symmetric designs: an algebraic approach*. London Mathematical Society Lecture Note series, 74. Cambridge University Press, Cambridge, 1983.

[13] Li, X.D.; Fan, P.Z.; Mow, W.H.; Darnell, M *Multilevel perfect sequences over integers*. Electron. Lett. **47** (2011), no. 8, 496-497.

[14] Mann, H. B. *Balanced incomplete block designs and Abelian difference sets*. Illinois J. Math. **8** 1964 252-261.

[15] Matsufuji, Shinya; Fan, Pingzhi *Constructions of factorizable multilevel hadamard matrices.* IEICE Transactions 92-A (12): 3404-3406 (2009).

[16] McFarland, Robert Lee; *On multipliers of abelian difference sets*. Thesis (Ph. D.)-The Ohio State University. 1970. 89 pp

[17] McFarland, Robert L.; Rice, Bart F. *Tranaslates and multipliers of abelian difference sets*. Proc. Amer. Math. Soc. **68** (1978), no. 3, 375-379.

[18] Parker, Keli *On the Construction of Order Six Multilevel Hadamard Matrices*, Elec. Proc. Und. Math. Day, Vol 5 (2010), No. 5, 1–5.

[19] Pott, Alexander *Finite geometry and character theory*. Lecture Notes in Mathematics, 1601. Springer-Verlag, Berlin, 1995.

[20] Schmidt, Bernhard *Characters and cyclotomic fields in finite geometry*. Lecture Notes in Mathematics, 1797. Springer-Verlag, Berlin, 2002.

[21] Szöllősi, Ferenc *Parametrizing complex Hadamard matrices*. European J. Combin. 29 (2008), no. 5, 1219-1234.

[22] Trinh, Q. K.; Fan, P.; Gabidulin, E. M., *Multilevel Hadamard matrices and zero correlation zone sequences*. Electron. Lett. **42** (2006), no. 13, 748-750.