Winter 1998

Error-Correcting Codes Associated With Generalized Hadamard Matrices Over Groups

Iem H. Heng
Old Dominion University

ERROR CORRECTING CODES ASSOCIATED WITH GENERALIZED HADAMARD MATRICES OVER GROUPS

by

Iem H. Heng
M.S. April 1995, Western Michigan University
B.S. May 1993, Columbia University
B.S. May 1991, Providence College

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirement for the Degree of

DOCTOR OF PHILOSOPHY

COMPUTATIONAL AND APPLIED MATHEMATICS

OLD DOMINION UNIVERSITY
December 1998

Approved by:

Charlie H. Cooke (Director)

John M. Dorrepaal (Member)

Hideaki Kaneko (Member)

Linda L. Vahala (Member)

ABSTRACT

ERROR CORRECTING CODES ASSOCIATED WITH
GENERALIZED HADAMARD MATRICES OVER GROUPS

Iem H. Heng
Old Dominion University, 1998
Director: Dr. Charlie H. Cooke

Classical Hadamard matrices are orthognal matrices whose elements are ± 1. It is well-known that error correcting codes having large minimum distance between codewords can be associated with these Hadamard matrices. Indeed, the success of early Mars deep-space probes was strongly dependent upon this communication technology.

The concept of Hadamard matrices with elements drawn from an Abelian group is a natural generalization of the concept. For the case in which the dimension of the matrix is q and the group consists of the p-th roots of unity, these generalized Hadamard matrices are called "Butson Hadamard Matrices $BH(p,q)$". first discovered by A.T. Butson [6].

In this dissertation it is shown that an error correcting code whose codewords consist of real numbers in finite Galois field $Gf(p)$ can be associated in a simple way with each Butson Hadamard matrix $BH(p,q)$, where $p > 0$ is a prime number. Distance properties of such codes are studied, as well as conditions for the existence of linear codes, for which standard decoding techniques are available.

In the search for cyclic linear generalized Hadamard codes, the concept of an M-invariant infinite sequence whose elements are integers in a finite field is introduced. Such sequences are periodic of least period, T, and have the interesting property that

arbitrary identical rearrangements of the elements in each period yields a periodic sequence with the same least period. A theorem characterizing such M-invariant sequences leads to discovery of a simple and efficient polynomial method for constructing generalized Hadamard matrices whose core is a linear cyclic matrix and whose row vectors constitute a linear cyclic error correcting code.

In addition, the problem is considered of determining parameter sequences $\{t_n\}$ for which the corresponding potential generalized Hadamard matrices $BH(p, pt_n)$ do not exist. By analyzing quadratic Diophantine equations, new methods for constructing such parameter sequences are obtained. These results show the rich number theoretic complexity of the existence question for generalized Hadamard matrices.

To my mother Teang Keo, my aunt Dy Keo

and my surrogate mother Bernadette Mernin

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Charlie H. Cooke, who influenced my decision to work in the area of error correcting codes associated with generalized Hadamard matrices. This is an area which is rich in both interesting theories and applications. I am very grateful for my advisor's many helpful insights and thoughtful suggestions. His virtues of patience, encouragement, understanding and untiring efforts will long be remembered.

I would also like to thank Dr. John M. Dorrepaal, Dr. Hideaki Kaneko and Dr. Linda L. Vahala for serving on my committee. In addition, I am very grateful that they carefully read my dissertation and offered thoughtful comments and suggestions.

I would like to thank my mother, my aunt and my surrogate mother for their encouragement and support during my stay in graduate school. I would also like to thank my sisters Gucely and Gucemuy, my brothers Kia, Kimseng and Tong and my brother-in-laws Kimleng and Neing for encouraging and standing by me.

I would like to express to the faculty and staff of the mathematics department my appreciation for their outstanding support. First, I would like to thank Barbara Jeffrey, Gail Tuckelson and Dr. Rao Chaganty for their assistance with Tex and Latex. Next, I would like to thank Dr. John Heinbockel and Dr. John Swetits for their assistance in helping me to succeed with my graduate studies, by always being available to answer my questions.

Last, I would like to thank my good friends Eilen Biancuzzo, Jeffrey Hoag, Judith Jamieson and Jim Tattersall who encouraged me to pursue my goal of obtaining a Ph.D. degree in applied mathematics. Without their help in the past, I would not be where I now am. I am very fortunate to have these friends.

Contents

1 Introduction **1**

1.1 Hadamard Matrices 1

1.2 Existence of Hadamard Matrices 3

1.3 Statement of Purpose 4

1.4 Basic Literature Survey 5

1.5 Outline of Procedure 9

2 Criteria for Non-Existence of Generalized Hadamard Matrices **11**

2.1 Introduction 11

2.2 Preliminary Considerations 12

2.3 Hadamard Matrices Over Groups 13

2.4 The Imbedding Problem 16

2.5 Quadratic Diophantine Equations 19

2.6 Reciprocity 20

2.7 **Summary** 28

3 Error Correcting Codes Associated With Complex Hadamard Matrices Over Groups **30**

3.1 Introduction 30

3.2 Ternary Hadamard Codes 32

3.3 Vectors Over C_p 35

3.4 Exponent Generation By Direct Sum 37

3.5 Linear Hadamard Codes 38

3.6 Summary 42

4 Polynomial Construction Of Complex Hadamard Matrices With Cyclic Core **44**

4.1 Introduction 44

4.2 M-Sequences 45

4.3 Cyclic Hadamard Codes 48

4.4 Polynomial Construction Algorithm 50

4.5 Computer-Aided Construction of Polynomial Pairs 52

5 M-Sequences and Circulant Matrices **55**

5.1 Review of the Theory of m-Sequences 55

5.2 Classification of Circulant Matrices Over $Gf(q)$ 57

5.3 The Relation Between m-Sequences and M-Sequences 60

6 Summary and Conclusions **64**

6.1 Directions of Future Research 65

REFERENCES 67

Appendix 1: Non-Quadratic Residues 72

Appendix 2: Computer Program for Finding the Generator Polynomial of a Cyclic Code 74

Vita 79

List of Tables

1 (3,7,15)-Difference Matrix 18

2 (3,8,15)-Difference Matrix 18

3 Reciprocal Pairs 24

4 Hadamard Matrix $H(3,6) = x^Q$ 33

5 Hadamard Matrix $H(3,9) = x^D$ 34

6 Hadamard Exponent 38

7 Generating Matrix For $K(3,27)$ 41

8 Parity Check Polynomials 53

9 Coefficients of Generating Polynomials 54

Chapter 1

Introduction

1.1 Hadamard Matrices

The matrix $H = H(q, r)$ is a Hadamard matrix in the classical sense provided

- H is of dimension $r \times r$.
- The elements of H are ± 1.
- $H \cdot H^T = H^T \cdot H = rI_r$, where H^T is the transpose of H.

There is a long history of the theory of such matrices, with applications in algebraic coding theory, combinatorial design, and weights and measures [13], [17], [30], [31], [32] and [33]. Reference [33] contains an in-depth survey of these interesting matrices.

A first generalization of the concept was discovered by A.T. Butson [5], who defined what is called a "Butson Hadamard matrix $BH(q, r)$" having the following attributes:

The journal used as a model for this dissertation is Applied Math Letters.

• $H = BH(q, r)$ has dimension $r \times r$.

• The elements of H are q-th roots of unity, which lie in the cyclic group

$G = \{1, w, w^2, ..., w^{q-1} : w^q = 1\}$.

• $H \cdot H^* = H^* \cdot H = rI_r$, where H^* is the conjugate transpose of H.

Clearly, the case $q = 2$ represents the classical Hadamard matrices.

In this dissertation interest is directed to the case in which q is a prime number greater than two. A generalization of the concept which encompasses both the classical case and the complex Butson Hadamard matrices $BH(q, r)$ is that of generalized Hadamard matrices over general Abelian group G [6]. Such matrices are denoted by $GH(g, \lambda)$ or $GH(G, n)$, $n = g\lambda$, and have the following attributes:

• $H = GH(g, \lambda)$ has dimension $n \times n$, where $n = g\lambda$.

• The elements of $H = GH(g, \lambda)$ are members of Abelian group G,

whose order is $|G| = g$.

• Homogeneity-Under group operation $\ominus$, the vector difference of two arbitrary rows of H satisfies a uniformity property: Each element of the group G appears λ times.

Observe that for multiplicative groups, the analogy of an element difference is $a - b \longleftrightarrow ab^{-1}$. Clearly, when $H = GH(g, \lambda)$ has elements drawn from the complex cylic group $C_p = \{1, w, w^2, ..., w^{p-1} : w^p = 1\}$, then $H = BH(g, g\lambda)$ is also Butson Hadamard.

Generalized Hadamard matrices have been studied by several authors[Brock [4], Butson [5] and [6], Dawson [9], de Launey [10], [11] and [12], Drake [13], Jungnickel [17], Street [33]]. Brock and Street use the following definition or some closely related form:

A generalized Hadamard matrix $H = GH(\lambda s, G)$ over the group G of order s is a $\lambda s \times \lambda s$ matrix $H = [h_{ij}]$ whose elements satisfy

(i) $h_{ij} \in G$ for all $1 \leq i, j \leq \lambda s$,

(ii) $\sum_{k=1}^{\lambda s} h_{ik} h_{jk}^{-1} = \sum_{g \in G} \lambda g$ whenever $i \neq j$, where the summation is in the group ring associated with G.

Certainly, if G is the additive group from a finite field, $\sum_{g \in G} g = 0$. Thus, Brock's definition amounts to a slight generalization of the previous. In the present work, Brock's generalization will not be a major concern.

1.2 Existence of Hadamard Matrices

It is known [22] that a necessary condition for existence of the classical Hadamard matrices $BH(2, r)$ is that $r = 1, 2$, or a multiple of $4k$, where $k > 0$ is an integer. It is a demonstrated fact [24] that $BH(2, 4k)$ exists for each $0 < k \leq 106$, and a classical Hadamard conjecture is that existence occurs for all integers $k > 0$. No counter example to this conjecture is presently known.

For primes $p > 2$, the situation is quite different. Butson [6] establishes that a necessary condition for existence of $H = BH(p > 2, r)$ is that $r = pt$, where $t > 0$ is an integer. The condition is also sufficient [5], for the special case of $BH(p > 2, 2^m p^k)$, provided $0 \leq m \leq k$, where $k \geq 1$ and m are integers.

It has been conjectured fairly recently [3] that $BH(p, pt)$ exists for all primes $p > 2$ whenever $t > 0$ is an integer. However, instances previously have been

discovered where this generalized Hadamard conjecture fails [7]. The most recent generalized Hadamard conjecture [10] which appears to have merit is that $BH(p,n)$ exists only if I_n is Hermitian congruent to nI_n, where $n = pt$.

As the circumstances for non-existence of generalized Hadamard matrices are not completely known, one aim of this dissertation will be to obtain parameter sequences $\{t_n\}$ for which the corresponding potential generalized Hadamard matrices $BH(p, pt_n)$ fail to exist.

1.3 Statement of Purpose

The investigations of this dissertation are directed to the general case of Hadamard matrices over groups, with special consideration given to the question of non-existence, in general, and applications, in particular to the area of algebraic coding theory.

The first focus of interest is directed to techniques for constructing parameter sequences $\{r_k\}$ such that the infinite sequence of potential generalized Hadamard matrices $BH(q, r_k)$ can be proven non-existent for $k \in K$, where K is a countably infinite set. Techniques exploited consist chiefly of methods for proving non-existence of nontrivial integer solutions to homogeneous Diophantine equations

$$ax^2 + by^2 + cz^2 = 0. \tag{1.3.1}$$

The second area of emphasis is application of Butson's Hadamard matrices to the discipline of algebraic coding theory. It is shown that for primes $p > 0$ an error

correcting code whose codewords consist of real numbers drawn from a finite Galois field $Gf(p)$ can be associated in a simple way with each existing Butson Hadamard matrix $BH(p, pt)$. Distance properties of these codes, as well as conditions for existence of linear codes, are investigated. By introducing the concept of an M-invariant periodic infinite sequence whose elements are integers in a finite field, an efficient polynomial method for constructing Hadamard matrices which possess an associated linear cyclic code is made posssible.

1.4 Basic Literature Survey

Although necessary conditions for existence are known, for given integers q and r there are no general methods for proving non-existence of generalized Hadamard matrix $BH(q, r)$. However, there are several parameter dependent methods for investigating specific cases. A.T. Butson [5] determined that for primes $p > 2$ a necessary condition for the existence of $BH(p > 2, r)$ is that $r = pt$, where t is a positive integer. In addition, he showed the condition is sufficient for the existence of Hadamard matrix $BH(p > 2, 2^m p^k)$, provided $0 \leq m \leq k$, where $k \geq 1$ and m are non-negative integers. Existence or non-existence for the case $m > k$ is generally an open question.

Butson [6] subsequently established that the existence of a generalized Hadamard matrix $H(p, r)$ is equivalent to the existence of Hadamard exponent matrix, E, whose elements are in Galois field $Gf(p)$. Here, if H is written in standard form, then the first row and first column of E are all zero. Without the first row and first column

of E, the remaining elements constitute a square submatrix, E_c, called the core of H. In order to determine a cyclic core E_c for the case where $H(p, p^n)$ is considered, Butson introduced the concept of constructing a relative difference set. He showed that the existence of a relative difference set is equivalent to the existence of cyclic matrix E_c which constitutes a cyclic core for matrix $H(p, p^n)$. However, Butson's method for constructing cyclic matrix E_c by means of a relative difference set is not very practical as matrix size increases. In the present dissertation, a polynomial method is introduced for constructing a cyclic matrix in an efficient manner.

Whereas Butson studies the concept of the existence of Hadamard matrices, Warwick de Launey [10] focused upon a method for establishing non-existence. He was able to exploit the number theoretic character of the Hadamard determinant to establish non-existence in certain special cases, for groups whose orders are divisible by 3, 5 or 7. In particular, the $GH(3,5)$, $GH(5,3)$ and $GH(15,1)$ do not exist.

Moreover, de Launey [11] established that the existence of generalized Hadamard matrices $GH(n, G)$ developed modulo N is equivalent to the existence of a solution to a certain equation over the group ring of $G \times N$ over the integers. Here, G and N are finite groups of order $|G| = g$ and $|N| = n$, respectively. These matrices are equivalent to relative difference sets, $RDS(g, n, n, 0, n/g)$, modulo the direct sum of N and G. By analyzing $GH(q, EA(q))$ developed modulo $EA(q)$, and $GH(q^2, G)$ devloped modulo $EA(q^2)$, where q is an odd integer and $EA(q)$ denotes the elementary Abelian group of order q, he was able to come up with some non-existence results. Indeed, in all but 15 of the 108 cases with $n \leq 50$, the existence of a $GH(n, EA(q))$,

developed modulo $EA(n)$, is either proved or disproved.

Furthermore, de Launey [12] determined that for Abelian groups G, only group Hadamard matrices of type p^s for $C_p \times ... \times C_p$ exist. A group Hadamard matrix H is a generalized Hadamard matrix whose rows and columns form a group. He also defined a group Hadamard matrix as reducible if there exist two group Hadamard matrices of smaller order such that H is equivalent to $H_1 \otimes H_2$, denoted as $H \sim H_1 \times H_2$; otherwise the group Hadamard matrix is said to be irreducible. Two generalized Hadamard matrices over an Abelian group G are said to be equivalent if one can be obtained from the other by permuting the rows and columns or multiplying rows and columns by element of G. Through de Launey's concept of irreducibility, he is able to count what he calls the $p(m,t)$-Hadamard matrices.

On the other hand, Bradley W. Brock [4] generalized the Witt cancellation law for Hermitian congruence and theorems of Hall and Ryser [14] to matrices whose elements are members of a general Abelian group. The matrix equation

$$H \cdot H^* = H^* \cdot H = mI_n + \mu J_n \tag{1.4.2}$$

is investigated. Here, H^* is a conjugate transpose of H of order m, J_n is a square matrix whose elements are all 1's, and μ is an integer. He obtains a necessary condition for the existence of a nonsingular matrix H of order m such that $H \cdot H^* = mI_n + \mu J_n$. With $m = n$ and $\mu = 0$, Brock's results yield a non-existence theorem for certain generalized Hadamard matrices, particularly those of the Butson type.

Deborah J. Street [33] analyzed the connections between generalized Hadamard

matrices, orthogonal arrays and F-squares. By combining known orthogonal arrays associated with generalized Hadamard matrices, several results of Shrikhande [32] are extended. In addition, established sets of mutually orthogonal F-squares emerge.

Motivated by an example of Rajkundlia [28] on balanced incomplete block designs(BIBD), Jennifer Seberry [30] was able to construct mutually orthogonal F-squares from generalized Hadamard matrices. First, for the case where p^r and $p^r - 1$ are both prime powers, with r being an integer, there is a generalized Hadamard matrix of order $p^r(p^r - 1)$ with elements from the elementary Abelian group $Z_p \times ... \times Z_p$. This result is then used to produce $p^r - 1$ mutually orthogonal F-squares $F(p^r(p^r - 1); p^r - 1)$.

Jennifer Seberry and H. Kharaghani [19] have investigated the excess of complex Hadamard matrices. The excess of a complex Hadamard matrix can be obtained as follows: Let $H = [h_{ij}]$ be a complex Hadamard matrix of order n with elements 1, -1, i, $-i$ which satisfies $H \odot H^* = nI_n$, where H^* is the conjugate transpose of H. Then the excess of H, denoted as $\sigma(H)$, is the sum of all entries of H. In mathematical terms, if $S(H) = \sum_{ij} h_{ij}$, then $\sigma(H) = |S(H)|$ is the excess of H. As an application there emerges many real Hadamard matrices of large excess and new clsses of Hadamard matrices of maximum excess.

Furthermore, with W. Holzmann, H. Kharaghani [16] investigated an infinite class of Hadamard matrices of order n, where $n - 4$ is a perfect square, with an excess of $n\sqrt{n-4}$. An exhaustive computer search indicates that for $n = 40$, the corresponding matrix constructed has the maximum possible excess in its Hadamard equivalence class. The key to success of this exhaustive computer search is start-

ing the construction using different Golay sequences [34]. There emerges various interesting classes of Hadamard matrices.

Following up with the idea of a Golay sequence, H. Kharaghani [18] went further to construct the class of Hadamard matrices, with order $(r+4^n+1)4^{n+1}m^2$, by using the concept of block Golay sequences. Here, $2^n m$ is the order of Hadamard matrix and r is the length of a Golay sequence, where m and n are block size and length of block Golay sequence, respectively. This provides more results on many regular complex Hadamard matrices and Hadamard matrices of new order.

1.5 Outline of Procedure

The purposes of this dissertation are two-fold: First, to determine methods for proving non-existence of generalized Hadamard matrices, and second, to investigate error correcting codes which can be associated with certain generalized Hadamard matrices of Butson.

In Chapter 2, the subject of generalized Hadamard matrices over groups is introduced. The aim in this chapter is to investigate methods for establishing that certain parameter sequences $\{t_n\}$ lead to non-existence of corresponding generalized Hadamard matrices $GH(s, t_n)$ over group G of order s. This work complements Warwick de Launey's approach to non-existence by way of number theoretic properties of the Hadamard determinant [10]. The two investigations, whereas neither is exhaustive of all possibilities, together reveal the rich number theoretic complexity of this existence problem.

The aim of Chapter 3 is to investigate error correcting codes which can be associated with generalized Hadamard matrices by means of the Hadamard exponent matrix. In many cases where D is a difference matrix, for appropriate variable x

$$H = x^D \tag{1.5.3}$$

is a generalized Hadamard matrix, where the row vectors of D form an error correcting code. Both linear and nonlinear such codes are possible. It is desirable to determine exactly when linear codes occur.

In Chapter 4 the task is considered of constructing generalized Hadamard matrices whose exponent matrix, D, has a cyclic core and whose row vectors constitute a linear cyclic error correcting code. For such cases the task of decoding becomes particularly simple. By introducing the concept of an M-invariant sequence over a finite field, a theorem which characterizes such sequences aids in determining a simple polynomial method for constructing generalized Hadamard matrices with cyclic core. Having the polynomial in hand also allows one to determine readily which relative difference set is associated with the particular Hadamard matrix, although this concept will not be explored fully.

In Chapter 5 the task is to introduce the concept of M-sequences and circulant matrices. After reviewing the basic properties and theorems stated in Zierler [37], it is established that every m-sequence is M-invariant. Moreover, because Butson [6] does not give a clear explanation or definition of what the cyclic core of a Hadamard matrix is, a precursory study of circulant matrices is accomplished.

Chapter 2

Criteria for Non-Existence of Generalized Hadamard Matrices

2.1 Introduction

In this chapter attention is focused upon the question of non-existence for generalized Hadamard matrices over groups. A well-known conjecture of Brock [4] states that generalized Hadamard matrix $GH(p, h)$ over group G of prime order p exists only if the matrices I_n and nI_n are Hermitian congruent, where $n = ph$. The CRC Handbook of Combinatorial Design, 1996 edition, documents some parameter values for which non-existence is known to occur. Here, methods for establishing the lack of solutions to quadratic Diophantine equations are used to prove non-existence of $GH(p, h)$ for various parameter sequences. The methods exploited complement Warwick de Launey's approach to non-existence via number theoretic properties of the Hadamard determinant, which is published in *J. Stat. Plann. and Infer-*

ence, Volume 11, pages 103-110, (1985). Neither investigation is exhaustive of all possibilities.

2.2 Preliminary Considerations

Let C_s be the multiplicative group of all complex s^{th} roots of unity. The square matrix $H = [h_{ij}]$ of order r over C_s is said to be a "*Butson Hadamard matrix*", briefly a $BH(s,r)$ matrix, if and only if $HH^* = rI_r$. Here, H^* is the conjugate transpose of H.

$BH(2,r)$ matrices are referred to simply as Hadamard matrices (or ± 1 matrices). Such matrices exist only if $r = 1, 2$ or else $r = 4k$, where k is a positive integer. Existence has been verified for at least each and every $k \leq 106$, and the classical Hadamard conjecture states that existence occurs for each integer $k > 0$.

For primes $p > 2$, the situation is quite different. A necessary condition for the existence of $BH(p > 2, r)$ is that $r = pt$, where t is a positive integer. This condition is also sufficient, for the case of $BH(p > 2, 2^m p^k)$, provided $0 \leq m \leq k$, where k is an integer [6].

It has been conjectured [3] that $BH(p, pt)$ exists, for primes $p > 2$ and all positive integers t. However, instances have been discovered where this conjecture fails [7]. The most recent generalized Hadamard conjecture[6] of any merit is that $H(p,n)$ exists only if I_n is Hermitian congruent to nI_n, where $n = pt$.

In this chapter techniques are explored for proving non-existence of infinite sequences of potential $BH(s, r_k)$, $k \in K$, where K is a countably infinite set of positive

integers. Sets K are identified for which $\{BH(s, r_k) : k \in K\} = \phi$. These techniques consist chiefly of methods for proving non-existence of nontrivial solutions to homogeneous Diophantine equations

$$ax^2 + by^2 + cz^2 = 0.$$

2.3 Hadamard Matrices Over Groups

Definition 2.3.1 *Let $(G, \odot)$ be a group of order g. A $(g, k; \lambda)$-difference matrix is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G, such that for each $1 \leq i < j \leq k$, the multiset*

$$\{d_{il} \odot d_{jl}^{-1} : 1 \leq l \leq g\lambda\}$$

contains every element of G, λ times. When G is Abelian, typically, additive notation is used, so that differences $d_{il} - d_{jl}$ are employed.

Consider the additive group $G = \{0, 1, 2\}$ with modulo three arithmetic. Two inequivalent $(3, 6; 2)$-difference matrices over G are

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \end{bmatrix} \tag{2.3.1}$$

and

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 0 & 1 \\ 1 & 0 & 2 & 2 & 1 & 0 \\ 0 & 2 & 2 & 0 & 1 & 1 \\ 2 & 2 & 0 & 1 & 1 & 0 \\ 2 & 0 & 2 & 1 & 0 & 1 \end{bmatrix}. \tag{2.3.2}$$

Definition 2.3.2 *A generalized Hadamard matrix $GH(g, \lambda)$ over group G is a $(g, g\lambda; \lambda)$-difference matrix [7].*

A number of authors have studied theses matrices [13], [17], [30], [31], [32], and [33]. For a summary of the known matrices, see Theorem A of Street [33].

Clearly, both difference matrices A and B from (2.3.1) and (2.3.2), respectively, are generalized Hadamard matrices $GH(3, 2)$, each having an associated Butson Hadamard matrix $BH(3, 6)$. This association will now be clarified.

Theorem 2.3.1 *For primes $p > 2$, there exists a generalized Hadamard matrix $BH(p, p\lambda)$ over the cyclic group C_p if and only if there exists a generalized Hadamard matrix $GH(p, \lambda)$ over the additive group $Z_p = \{0, 1, 2, ..., p-1\}$, (+).*

A generalization of this result is stated by Drake [13], whose proof follows from results of Butson [6]. This association will be illustrated by example.

Let $C_3 = \{1, x, x^2\}$, where $x = e^{2\pi i/3}$ is a primitive cube root of unity. Consider the Butson Hadamard matrices

$$H = BH(3, 6) = x^E$$

where E is one of the difference matrices A, B from (2.3.1) and (2.3.2), respectively. The notation means that matrix elements obey $h_{ij} = x^{e_{ij}}$.

By calculation, $HH^* = 6I$; therefore, H is a generalized Hadamard matrix in the classical sense. Also, by calculation H is a $GH(3, 2)$ matrix with respect to C_3, $\cdot$. The Hadamard exponent forms (matrices A, B above) have already been cited as $GH(3, 2)$ with respect to the group $Z_3, \oplus$.

The next theorem provides a necessary condition for the existence of $GH(g, \lambda)$ over an Abelian group G, whose order is $|G| = g$:

Theorem 2.3.2 *A $GH(g, \lambda)$ with $n = g\lambda$ odd exists over Abelian group G of order $|G| = g$ only if a nontrivial solution in integers (x, y, z) exists to the quadratic Diophantine equation*

$$z^2 = nx^2 + (-1)^{(t-1)/2} t y^2, \tag{2.3.3}$$

for every order, t, of a homomorphic image of G.

The proof of this theorem can be found in Brock [4], and it is discussed in Colbourn and Dinitz [7].

Corollary 2.3.1 *For primes $p > 2$, and $\lambda > 0$ an odd integer, $BH(p, p\lambda)$ exists only if there are nontrivial solutions in integers (x, y, z) to both equations*

$$z^2 = p\lambda x^2 + (-1)^{(p-1)/2} p y^2 \tag{2.3.4}$$

and

$$z^2 = p\lambda x^2 + y^2. \tag{2.3.5}$$

Proof. If G is an Abelian group of order $p > 2$, where p is prime, there exist homomorphic images of G of orders $t = 1, p$. □

2.4 The Imbedding Problem

Definition 2.4.1 *Let G be an Abelian group of order g, with $n = g\lambda$, where λ is a positive integer. For $0 < k < n$, a $k \times n$ difference matrix D over the group G is "completable" if and only if there exists a $GH(g, \lambda)$ matrix having D as its first k rows.*

The Hadamard imbedding problem concerns the question of whether the matrix D can be extended by the process of row addition so as to be completable. This problem has been studied variously by Beder [3], Brock [4], Drake [13] and others.

Definition 2.4.2 *Difference matrix D of dimension $k \times n$, where $n = g\lambda$, is "locally maximal" (in dimension) if there is no $(k+1) \times n$ difference matrix which reduces to D by deletion of a single row. If D is a $GH(g, \lambda)$, then it is globally maximal [7].*

It is interesting to note that there may exist locally maximal $(g, k; \lambda)$-difference matrices for which $k < g\lambda$, even in cases where a $(g, g\lambda; \lambda)$-difference matrix exists. For $g = 2$ and $\lambda = 10$, Beder [3] constructs such (± 1) matrices, characterized by $k = 8, 12, 16$.

With respect to the group $G = \{0, 1, 2\}$, $(+)$, by computational methods the present authors have discovered locally maximal difference matrices $D_{k \times 15}$ with $k = 7, 8$ (see Tables 1 and 2 on next page). The observation that $gcd(7, 15) = gcd(8, 15) = 1$ appears a stark contrast to what may be observed in Beder's (± 1) difference matrices; namely, in cases where locally maximal difference matrices of dimension $D_{k \times n}$ and $D_{n \times n}$ simultaneously exist, $gcd(k, n) \neq 1$ (for $n = 20$; $k = 8, 12, 16$).

This contrasting behaviour leads to the likely conjecture that $GH(3, 15)$ does not exist. Actually, this has been known for several years. However, following up this conjecture in absence of this knowledge motivated the present research on non-existence of certain $GH(g, \lambda)$.

Tables 1 and 2 show the locally maximal difference matrices over group $G = \{0, 1, 2\}$, $(+)$; previously discussed:

Table 1: (3,7,15)-Difference Matrix

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 \\
0 & 0 & 1 & 1 & 1 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 \\
0 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 2 & 0 & 2 & 2 & 1 & 1 & 0 \\
0 & 0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 & 0 & 1 \\
0 & 1 & 2 & 0 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 0 & 1 & 2 & 0 \\
0 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 1 & 0 & 0 & 1 & 1 & 0 & 2
\end{bmatrix}$$

Table 2: (3,8,15)-Difference Matrix

$$\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \\
0 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 0 & 2 & 0 & 2 & 2 & 0 & 0 \\
0 & 1 & 2 & 2 & 2 & 0 & 1 & 2 & 1 & 0 & 0 & 1 & 1 & 2 & 0 \\
0 & 2 & 1 & 1 & 0 & 2 & 1 & 0 & 2 & 0 & 2 & 1 & 0 & 2 & 1 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 & 2 & 0 & 1 & 1 & 2 & 0 & 2 & 1 \\
0 & 2 & 0 & 0 & 1 & 2 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 1 & 0 \\
0 & 1 & 0 & 2 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 0 & 2 & 1 & 2
\end{bmatrix}$$

2.5 Quadratic Diophantine Equations

We now consider methods for establishing non-existence of nontrivial integer solutions to the homogeneous Diophantine equation

$$ax^2 + by^2 + cz^2 = 0 \tag{2.5.6}$$

Lemma 2.5.1 *If a and b of equation(2.5.6) are integers, then the equation*

$$z^2 = abx^2 \pm ay^2 \tag{2.5.7}$$

has nontrivial integer solutions only if the reduced equation

$$a\ell^2 = bx^2 \pm y^2 \tag{2.5.8}$$

has nontrivial integer solutions.

Proof. The result is obvious. If (x, y, z) is a solution of (2.5.7), of necessity $a|z$. Therefore, let $z = a\ell$, where ℓ is an integer if z is. □

<u>Method I:</u>

Legendre's Theorem: [29]

Let a, b, c be pairwise relatively prime integers which are squarefree and not all of the same algebraic sign. Then equation (2.5.6) has a nontrivial solution in the integers if and only if $-bc$, $-ac$, $-ab$ are quadratic residues of a, b, c, respectively.

Warwick de Launey [10] has approached the non-existence question for generalized Hadamard matrices by means of number theoretic properties of the Hadamard determinant. Basically, he proves the non-existence of many generalized Hadamard matrices for groups whose orders are divisible by 3, 5 or 7; for example, $GH(15, C_{15})$, $GH(15, C_3)$, and $GH(15, C_5)$.

That his work is non-exhaustive is evidenced by the following result:

Theorem 2.5.1 *For Abelian groups of order p, and for odd primes* $p \equiv \pm 3 (mod\ 5)$, $GH(p, 5)$ *does not exist.*

Proof. Consider the problem of finding integer solutions to the equation

$$z^2 = 5px^2 \pm py^2, \tag{2.5.9}$$

where $p \equiv \pm 3 (mod\ 5)$. This can be done only if one can find integer solutions of

$$pq^2 = 5x^2 \pm y^2 \tag{2.5.10}$$

As $x^2 \equiv \pm 3 (mod\ 5)$ has no solutions, by Legendre's theorem neither does (2.5.9) or (2.5.10) have nontrivial integer solutions. □

Note. Clearly, Theorem(2.5.1) generalizes some of de Launey's results.

2.6 Reciprocity

Definition 2.6.1 *For groups G, H with $|G| = g$ and $|H| = \lambda$, potential generalized Hadamard matrices $GH(g, \lambda)$ and $GH(\lambda, g)$ satisfy a reciprocity relation provided both exist or both do not exist.*

Example. $GH(3,5)$ and $GH(5,3)$ are reciprocally non-existent, as in each case the pertinent reduced equation is of the form

$$5a^2 = 3b^2 + c^2.$$

By Legendre's theorem, this equation has no nontrivial integer solutions (a, b, c), since ± 3 is a quadratic non-residue of 5. (The concept of quadratic residues is elaborated more completely in Appendix 1.)

By the same approach, the following result can be established:

Theorem 2.6.1 *Let λ be a prime number. If $(-1)^{\frac{5+1}{2}}\lambda$ and $(-1)^{\frac{\lambda-1}{2}}\lambda$ are both quadratic non-residues of 5, or if $(-1)^{\frac{5+1}{2}}5$ and $(-1)^{\frac{\lambda-1}{2}}5$ are both quadratic non-residues of λ, then $GH(5, \lambda)$ and $GH(\lambda, 5)$ constitute a reciprocally non-existent pair.*

Corollary 2.6.1 *If $7+5k$ is a prime number, then $GH(5, 7+5k)$ and $GH(7+5k, 5)$ constitute a reciprocally non-existent sequence of potential generalized Hadamard matrices.*

Theorem 2.6.2 *Let $p = 4k + 3$ and $q = 4l + 5$ be prime numbers, where 2 is a quadratic non-residue of p. Then (p, q) is a reciprocal pair.*

Proof. Since p, q are squarefree and relatively prime. Legendre's theorem applies to determine integer solutions of the equations

$$z^2 = pqx^2 - py^2$$

and

$$z^2 = pqx^2 + qy^2.$$

Existence of a nontrivial integer solution of either equation can happen only if there exists a nontrivial integer solution (ℓ, m, n) for equations of the following type

$$p\ell^2 = qm^2 - n^2.$$

No solution for this equation exists, as

$$x^2 \equiv 2(mod\ p)$$

has no solution. □

A more general method for finding reciprocal pairs employs a result of Euler:

Euler's Theorem: [35]

If p is an odd prime which does not divide a, then $x^2 \equiv a(mod\ p)$ has a solution or no solution according as

$$a^{(p-1)/2} \equiv 1(mod\ p) \tag{2.6.11}$$

or

$$a^{(p-1)/2} \equiv -1 (mod\ p). \tag{2.6.12}$$

Reciprocity Theorem: *Let $p = 4k + 3$ and $a = 4l + 5$ be odd primes which satisfy Euler's condition*

$$a^{(p-1)/2} \equiv -1 (mod\ p).$$

Then $GH(a, p)$ and $GH(p, a)$ constitute a reciprocal non-existent pair of generalized Hadamard matrices over groups G, H of order p, a.

Proof. Under the hypotheses of the theorem, Euler's condition guarantees the non-existence of nontrivial integer solutions (x, y, z) to both equations

$$z^2 = apx^2 - py^2$$

and

$$z^2 = apx^2 + ay^2,$$

whose reduced equation is of the form

$$p\ell^2 = ax^2 - y^2.$$

□

Several reciprocal pairs are given by Table 3:

Table 3: Reciprocal Pairs

3	5
3	17
3	29
11	13
11	17
11	29
19	29
19	37
19	41
59	61
107	109

Method II:

When the hypotheses of Legendre's theorem fail, an analysis of the last digit [26] of separate members of equation (2.5.6) is sometimes fruitful. Here, if x is a nonzero integer, the last digit of x is denoted by $[x]$. For instance, the last digit of x^2 is in the set

$[x^2] = \{0, 1, 4, 5, 6, 9\}$, and

$[3x^2] = \{0, 2, 3, 5, 7, 8\} = [7x^2]$,

$[(10k + 1)x^2] = [x^2]$, $k \geq 0$ an integer,

$[5x^2] = \{0, 5\}$,

$[9x^2] = \{0, 1, 4, 5, 6, 9\}$.

These facts are useful in proving some non-existence lemmas below.

Lemma 2.6.1 *The equation*

$$z^2 = 3 \cdot 5 \cdot (2k+1)x^2 - 3y^2 \tag{2.6.13}$$

where k is a non-negative integer satisfying $(2k+1) \not\equiv 0 (mod\ 5)$, does not possess a nontrivial solution in integers.

Proof. By the method of contradiction, assume a nontrivial solution (x, y, z) exists, where (x, y, z) are non-negative integers. As the equation is homogeneous of degree two, (x, y, z) is a solution if and only if (tx, ty, tz) is a solution, where t is an integer. Therefore, it can be assumed that $gcd(x, y, z) = 1$.

Clearly, z is divisible by 3. If $z = 3\ell$, where ℓ is an integer, then equation (2.6.13) reduces to

$$y^2 = 5(2k+1)x^2 - 3\ell^2. \tag{2.6.14}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0, 1, 4, 5, 6, 9\}$, the last digits of $5(2k+1)x^2$ and $3\ell^2$ are members of $\{0, 5\}$ and $\{0, 2, 3, 5, 7, 8\}$, respectively. For compatibility with (2.6.14), the last digit of y^2 can only be zero or five; therefore, $y = 5m$, where m is an integer.

Now equation (2.6.14) becomes

$$3\ell^2 = 5(2k+1)x^2 - 25m^2. \tag{2.6.15}$$

Therefore, $\ell = 5p$, where p is an integer. Equation (2.6.15) becomes

$$(2k+1)x^2 = 15p^2 + 5m^2.$$

Since five does not divide $2k+1$, it is necessary that $x = 5q$, where q is an integer. The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x, y, z) = 1$, the assumption that (2.6.13) has a nontrivial solution in the integers must be false. □

Lemma 2.6.2 *The equation*

$$z^2 = 5 \cdot n \cdot (10k+1)x^2 + 5y^2 \tag{2.6.16}$$

has no nontrivial solution for integers $k \geq 0$ *and* $n = 1, 3, 7$.

Proof. By the method of contradiction, assume a nontrivial solution (x, y, z) exists, where (x, y, z) are positive integers. As the equation is homogeneous of degree two, (x, y, z) is a solution if and only if (tx, ty, tz) is a solution, where t is an integer. Therefore, it can be assumed that $gcd(x, y, z) = 1$.

Clearly, z is divisible by 5 in equation (2.6.16).

Case 1: $n = 1$

If $z = 5\ell$, where ℓ is an integer, then equation (2.6.16) reduces to

$$y^2 = 5\ell^2 - (10k + 1)x^2. \tag{2.6.17}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0, 1, 4, 5, 6, 9\}$, the last digits of $5\ell^2$ and $(10k + 1)x^2$ are members of $\{0, 5\}$ and $\{0, 1, 4, 5, 6, 9\}$, respectively. For compatibility with (2.6.17), the last digit of x^2 and y^2 can only be zero or five; therefore, $x = 5m$ and $y = 5p$, where m and p are integers.

The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x, y, z) = 1$, the assumption that (2.6.16) has a nontrivial solution in the integers must be false.

Case 2: $n = 3$

If $z = 5\ell$, where ℓ is an integer, then equation (2.6.16) reduces to

$$y^2 = 5\ell^2 - 3(10k + 1)x^2. \tag{2.6.18}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0, 1, 4, 5, 6, 9\}$, the last digits of $5\ell^2$ and $3(10k + 1)x^2$ are members of $\{0, 5\}$ and $\{0, 2, 3, 5, 7, 8\}$, respectively. For compatibility with (2.6.18), the last digit of y^2 can only be zero or five; therefore, $y = 5m$, where m is an integer.

Now equation (2.6.18) becomes

$$3(10k + 1)x^2 = 5\ell^2 - 25m^2. \tag{2.6.19}$$

Since five does not divide $3(10k+1)$, it is necessary that $x = 5p$, where p is an integer. The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x, y, z) = 1$, the assumption that (2.6.16) has a nontrivial solution in the integers must be false.

Case 3: $n = 7$

If $z = 5\ell$, where ℓ is an integer, then equation (2.6.16) reduces to

$$y^2 = 5\ell^2 - 7(10k + 1)x^2. \tag{2.6.20}$$

As the last digit of each integer (x^2, y^2, ℓ^2) belongs to the set $L = \{0, 1, 4, 5, 6, 9\}$, the last digits of $5\ell^2$ and $7(10k + 1)x^2$ are members of $\{0, 5\}$ and $\{0, 2, 3, 5, 7, 8\}$, respectively. For compatibility with (2.6.20), the last digit of y^2 can only be zero or five; therefore, $y = 5m$, where m is an integer.

Now equation (2.6.20) becomes

$$7(10k + 1)x^2 = 5\ell^2 - 25m^2. \tag{2.6.21}$$

Since five does not divide $7(10k+1)$, it is necessary that $x = 5p$, where p is an integer. The conclusions $5|y$ and $5|x$ imply that $5|z$. As this contradicts $gcd(x, y, z) = 1$, the assumption that (2.6.16) has a nontrivial solution in the integers must be false. □

2.7 Summary

Theorem 2.7.1 *Several sequences of potential Hadamard matrices over Abelian group G of order g which do not exist are:*

1. $GH(3, 5(2k + 1))$, $(2k + 1) \not\equiv 0 (mod\ 5)$, *with k a non-negative integer,*

2. $GH(5, n(10k + 1))$, *for $n = 1, 3, 7$, k non-negative,*

3. $GH(5,p)$, *where* $p \equiv \pm 3 (mod\ 5)$ *is an odd prime,*

4. *Reciprocal pairs* $GH(5, 7+5k)$ *and* $GH(7+5k, 5)$, *where* $7+5k$ *is an odd prime.*

Corollary 2.7.1 *For* k *a non-negative integer, the following classes of* BH *matrices do not exist:*

1. $BH(3, 15(2k+1))$, $(2k+1) \not\equiv 0 (mod\ 5)$,

2. $BH(5, 5n(10k+1))$, *for* $n = 1, 3, 7$,

3. $BH(5, 5p)$, $p \equiv \pm 3 (mod\ 5)$, *an odd prime,*

4. *Reciprocal pairs* $BH(5, 35+25k)$ *and* $BH(7+5k, 35+25k)$, *where* $7+5k$ *is an odd prime.*

The following conjecture, which motivated this research, appears to gain some support from Corollary 2.7.1 and Tables 1 and 2:

Conjecture 2.7.1 *If for* $0 < k < g\lambda$ *a locally maximal* (g, k, λ)*-difference matrix with respect to Abelian group* G *of order* g *exists for which* $gcd(k, g\lambda) = 1$, *then* $GH(g, \lambda)$ *does not exist.*

Chapter 3

Error Correcting Codes Associated With Complex Hadamard Matrices Over Groups

3.1 Introduction

In this chapter it is shown that the row vectors of the exponent matrix associated with a Butson Hadamard matrix $BH(p, pt)$, $p > 0$ a prime number, constitute an error correcting code. Some background from algebraic coding theory will therefore now be introduced.

A block code whose codewords are of length n is a set of vectors of length n whose elements are symbols drawn from some alphabet. For example, the alphabet of a p-ary code may consist of the symbols which are elements of a finite field $Z_p = Gf(p)$, $p > 0$ a prime number. Thus, any subset K of Z_p^n constitutes a block

code of length n. The code is called a linear group code if and only if K is a linear subspace. Otherwise, the code is called nonlinear. K is cyclic if and only if every cyclic permutation of the symbols in a particular codeword $x \in K$ produces another codeword $y \in K$.

The Hamming metric allows block code K to become a metric space. The distance $d(x, y)$ between codewords x and y equals the number of differences between symbols which occupy corresponding element positions. The minimum distance $d(K)$ between codewords of code K is a distinguishing feature of the code.

Theorem 3.1.1 *(Fundamental Theorem of Algebraic Coding Theory): An error correcting code K corrects t errors if and only if its minimum distance, $d(K)$, between codewords is greater than $2t$.*

The fundamental parameters which characterize a linear code, K, are (n, k, d), where

- n = block length,
- k = number of information bits(per word),
- d = minimum distance between codewords.

The information rate $R = \frac{k}{n}$ characterizes the efficiency of a linear code, where $n - k$ is the number of redundant bits per word, which is what allows error correction to occur. The parameter d determines capacity to correct errors in transmission.

The purpose of this chapter is to introduce a class of error correcting codes which we call generalized Hadamard codes. Such codes are discovered by analyzing the Hadamard matrix of exponents, E, which is associated with a complex (Butson) Hadamard matrix, H.

Recall, Hadamard matrices $H(p,q)$, of index p, are matrices of dimension q whose elements are p-th roots of unity and whose rows are orthogonal. For the case $p = 2$, the elements are ± 1, and the matrix is referred to as a classical Hadamard matrix.

For $p > 2$, the elements are numbers on the unit circle, and the terminology used is that of a complex, or Butson Hadamard matrix. References [5], [6], [8] and [32] concern definition, structure, properties, and applications of generalized Hadamard matrices.

Butson [6] proves that for a fixed prime p, a necessary condition for existence of $H(p,q)$ is that p divides q. Thus, interest here is directed to complex Hadamard matrices $H(p,pt)$, where $p > 2$ is a fixed prime and t is a positive integer. When such matrices exist, a real matrix $E(p,pt)$, which is called a Hadamard exponent [8], can be associated with $H(p,pt)$. If x is a primitive p-th root of unity, the association is $H(p,pt) = x^{E(p,pt)}$. The notation means that matrix elements are related by $h_{ij} = x^{e_{ij}}$, where i and j are matrix indices.

The elements of the Hadamard exponent, E, lie in the Galois field $Gf(p)$, and its row vectors can be viewed as the codewords of what shall be called a generalized Hadamard code. Depending upon the value of the non-negative integer t, either a linear group code or a nonlinear code may emerge.

3.2 Ternary Hadamard Codes

As a first example of a nonlinear Hadamard code, the array Q given below provides the Hadamard exponent for a standard form Hadamard matrix $H(3,6) = x^Q$:

Table 4: Hadamard Matrix $H(3,6) = x^Q$

$$\begin{bmatrix} * & * & Q & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 0 & 2 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 & 0 & 1 \\ 0 & 2 & 1 & 2 & 1 & 0 \end{bmatrix}$$

Clearly, in forming code words by utilizing matrix row vectors, the first column is superfluous. It may be seen that code Q has minimum distance $d(Q) = 4$: therefore, Q corrects up to one error per codeword when utilized as an error correcting code.

The next example (see Table 5 on next page) exhibits a linear group code, D, obtained from the Hadamard exponent of $H(3,9)$, again written in standard form. D has minimum distance 6; therefore, up to two errors in each transmitted codeword can be corrected.

Table 5: Hadamard Matrix $H(3,9) = x^D$

$$\begin{bmatrix}
* & * & * & * & D & * & * & * & * \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\
0 & 2 & 1 & 0 & 2 & 1 & 0 & 2 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\
0 & 1 & 2 & 1 & 2 & 0 & 2 & 0 & 1 \\
0 & 2 & 1 & 1 & 0 & 2 & 2 & 1 & 0 \\
0 & 0 & 0 & 2 & 2 & 2 & 1 & 1 & 1 \\
0 & 1 & 2 & 2 & 0 & 1 & 1 & 2 & 0 \\
0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2
\end{bmatrix}$$

If the first all-zero column is omitted, one readily observes that the nine row vectors of $D = E(3,9)$ constitute a ternary linear error correcting code characterized by parameters $(n,k,d) = (8,2,6)$. By augmentation, an $(8,3,5)$ code having twenty seven codewords can be obtained, which has the punctured $E(3,9)$ as a subcode.

Similarly, there is associated with $H(3,27)$ the exponent $E(3,27)$ whose corresponding punctured linear Hadamard code has parameters $(26,3,18)$. This code augments to a code which possesses eighty one codewords, and which has the punctured linear Hadamard code as a subcode.

3.3 Vectors Over C_p

In this section the problem of establishing the value, $d(K)$, which represents the minimum Hamming distance between the codewords of a generalized Hadamard code, K, is considered.

Let $C_p = \{1, x, x^2, ..., x^{p-1}\}$ be the cyclic group generated by x, where $x = exp(2\pi j/p)$ is a complex primitive p-th root of unity, and $p > 2$ is a fixed prime. Further, let $A = (x^{a_i})$, $B = (x^{b_i})$ denote arbitrary vectors over C_p which are of length $N = pt$, where t is a positive integer. Define the collection of differences between exponents $Q = \{(a_i - b_i)(mod\ p) : i = 1, 2, ...N\}$, and let n_q be the multiplicity of element q of Z_p which appears in Q.

Property U: *Vectors A,B are said to satisfy this property U if each element q of Z_p appears in Q, exactly t times.*

The following lemma is of fundamental importance in constructing generalized Hadamard codes:

Lemma 3.3.1 *(Orthogonality Of Vectors Over C_p) For fixed primes p, arbitrary vectors A, B whose elements are from C_p are orthogonal if and only if for each element q in Z_p, q appears in Q with multiplicity t, where $N = pt$ is the length of A, B, and Q is the collection of mod p differences between the Hadamard exponents associated with A,B.*

Proof.

Sufficiency: If Q contains each element q of Z_p, t times, then the inner product of A and B

$$(A, B) = t \cdot \sum_{j=0}^{p-1} x^j,$$

vanishes, since x is a p-th root of unity. Hence, A and B are orthogonal.

Necessity: To the contrary, suppose n_q is not uniform as q varies over Q. If all n_q are non-zero, by using the fact that the sum of all p-th roots of unity vanishes, the happy circumstance is arrived at where the sum involved in (A, B) reduces to an integral linear combination which does not involve all p-th roots of unity. Moreover, if any $n_q = 0$, this circumstance is already present. Because the coefficients are positive integers, such a linear combination can not vanish. (Indeed, if $p = 3$, for any arbitrary set of non-zero coefficients the linear combination can not vanish, as any two cube roots of unity represent non-collinear vectors in the plane.) Hence, A and B are not orthogonal. □

Comment 1: Lemma 3.3.1 above can also be inferred from assertions of Butson [6], for which he provides no proof, but which he maintains are clearly valid.

Comment 2: For any p, Property U is sufficient for orthogonality. However, if p is not prime, cases are easily discovered of vectors over C_p which are orthogonal but which do not satisfy Property U. Thus, Property U is not always necessary for orthogonality.

Corollary 3.3.1 *If p is a prime number and if the Hadamard matrix $H(p, pt)$ exists,*

the error correcting code, $K(p, pt)$, associated with the corresponding row vectors of the Hadamard exponent, $E(p, pt)$, is characterized by the error protection afforded by $d(K) = (p-1)t$.

Proof. In the mod p difference of any two arbitrary row vectors of the Hadamard exponent matrix, the zero element of Z_p appears exactly t times; hence, two code words differ in $(p-1)t$ symbols. □

Standard Form: Any Butson's Hadamard matrix can be transformed into a Hadamard matrix for which every element of the first row and first column is unity. In this case, the first row and column of the Hadamard exponent consists of elements which are all zero. Some equivalent of a standard form matrix which is obtained by row and/or column interchanges is necessary but not sufficient in order to obtain from E a linear group code, as such codes require presence of the zero vector.

The code words can now be shortened by removing the first column, obtaining what is called a punctured code, which possesses the same level of error protection. When the code is linear, it can be imbedded in a linear group code having p times as many code words, through augmentation accomplished by adding appropriate cosets (add, respectively, each element of Z_p to each symbol of each code word, to get a new codeword).

3.4 Exponent Generation By Direct Sum

Whereas the matrix Q of Table 4 is tediously obtainable by trial and error, the matrix D of Table 5 easily follows by use of a direct sum, employing the matrix E

now given,

Table 6: Hadamard Exponent

$$\begin{bmatrix} * & E & * \\ 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix}$$

together with the direct sum below, plus row and column interchanges:

Lemma 3.4.1 *If $E = E(p,p)$ of Table 6 is a Hadamard exponent, then the direct sum*

$$E(p,p^2) = (e_{ij} + E; i,j = 0,1,...p-1)$$

is a block Hadamard exponent which is also a Hadamard exponent.

Likewise, $E(3,27)$ may be obtained as the direct sum of $E(3,3)$ and $E(3.9)$.

3.5 Linear Hadamard Codes

An initial exploration of the properties of the exponent matrix associated with a complex Hadamard matrix allows identification of a class of generalized Hadamard codes which can be linear or nonlinear, depending upon matrix dimension $N = pt$. In this section values of N are identified which permit existence of a sequence of linear Hadamard codes.

By definition, code $K = K(p, N)$ is a linear group code if and only if K is a linear subspace of $S = {Z_p}^N$ [1]. Thus, every linear group code can be generated by a finite set S_k of linearly independent vectors in S. If $G = G_k$ is the $k \times N$ matrix whose row vectors are the generators of K, G is called the generator matrix of K, and the parameters (N, k, d) completely characterize K. where $d = d(K)$ is the minimum Hamming distance between codewords of K. K is called systematic if and only if $G = \{I_k|B\}$, where B is of dimension $k \times (N - k)$.

For primes p, the sequence of codes characterized by the rows of the exponent matrix $E(p, p^k)$ form a sequence of linear error correcting codes whose codewords are equidistant at Hamming distance $d(K) = p^{k+1} - p^k$. Butson's results [6] guarantee the existence of such codes: whereas, linearity has not been established for the general case. Establishment requires only a determination that the code space possesses k generating vectors, a pattern which has been verified for $k = 2, 3, 4$. The following conditions characterize linear codes, $K = K(p, N)$:

Lemma 3.5.1 *A necessary condition that $K(p, N)$ be linear is that p^N/N be an integer.*

Proof. Otherwise, K is not a subgroup of S. □

Lemma 3.5.2 *If p is a prime, a necessary condition that $K(p, pt)$ be a linear code is that pt be a positive integer power of p.*

Proof. Clearly, if p is a prime and $N = pt$, $K(p, N)$ meets the condition of Lemma 3.5.1 if and only if t is a positive integer power of p. □

Theorem 3.5.1 *If p is a prime, the necessary and sufficient condition that $K = K(p, p^k)$ be a linear code is that the rowspace of K be of dimension k.*

Proof. Butson's existence theorems [6] assure that $H(p, p^k)$ exists. Let G be a maximal independent set of the row vectors of $K = K(p, p^k)$. If $dim(G) = n$, the linear code $span(G)$ generated by G coincides with the code constituted by the rows of K if and only if $n = k$. The reason is that $span(G)$ is a linear vector space over $Gf(p)$ which contains exactly p^n elements. As $K \subseteq span(G)$, the cardinality of K can not exceed that of $span(G)$, and the two cardinalities are equal if and only if $n = k$. When the cardinalities are equal, K must be a linear space, as K coincides with $span(G)$. □

Theorem 3.5.2 *If p is a prime and k is a positive integer, then $dim\{rowspace(K(p, p^k))\} = k$.*

Proof. There is now given a constructive algorithm for calculating a generating matrix G_k for $K = K(p, p^k)$:

Row 1: Fill row 1 by repeating the group of elements $\{0, 1, ...p-1\}$ t times, where $t = p^{k-1}$.

Row i: $i = 2, 3, ...k$: Until row i is full, focusing consecutively upon elements $g_{(i-1)j}$: repeat each element p times; $j = 1, 2, ...p^{k-1}$.

That this procedure produces the generating matrix for a Hadamard exponent $K(p, p^k)$ can be confirmed by the following observations:

Columns $\{p^j + 1 : j = 0, 1, ..., k-1\}$ form an identity matrix. Therefore, placing these columns in the first k positions yields the generating matrix of a systematic

linear code possessing $N = p^k$ codewords. Moreover, it can be verified by computer aided experiment that, for fixed k, the vector difference, mod p, of any two codewords possesses a uniform distribution of the elements $\{0, 1, ..., p-1\}$. Hence, the $N = p^k$ codewords form a Hadamard exponent $K(p, p^k)$, which can be placed in standard form by row interchanges. □

From another point of view, the k row vectors of the generating matrix coincide with certain rows of the direct sum

$$E(p, p^k) = E(p, p) \oplus E(p, p^{k-1});$$

namely, the vectors whose row indices are $\{p^j + 1 : j = 0, 1, ..., k-1\}$. Thus, $E(p, p^k)$ is the Hadamard exponent generated by G_k.

The following example demonstrates the concept:

Table 7: Generating Matrix For $K(3, 27)$

$$\begin{bmatrix} 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \end{bmatrix}$$

The code K generated by the above matrix is not systematic. However, by placing columns four and nine in the column three and column four positions, after shuffling the first column of zero's an equivalent systematic code will be generated. If the first column of zeroes is not shuffled, after the zero codeword is moved to the

first row position, the codewords of the generated code form the Hadamard exponent $K(3,27)$ in standard form.

3.6 Summary

An initial exploration of the properties of the exponent matrix associated with a complex Hadamard matrix allows identification of a class of generalized Hadamard codes. For primes p, the sequence $K(p,p^n)$ appears to be a sequence of linear error correcting codes whose codewords are equidistant at Hamming distance $d(K) = p^{n+1} - p^n$. Butson's results [6] guarantee the existence of such codes; whereas, linearity has not been established for the general case. Establishment would require only a determination that the code space possesses n generating vectors, a pattern which has been verified for $n = 2, 3$.

For some values of q it is not at all certain that $H(p,q)$ exists. In particular, the authors conjecture (and it is established in Chapter 2) that $H(3,15)$ does not exist, which is a case not covered by Butson's results on existence by construction or by direct sums.

A particularly interesting question is whether the linear codes possess an equivalent cyclic version, as then the potential exists for burst error protection against bursts of increasingly long duration.

Finally, one question whether there is a decoding technique which is unique to the Hadamard codes, and exactly what is the best use for the nonlinear codes. In all cases, nature seems to have formed a vast lode of interesting codes, waiting to

be exploited.

Chapter 4

Polynomial Construction Of Complex Hadamard Matrices With Cyclic Core

4.1 Introduction

Consider complex Hadamard matrix $H = H(p, p^n)$, where $p > 2$ is prime and n is a positive integer. Let E be the exponent matrix which is defined by $H = x^E$, with $x = exp(2\pi i/p)$. The notation implies $h_{jk} = x^{e_{jk}}$, where j and k are matrix indices. Here, the elements of E lie in the Galois field $Gf(p)$.

If H is written in standard form, then the first row and first column of E are all zero, and the remaining elements constitute a square submatrix, E_c, called the core of H. Using the theory of linear recurring sequences, Butson [6] shows how to construct from an appropriately chosen relative difference set, a cyclic matrix E_c

(see Chapter 5 for a study of cyclic matrices) which qualifies as the core of some Hadamard matrix $H(p, p^n)$. In conjunction with the zero vector, the row vectors of E_c form a linear group. Thus, by omission of the all-zero first column, cyclic generalized Hadamard codes are possible, whose codewords are the row vectors of the punctured matrix. Generalized Hadamard codes, both linear and nonlinear, are discussed in Chapter 3.

As matrix size increases, Butson's method for constructing cyclic core E_c becomes proportionately less desirable. It is the opinion of the authors that a simple equivalent constructive approach can be obtained, by searching for polynomials over $Gf(p)$ whose zero-augmented coefficient vector satisfies a certain uniformity property later introduced. For several cases studied the approach has been found fruitful.

The purpose of the present chapter is to supply proof that this approach is generally applicable. In order to do so, it will first be necessary to develope a theorem concerning invariant M-sequences. Properties of Hadamard matrices and complex Hadamard codes are then reviewed, followed by statement and proof of the main results, with some accompanying numerical examples.

4.2 M-Sequences

In this section there is examined certain properties of infinite sequences with elements in the finite field Z_p which are obtained by cycling the elements of some initial vector V of length N. The resulting sequence is denoted by $a(V)$. These sequences are usually studied in the context of solutions to homogenuous linear

difference equations [37] (see Chapter 5 also).

Such sequences are clearly periodic, of period N; however, a smaller period may be possible. If N is the least period, the sequence is called an M-sequence, or a sequence of maximal least period obtained by cycling N elements. If, when the elements of the ordered set V are permuted arbitrarily to yield V^*, the sequence $a(V^*)$ is an M-sequence, then the sequence $a(V)$ is called M-invariant under rearrangements of its first period. In the sequel, the property of M-invariance proves useful in constructing Hadamard matrices with cyclic core.

Let $V = v_0 v_1 ... v_{N-1}$ be a vector over Z_p. If j is a residue in Z_p, let λ_j be the multiplicity of j, as a member of the set of elements of V. If j is not such an element, define the multiplicity to be zero. Cyclic rotations of V are defined by $T^k(V)$, where k is a positive integer and $T(V) = v_{N-1} v_0 v_1 ... v_{N-2}$.

Let $(i) = l$ signify that i is congruent to $l(mod\ p)$. Cycling V produces an infinite sequence $a(V) = \{v_{(i)} : i = 0, 1, 2, ...\}$. The following theorem provides conditions under which $a(V)$ will be an invariant M-sequence:

Theorem 4.2.1 *Let $\zeta = \lambda_0 \lambda_1 ... \lambda_{p-1}$ be a vector whose components are non-negative integers which satisfy compatibility relations (I-II):*

$$(I): \quad \sum_{j=0}^{p-1} \lambda_j = N$$

$$(II): \quad g.c.d.(\zeta, N) = q.$$

There exists a vector $V = v_0 v_1 ... v_{N-1}$, *whose set of components includes all residues from* Z_p *with multiplicities* ζ, *such that the sequence* $a(V)$ *is an invariant M-sequence, if and only if* $q = 1$.

Proof.

Necessity: For ζ a vector having non-negative integer components satisfying (I-II) with $q > 1$, suppose there exists a vector V with associated multiplicities ζ which generates an M-invariant sequence $a(V)$. A contradiction will be arrived at by showing that the ordered set V can be permuted into an ordered set V^* such that $a(V^*)$ is periodic of period $0 < L < N$.

To this purpose, define non-negative integers $\lambda_j{}^0 = \lambda_j/q; j = 0, 1, ...p-1$, which sum to $L = N/q$. It is clear that the sets $S_j = \{V_i : V_i = j\}$ of residues which appear in V are either empty, or else can each be divided into subsets $S_j{}^i : i = 1, 2, ...q$ of cardinality $\lambda_j{}^0$. For $i = 1, 2, ...q$, form a vector Q_i of length L by arranging sequentially the elements from $S_j{}^i$, for all residues j represented in V. Next, form vector V^* by sequentially placing all elements of the group Q_i after the elements of Q_{i-1}, for $i = 2, 3, ...q$.

As it is clear that $a(V^*)$ is periodic of period L, $a(V)$ can not be M-invariant. Thus, the assumption of an M-invariant sequence in conjunction with $q > 1$ is a contradiction.

Sufficiency: Suppose V is a vector whose associated multiplicity vector ζ satisfies (I-II), where $a(V)$ is an M-sequence, and $q = 1$. It will be shown that $a(V)$ is M-invariant. Assume $a(V)$ is not M-invariant. Then, there is a permutation V^*

of V whose elements satisfy multiplicity condition (I), such that $a(V^*)$ is not an M-sequence, but has period L which satisfies $0 < L < N$. But this means V^* has a first L element pattern which repeats Q times, with $N = QL$. Moreover, this pattern assures that $\lambda_j = Q\lambda_j{}^0; j = 0, 1, ...p-1$. Therefore, $g.c.d.(\zeta, N) = Q$, with $1 < Q < N$. This contradicts $q = 1$. Hence, the assumption a(V) is not M-invariant is false. □

Comments: Suppose V is of length N and its associated vector ζ of multiplicities has non-negative integer components, which satisfy (I-II) with $q > 1$. Suppose $a(V)$ is periodic of period $L < N$, and suppose two distinct residues appear in the first L components of V. By interchanging one distinct pair of components only in the first period, the resulting vector V^* generates an M-sequence. Thus, M-sequences exist which are not M-invariant.

4.3 Cyclic Hadamard Codes

Consider matrix E which is the Hadamard exponent associated with $H = H(p, p^n)$ when it is written in standard form. Thus, the first row and first column of E are all zero, and the remaining elements constitute a square submatrix, E_c, called the core of H. Using the theory of linear recurring sequences, Butson [6] shows how to construct from an appropriately chosen relative difference set, a cyclic matrix E_c which qualifies as the core of a complex Hadamard matrix $H(p, p^n)$. Thus, cyclic generalized Hadamard codes are possible, by omission of the all-zero first column of E. In coding theory, this is called puncturing (The concept of a cyclic matrix is

clarified in Chapter 5).

However, Butson's method is somewhat unwieldy, and becomes less desirable as matrix size increases. It is the opinion of the authors that a simpler, yet equivalent approach to constructing E_c is possible. The approach now outlined has been found to provide in several cases attempted a cyclic matrix E_c which qualifies as a Hadamard core for specific $H(p, p^n)$.

The goal is to find cyclic matrix $E = E_c$ whose elements are in Galois field $Gf(p)$ and whose dimension is $N = p^n - 1$. The rows of E will be the non-zero codewords of a linear cyclic code K if and only if there is a polynomial $g(x)$ with coefficients in $Gf(p)$, which is a proper divisor of $x^N - 1$ and which generates K [1], [22]. In order to have N non-zero codewords, $g(x)$ must be of degree $N - n$. Further, in order to generate a cyclic Hadamard core, the vector (of coefficients of) $g(x)$ when operated upon with the cyclic shift operation must be of period N, and the vector difference of two arbitrary rows of E (augmented with zero) must satisfy the uniformity condition of Butson, previously referred to as Property U.

One necessary condition for N-peridoicity is that $x^N - 1 = g(x)h(x)$, where $h(x)$ is monic irreducible over $Gf(p)$ [37]. A sufficient condition is that, in addition, a certain subset [6] of the indices from the coefficients of $g(x)$ be a relative difference set.

The approach here is to replace the last requirement with the condition that the coeffieients of the vector $[0, g(x)]$ be uniformly distributed over $Gf(p)$: each residue 0,1,...p-1 appears the same number of times (Property U). This heuristic approach has succeeded for all cases tried, and a proof that it always produces a cyclic core

is now given.

4.4 Polynomial Construction Algorithm

Consider all monic irreducible polynomials $h(x)$ over $Gf(p)$ which are of degree n, and which permit a suitable companion $g(x)$ of degree $N-n$ such that $g(x)h(x) = x^N - 1$, where also vector $[0, g(x)]$ satisfies property U. This requires only a simple computer algorithm for long division over $Gf(p)$. Since $h(x)|x^N - 1$, the ideal generated by $g(x)\ mod(x^N - 1)$, will be a cyclic code, K [1], [22]. Moreover, Property U guarantees the non-zero codewords form a cyclic matrix, each row being of period N under cyclic permutation, which serves as a cyclic core for Hadamard matrix $H(p, p^n)$.

As an example, a cyclic core for $H(3,9)$ results from the companions $h(x) = x^2 + x + 2$, and $g(x) = x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1$. The coefficients of $g(x)$ indicate that $\{0, 1, 6\}$ is the relative difference set, mod 8, which instead could be used to generate the cyclic core [5], certainly more intricately than by calculating the codewords associated with $g(x)$ using the cyclic shift operation.

Theorem 4.4.1 *Let p be a prime and $N+1 = p^n$, with $g(x)$ a monic polynomial of degree $N-n$ whose vector of coefficients $C = [c_0, c_1, ...c_{N-1}]$ are elements of $Gf(p)$. The conditions*

(i) The extended vector $\bar{C} = [0, c_0, c_1, ..., c_{N-1}]$ satisfies property U,

(ii) $g(x)h(x) = x^N - 1$, where $h(x)$ is a monic irreducible polynomial of degree n,

guarantee the existence of a p-ary, linear cyclic code, $\bar{K}$, of blocksize N, such that the augmented code $K = [0, \bar{K}]$ is the Hadamard exponent, for Hadamard matrix $H(p, p^n) = x^K$, with $x = exp(2\pi i/p)$, where the core of H is a cyclic matrix.

Proof. Since $g(x)$ is monic, divides $x^N - 1$, and has degree $N - n$, $g(x)$ generates a p-ary, cyclic code which is an n-dimensional linear subspace, $\bar{K}$ of $Z_p{}^N$ [1], [22], and which possesses p^n codewords, N of which are nonzero. It is intended to show that the matrix E_c whose rows are the nonzero codewords constitutes a cyclic core for some complex Hadamard matrix, $H(p, p^n)$, written in standard form.

First, since $\bar{C}$ satisfies property U, the nonzero residues of $Gf(p)$, all of which appear in C, will have multiplicity which is one unit greater than the multiplicity of the zero residue. Since any two successive positive integers are relatively prime, by Theorem 4.2.1, the infinite sequence, $a(C)$, obtained by cycling C will be an M-invariant sequence, periodic of least period N. Thus, every codeword of E_c can be obtained by cyclicly permuting the first codeword. Hence, E_c is a cyclic matrix (circulant with least period N).

Second, it follows that augmentation of each codeword of E_c by adding a leading zero element produces a vector which satisfies Property U. Moreover, since the code is linear, the mod p vector difference of two arbitrary codewords is also a codeword. Hence, vector differences of arbitrary zero-augmented codewords satisfy property U. Therefore, the row vectors of the augmented code, K, form a Hadamard exponent. It may be concluded that x^K is the standard form of some complex Hadamard matrix $H(p, p^n)$. □

Corollary 4.4.1 *Existence of Hadamard matrix $H(p, p^n)$ having cyclic core is equivalent to the existence of a pair of polynomials over Gf(p) which satisfy $g(x)h(x) = x^N - 1$, where $h(x)$ is irreducible of degree n, and $[0, g(x)]$ satisifies Property U, mod p, where p is prime.*

Proof. It is clear that the lines of proof in Theorem 4.4.1 can be reversed: Given $H = H(p, p^n)$, where p is prime, which has cyclic core, delete the first row and first column, and associate with the elements of arbitrary remaining punctured row i, a polynomial $f_i(x)$ whose coefficients are in $Gf(p)$. Let $g(x)$ be the unique polynomial of minimal degree $(N - n)$ from the collection $\{f_i(x) : i = 2, 3, ...N + 1\}$. (If $g(x)$ is not monic, it becomes such upon multiplication by a suitably chosen element of $Gf(p)$). As the core of H is cyclic, let $h(x) = (x^N - 1)/g(x)$, where $N + 1 = p^n$. Clearly, $g(x)$ satisfies Property U. As the period of each row of core(H) under cyclic permutation is N [6], $h(x)$ is irreducible [37]. □

4.5 Computer-Aided Construction of Polynomial Pairs

In this section there is given some results from computer-aided construction (see Appendix 2) of the polynomial pairs $(g(x), h(x))$ which satisfy Theorem 4.4.1. Table 8 shows typical irreducible $h(x)$, whose companion $g(x)$ (see Table 9) satisfies Property U.

Interestingly enough, analysis of the type represented by Table 8 yields insights

into the question of how many Hadamard matrices $H(p, p^n)$, unique to within row and column interchanges when written in standard form, can be expected to exist.

Table 8: Parity Check Polynomials

$N+1=p^n$	$h(x)$
3^2	x^2+x+2
	x^2+2x+2
3^3	x^3+2x+1
	x^3+2x^2+1
	x^3+2x^2+x+1
	x^3+x^2+2x+1
3^4	x^4+x+2
	x^4+2x+2
	x^4+x^3+2
	x^4+2x^3+2
	$x^4+x^3+x^2+2x+2$
	$x^4+2x^3+x^2+x+2$
	$x^4+x^3+2x^2+2x+2$
	$x^4+2x^3+2x^2+x+2$

Table 9: Coefficients of Generating Polynomials

$N = p^n - 1$	$g(x) = a_0 + a_1 x + ... + a_n x^n$
8	11202210
	12202110
26	22201221202001110211210100
	20212210222001012112011100
	21112102022001222120101100
	22020121112001101021222100
80	11112012112120202211020110012220210020002222102122121010 11
	22010220021110120010 00
	12122011122222020211201021002212022002000212110222111101012
	21020120011210110010 00
	10011012110021020122101011112220112120002002202122001201 02
	11202022221110221210 00
	10021011120022010221101012122120122220002001202221001102 01
	12202021211210211110 00
	12211100220100101022102121101111210120002112220011020020 20
	11201212202222120210 00
	11221200210200101021102222101212220220002211210012010020 20
	12201111202121110110 00
	12021222202212102110202002011002221120002101211110112120 12
	20101001022001112210 00
	11011121202111102210202001021001211220002202221210122220 11
	20101002012002122110 00

Chapter 5

M-Sequences and Circulant Matrices

5.1 Review of the Theory of m-Sequences

Consider a homogeneous linear difference equation of order m

$$\sum_{k=0}^{m} h_k v_{i+k} = 0 \tag{5.1.1}$$

which has characteristic polynomial

$$h(x) = \sum_{k=0}^{m} h_k x^k.$$

It will be assumed that the coefficients, h_k, lie in a finite field $Gf(q)$, where $q = p^n$, with $p \geq 2$ a prime number, and n a positive integer.

Denote by $G(h)$ the m-dimensional linear space of infinite sequences over $Gf(q)$ which are solutions to (5.1.1). It is known that each solution $a \in G(h)$ is a periodic infinite sequence whose period $p(a)$ is bounded by $N = q^m - 1$. Sequence a is called an m-sequence, or a sequence of maximal least period, if and only if $p(a) = N$.

It is the intent of this section to review the classical theory of m-sequences as presented by Zierler [37]. The connection to the problem of prescribing a circulant matrix whose rows form a linear space (whose zero vector has been removed) is indicated. Such cyclic matrices are called linear circulant, and appear naturally (see Chapter 4) in a study of Hadamard matrices whose associated exponent has a cyclic core. The relation between m-sequences and M-sequences is established. As it turns out, an m-sequence is M-invariant.

Let $p(a)$ be the least period of sequence a, and $d(f)$ the degree of polynomial $f(x)$. The minimium polynomial of periodic sequence a is the nonzero polynomial $f(x)$ of smallest degree such that $a \in G(f)$.

Let $p(f) = inf\{s > 0 : f|x^s - 1\}$.

Zierler proves the following:

Theorem 5.1.1 $a \in G(f) \Leftrightarrow p(a)|p(f)$.

Theorem 5.1.2 *If f is the minimium polynomial of a, $p(a) = p(f)$.*

Corollary 5.1.1 *If f is irreducible, $p(a) = p(f)$ for every $a \in G(f)$.*

Theorem 5.1.3 *$a \in G(f)$ is an m-seqence if and only if f is irreducible and of degree n, where $p(a) = q^n - 1$.*

Corollary 5.1.2 *$a \in G(f)$ is an m-sequence if and only if f is an irreducible, primitive polynomial in $Gf(q^n)$, where $d(f) = n$.*

Corollary 5.1.3 *The number of translation distinct m-sequences of least period $N = q^n - 1$ is $\Phi(q^n - 1)/n$, where Φ is the Euler totient function.*

Theorem 5.1.4 *If a is an m-sequence of least period $N = q^n - 1$, each nonzero element of $Gf(q)$ appears q^{n-1} times, and the zero element appears $q^{n-1} - 1$ times, in a period of a.*

As Zierler states but does not prove Theorem (5.1.4), this theorem will be proved in the sequel.

5.2 Classification of Circulant Matrices Over $Gf(q)$

Butson's paper [6] refers to the concept of the cyclic core of a Hadamard matrix, but with no explanation or definition of what is meant. In this section the concept is clarified, by a study of circulant matrices over a field. It is thus determined that by Butson's reference to a cyclic matrix is meant a linear cyclic circulant matrix with elements in a Galois field.

The notation $C = C(v)$, where v is a vector having N elements, denotes a circulant matrix which is generated by cycling the elements of v. A circulant matrix, C, of order N has elements which satisfy

$$C_{i,j} = C_{(i-1),(j-1)}, \quad i, j = 0, 1, 2, ..., N-1,$$

where (k) is the smallest non-negative mod N evaluation of k.

Let $C(v)$ be a circulant matrix of order N over $Gf(p)$, where sequence $a(v)$ has least period $p(a)$. $C(v)$ falls into one of the following classes:

1. $C(v)$ has a repeated row if and only if $0 < p(a) < N$, where of necessity $p(a)|N$.

2. $C(v)$ has no repeated row if and only if $p(a) = N$, in which case $a(v)$ is an m-sequence. Two finer classifications are possible:

3. $C(v)$ is nonlinear cyclic with no repeated row if and only if $C \bigcup 0$, where 0 is the zero vector, is a proper subset of rowspace (C). This happens if and only if either (i) the minimium polynomial of $a(v)$ is $m(x) = x^N - 1$, or else (ii) $m(x)|x^N - 1$, with N the degree of the smallest such polynomial which $m(x)$ divides. This means $a(v)$ is an M-sequence, but not an m-sequence.

4. $C(v)$ is linear cyclic if and only if $a(v)$ is an m-sequence. In other words, $a(v)$ has minimium polynomial $m(x)$ of degree n, where $N = p^n - 1$, and $m(x)$ is an irreducible, primitive polynomial over some extension field $Gf(p^n)$. This also implies that rowspace $(C) = C \bigcup 0$.

Example 1:

For $p = 2$, $v = (1010)$, $N = 4$, yields $C(v)$ which has repeated rows. Namely,

$$C = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

Example 2:

For $p = 3$, $v = (2110)$, $N = 4$, $a(v)$ is an M-sequence, with minimium polynomial $m_a(x) = x^4 - 1$. But $a(v)$ is not an m-sequence, as $N \neq p^4 - 1$. Thus, $C(v)$ is a nonlinear cyclic matrix with the rowspace (C) much larger than $C \bigcup 0$. Here,

$$C = \begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 2 \end{bmatrix}$$

Example 3:

For $p = 3$, $v = (22110)$, $N = 5$, $a(v)$ is an M-sequence, whose minimium polynomial $m_a(x) = 1 + x + x^2 + x^3 + x^4$ divides $x^N - 1$, with $N = 5$ being the smallest such N. $a(v)$ is not an m-sequence, as $N \neq p^4 - 1$. Therefore, $C(v)$ is nonlinear cyclic with rowspace much larger than $C \bigcup 0$. Here,

$$C = \begin{bmatrix} 2 & 2 & 1 & 1 & 0 \\ 0 & 2 & 2 & 1 & 1 \\ 1 & 0 & 2 & 2 & 1 \\ 1 & 1 & 0 & 2 & 2 \\ 2 & 1 & 1 & 0 & 2 \end{bmatrix}$$

Example 4:

For $p = 3$, $v = (11202210)$, $N = 8$, $a(v)$ is an m-sequence with minimium polynomial $h(x) = x^2 + x + 2$, which is irreducible primitive over $Gf(3^2)$. Clearly, $N = p^2 - 1$, $h(x)|x^N - 1$, with $N = 8$ the smallest such N (p(h)=8). Here,

$$C = \begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\ 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\ 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\ 2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\ 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\ 1 & 2 & 0 & 2 & 2 & 1 & 0 & 1 \end{bmatrix}$$

5.3 The Relation Between m-Sequences and M-Sequences

In this section, it will be established that every m-sequence is M-invariant.

Lemma 5.3.1 *Over a period N of an m-sequence which satisfies equation (5.1.1), every k-tuple $b_1b_2...b_k$ of $Gf(q^m)$ appears in a contiguous set of locations $v_iv_{i+1}...v_{i+k}$ for exactly l values of i, where*

$$l = \begin{cases} q^{m-k}, & \text{for nonzero k-tuples,} \\ q^{m-k}-1, & \text{for the zero k-tuple} \end{cases}$$

Proof. Recall, an m-sequence is a solution over $Gf(q)$ of the linear difference equation

$$\sum_{k=0}^{m} h_k v_{i+k} = 0, \quad h_0 h_m \neq 0.$$

Given a nonzero initial state $S_0 = (v_0v_1...v_{m-1})$, a succeeding non-zero state $S_1 = (v_1v_2...v_m)$ is obtained by solving the difference equation for v_m. This process defines a linear mapping

$$S_k = A \cdot S_{k-1}$$

where

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ . & & & & & \\ . & & & & & \\ . & & & & & \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ \frac{-h_m}{h_0} & \frac{-h_{m-1}}{h_0} & \frac{-h_{m-2}}{h_0} & \frac{-h_{m-3}}{h_0} & \cdots & \frac{-h_1}{h_0} \end{bmatrix}.$$

Since $|A| = (-1)^m h_m/h_0$, the map is one to one. As there are at most $N = q^m - 1$ possible non-zero states, eventually, for some $0 < R \leq N$,

$$S_R = A^R \cdot S_0 = S_0.$$

Hence, sequence $a(S_0)$ is periodic of least period R. $a(S_0)$ is called an m-sequence, or a sequence of maximal least period if and only if $R = N$. □

For an m-sequence, every possible nonzero initial state occurs exactly once over a period. Moreover, the starting element of a contiguous k-tuple will always coincide with the first element of some state S. To count the number of such states, observe that k positions of the m-tuple will be occupied, with $m - k$ positions free, which can be filled q^{m-k} ways. As the all-zero state is not possible in an m-sequence, the all-zero k-tuple appears one time less than does a nontrivial k-tuple.

Corollary 5.3.1 *Every non-zero element of $Gf(q)$ occurs exactly q^{m-1} times, and the zero element occurs $q^{m-1} - 1$ times, over period N, if and only if $a(v)$ is an*

m-sequence.

Theorem 5.3.1 *(M-Invariance): Every m-sequence over $Gf(q)$, where $q = p^l$, is M-invariant.*

Proof. By the corollary (5.3.1), a vector

$$v = [v_0 v_1 ... v_{N-1}]$$

whose elements constitute the first period of an m-sequence $a(v)$ is such that $v \bigcup 0$ obeys property U of section 3.3. Therefore, $a(v)$ is an M-invariant sequence. □

Chapter 6

Summary and Conclusions

1. Investigating the existence of $BH(3, 15)$ by numerically constructive means leads to the discovery of row maximal difference matrices which lead one to conjecture the non-existence of $BH(3, 15)$.
2. Therefore, investigation has been directed to the question of existence for generalized Hadamard matrices over groups. In particular, parameter sequences $\{t_n\}$ are identified for which the corresponding potential generalized Hadamard matrices $BH(p, t_n)$ and $GH(p, t_n)$ fail to exist, where $p > 2$ is a prime number. Several methods for establishing non-existence are identified.
3. Interest has been focused upon applications of Butson's complex Hadamard matrices $BH(p, pt)$ to the area of algebraic coding theory. It is shown that the row vectors of each existent such Hadamard exponent matrix can be viewed as an error correcting code. Both linear and nonlinear codes are possible.
4. Distance properties of generalized Hadamard codes have been explored. Minimum distance between codewords is derived. The exact circumstances

under which a code will be linear or nonlinear are determined.

5. An efficient polynomial method is obtained which can be used to construct a Butson Hadamard matrix $BH(p, p^n)$ whose associated Hadamard exponent possesses a linear cyclic core with row vectors which form a cyclic linear code. For such codes, standard decoding schemes may be employed.
6. The concept of an M-invariant sequence has been defined. Conditions necessary and sufficient for their construction are derived. Such sequences prove useful in constructing Hadamard matrices with cyclic core.
7. The characteristic polynomial used to construct $BH(p, p^n)$, $p > 2$ a prime number, can equally well be used to determine which relative difference set is associated with the matrix. In general, this is not easy.
8. It is established that every m-invariant sequence (in the sense of Zierler [37]) is also M-invariant.

6.1 Directions of Future Research

Although the classical linear Hadamard codes are optimal in the sense that the Plotkin bound [22] is satisfied, this optimality does not extend to the generalized Hadamard codes studied here. The Plotkin bound states that for any (n, M, d) code K for which $n < 2d$, we have

$$M \leq 2[\frac{d}{2d - n}].$$

The notation (n, M, d) code is a set of M vectors of length n such that any two vectors differ in at least d places, and d is the largest number with this property.

It is clear that the linear cyclic Hadamard codes investigated have a place in information and communication theory. However, the usefulness of the nonlinear Hadamard codes has not been ascertained.

REFERENCES

1. J. Adamek, *Foundations of Coding*, John-Wiley, New York, (1991).
2. E. F. Assmus and J. D. Key, *Designs and Their Codes*, Cambridge University Press, New York, (1992).
3. J. H. Beder, Conjectures about Hadamard Matrices, *R.C. Bose Memorial Conference On Statistical Design and Related Combinatorics*, Colorado State University, June 7-11, (1995).
4. B. W. Brock, Hermitian Congruence and the Existence and Completion of Generalized Hadamard Matrices, *J. of Combinatorial Theory (Series A)* **49**, 233-261, (1988).
5. A. T. Butson, Generalized Hadamard Matrices, *Proc. Amer. Math. Soc.* **13**, 894-898, (1962).
6. A. T. Butson, Relations Among Generalized Hadamard Matrices, *Can. J. Math.* **15**, 42-48, (1963).
7. C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, New York, (1996).
8. C. H. Cooke, The Hadamard Matroid and an Anomaly in its Single Element Extensions, *CMA* **38**, 115-120, (1997).
9. J. Dawson, A Construction for Generalized Hadamard Matrices GH(4q, EA(4q)), *J. Stat. Plann. and Inference* **11**, 103-110, (1985).
10. W. de Launey, On the Non-Existence of Generalized Hadamard Matrices, *J. Stat. Plann. and Inference* **10**, 385-396, (1984).
11. W. de Launey, Generalized Hadamard Matrices which are Developed Modulo a Group, *Discrete Math.* **104**, 49-65, (1992).
12. W. de Launey, Generalized Hadamard Matrices whose Rows and Columns form

a Group, *Combinatorial Mathematics X*, Lecture Notes in Mathematics **1036**, 154-176, Springer-Verlag, New York, (1983).

13. D. A. Drake, Partial λ-geometries and Generalized Hadamard Matrices over Groups, *Can. J. Math.* **31**, 617-627, (1979).
14. M. Hall and H. J. Ryser, Normal Completions of Incidence Matrices, *Amer. J. Math.* **76**, 581-589, (1954).
15. A. Hedayat and W. D. Wallis, Hadamard Matrices and Their Applications, *Annals Of Statistics* **6**, 1184-1238, (1978).
16. W. H. Holzmann and H. Kharaghani, On the Excess of Hadamard Matrices, *Congr. Numerantium* **92**, 257-260, (1993).
17. D. Jungnickel, On Difference Matrices, Resolvable Transversal Designs and Generalized Hadamard Matrices, *Math. Z.* **167**, 49-60, (1979).
18. H. Kharaghani, A Construction for Hadamard Matrices, *Discrete Math.* **120**, 115-120, (1993).
19. H. Kharaghani and J. Seberry, The Excess of Complex Hadamard Matrices, *Graphs and Combinatorics* **9**, 47-56, (1993).
20. Shu Lin, *An Introduction to Error-Correcting Codes*, Prentice-Hall, Englewood Cliffs, (1970).
21. Shu Lin and Daniel J. Costello, *Error Control Coding*, Prentice-Hall, Englewood Cliffs, (1983).
22. F. J. MacWilliams and N. J. Sloane, *The Theory of Error Correcting Codes*, Ninth Edition, North-Holland, Amsterdam, (1996).
23. Richard A. Mollin, *Quadratics*, CRC Press, Inc., New York, (1996).
24. R. E. A. C. Paley, On Orthogonal Matrices, *J. Math. Phys.* **12**, 311-320, (1933).
25. W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, Second Edition,

MIT Press, Cambridge, (1972).

26. Mark Dorrepaal, *Private Communication*, Department of Mathematics, Old Dominion University, Norfolk, Virginia, (1997).

27. Michael Purser, *Introduction to Error-Correcting Codes*, Artech House, Inc., Norwood, (1995).

28. J. Rajkundlia, *Some Techniques for Constructing New Infinite Families of Balanced Incomplete Block Designs*, Ph.D. Dissertation, Queen's University, Kingston, Ontario, Canada, (1978).

29. H. J. Ryser, *Combinatorial Mathematics*, Carus Math. Monograph **14**, Wiley, New York, (1963).

30. G. E. Sacks, Multiple Error Correction by Means of Parity Checks, *IRE Trans.* **IT-4**, 145-147, (1958).

31. J. Seberry, A Construction for Generalized Hadamard Matrices, *J. Stat. Plann. and Inference* **4**, 365-368, (1980).

32. J. Seberry, Some Remarks on Generalized Hadamard Matrices and Theorems of Rajkundlia on SBIBDs, *Combinatorial Mathematics VI*, Lecture Notes In Mathematics **748**, Springer-Verlag, New York, (1979).

33. H. S. Shapiro and D. L. Slotnick, On the Mathematical Theory of Error Correcting Codes, *IBM J. Research Develop.* **3**, 25-34, (1959).

34. S. S. Shrikhande, Generalized Hadamard Matrices and Orthogonal Arrays of Strength Two, *Can. J. Math.* **16**, 736-740, (1964).

35. R. C. Singleton, Maximum Distance q-ary Codes, *IEEE Trans.* **IT-10**, 116-118, (1964).

36. E. Spence, A New Class of Hadamard Matrices, *Glasgow Journal* **8**, 59-62, (1967).

37. J. J. Stone, Multiple Burst Error Correction, *Inf. and Control* **4** 324-331, (1961).

38. D. Street, Generalized Hadamard Matrices, Orthogonal Arrays and F-Squares, *Ars. Combinatoria* **8**, 131-141, (1979).

39. R. L. Townsend and E. J. Weldon, Self-Orthogonal Quasi-Cyclic Codes, *IEEE Trans.* **IT-13**, 183-195, (1967).

40. N. T. Tsao-Wu and S. H. Chang, On the Evaluation of Minimum Distance of Binary Arithmetic Cyclic Codes, *IEEE Trans.* **IT-15**, 628-631, (1969).

41. R. J. Turyn, Hadamard Matrices, Baumert-Hall Units, Four Symbol Sequences, Pulse Compression and Surface Wave Encodings, *J. Combin. Theory (Series A)* **16**, 313-333, (1974).

42. W. Ulrich, Non-Binary Error Correction Codes, *Bell System Tech. J.* **36**, 1341-1388, (1957).

43. D. Underwood, *Elementary Number Theory*, W.H. Freeman Company, San Francisco, (1969).

44. R. R. Varsharmov, Estimate of the Number of Signals in Error Correcting Codes, *Doklady A. N. S. S. S. R.* **117**, 739-741, (1957).

45. K. Vijayan, Hadamard Matrices and Submatrices, *J. Australian Mathematical Society (Series A)* **22**, 469-475, (1976).

46. A. J. Viterbi, Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm, *IEEE Trans.* **IT-13**, 260-269, (1967).

47. T. J. Wagner, A Remark Concerning the Minimum Distance of Binary Group Codes, *IEEE Trans.* **IT-11**, 458, (1965).

48. J. Wallis, A Note of a Class of Hadamard Matrices, *J. of Combinatorial Theory* **6**, 222-223, (1969).

49. N. Wax, On Upper Bounds for Error Detecting and Error Correcting Codes of

Finite Length, *IRE Trans.* **IT-5**, 168-174, (1959).

50. E. J. Weldon, Decoding Binary Block Codes on Q-ary Output Channels, *IEEE Trans.* **IT-17**, 199-206, (1971).

51. F. H. Young, Analysis of Shift Register Counters, *J. A. C. M.* **5**, 385-388, (1958).

52. L. H. Zetterberg, Cyclic Codes for Irreducible Polynomials for Correction of Multiple Errors, *IEEE Trans.* **IT-8**, 13-21, (1962).

53. Neal Zierler, (1959). Linear Recurring Sequences, *J. Soc. Indust. Appl. Math.* **7**, 31-48, (1959).

Appendix 1:

Non-Quadratic Residues

In Chapter 2 the non-existence of some quadratic residues was stated without proof. Therefore, a model proof of the non-existence of a certain quadratic residue is now given.

Lemma 6.1.1 $x^2 \equiv 10(mod\ 17)$ *has no solutions (10 is not a quadratic residue of 17).*

Proof.

$$x^2 \equiv 10(mod\ 17) \Rightarrow x^2 = 10 + 17y \tag{6.1.1}$$

Clearly, no integer pairs $(17m, y)$ is a solution of (6.1.1).

Consider integers

$$x = 17m + n, \quad where \quad 0 < n < 17$$

$$x^2 = (17m)^2 + 34mn + n^2 \tag{6.1.2}$$

Now let $y = 17m^2 + 2mn$

Then (6.1.2) becomes

$$x^2 = 17y + n^2$$

But if $0 < n < 17$, $n^2 \not\equiv 10(mod\ 17)$ as the quadratic residues of 17 are $\{0, 1, 2, 4, 8, 9, 13, 15, 16\}$. Thus, $x^2 \equiv 10(mod\ 17)$ has no solutions. □

Lemma (6.1.1) implies $GH(17, 7)$ has no solutions. Therefore, the reciprocal pairs $GH(7, 17)$ and $GH(17, 7)$ do not exist. Indeed, the result can be used to prove the following theorem:

Theorem 6.1.1 *Some sequences of potential Hadamard matrices over Abelian group G of order $|G| = g$ which fail to exist are:*

1. $GH(7, 17 + 14(2^{k-1} - 1))$, *where k is a non-negative integer.*

2. $GH(7, 19 + 14(2^{k-1} - 1))$, *where k is a non-negative integer.*

Appendix 2:

Computer Program for Finding the Generator Polynomial of a Cyclic Code

```
C**********************************************************************
C  This program divides two monic polynomials, base p.
C  where the divisor is X^(N-1) - 1 and the dividend
C  is the irreducible generator of Gf(N), with N = P^M.
C**********************************************************************
      program Ndivide
      implicit real*8 (A-H, O-Z)
      parameter(IP = 3,M = 5,N = (IP) * *M,MP1 = M + 1,
     ISTOP = N - M)
      integer F(N), G(MP1), Q(N)
      do 10 JK = 1, 50
      do 9 I = 1, M + 1
      write(6,*) 'enter G(I), I = ', I
      read(5,*), G(I)
    9 continue
      write(6,*) (G(I), I=1,M+1)
      read(5,*) IGO
C**********************************************************************
C  initialize
      do I = 1, N
```

```
      F(I) = 0
      Q(I) = 0
    1 continue
      F(1) = 1
      F(N) = -1
C*************************************************************************
C   the case G(X) = X**2 + X + 2:
C   G(1) = 1
C   G(2) = 1
C   G(3) = 2
C   the case G(X) = X**3 + 2X + 1
C   G(1) = 1
C   G(2) = 0
C   G(3) = 2
C   G(4) = 1
C*************************************************************************
C   IQP is the position where the action starts
      IQP = 1
      do 2 I = 1, ISTOP
C   get multiplier
      IMULT=F(IQP)
      write(6,*) 'I, IQP, IMULT=', I, IQP, IMULT
      Q(IQP)=IMULT
```

```
C   update dividend
      IQP2 = 0
      do 3 J = 1, MP1
      IJ = IQP - 1 + J
C*************************************************************************
C   logic test
      if (IJ.gt.N) then
       write(6,*) 'past end'
       stop
      endif
      F(IJ) = F(IJ) - G(J) * IMULT
      if (F(IJ).lt.0) F(IJ) = F(IJ) + IP
      if (F(IJ).lt.0) F(IJ) = F(IJ) + IP
C*************************************************************************
C   logic test
      if (IJ.gt.0) then
       write(6,*) 'FIJ = 0 at wrong time'
       stop
      endif
C*************************************************************************
      if ((F(IJ).gt.0).and.(IQP2.eq.0)) then
       IQP2 = IJ
      endif
```

```
C*************************************************************************
   3  continue
      if (IQP2.gt.IQP) then
       IQP = IQP2
      else
       write(6,*) 'that is all she wrote! Q(I) ='
       write(6,*) (Q(L), L = 1, N - 1)
       go to 6
      endif
C*************************************************************************
   2  continue
      write(6,*) 'Q(I)='
      do 5 J = 1, N
      write(6,*) Q(J)
   5  continue
C*************************************************************************
   6  continue
C    count
      I1 = 0
      I2 = 0
      I3 = 0
      do 17 J = 1, N
      if (Q(J).eq.1) then
```

```
        I1 = I1 + 1
        go to 16
       else
        if (Q(J).eq.2) then
         I2 = I2 + 1
         go to 16
        else
         I3 = I3 + 1
         go to 16
        endif
       endif
   16  continue
   17  continue
       write(6,*) 'I1, I2, I3=', I1, I2, I3
C*************************************************************************
   10  continue
       stop
       end
```

Vita

Name: Iem H. Heng

Address: Department of Mathematics and Statistics, Old Dominion University, Norfolk, VA 23529.

Education: 1995 M.S. in App. Math., Western Michigan University, Kalamazoo, MI.
1993 B.S. in Mech. Engineer., Columbia University, New York, NY.
1991 B.S. in Math. & Pre-Engineer., Providence College, Providence, RI.

Experience: 1995-present Teaching Assistant, Old Dominion University, Norfolk, VA.

August 1995-December 1995 Research Assistant, NASA-Langley Research Center, Hampton, VA.

1993-1995 Teaching Assistant, Western Michigan University, Kalamazoo, MI.

1991-1993 Engineering Laboratory Assistant, Columbia University, New York, NY.

Awards: 1991-1993 Columbia University Scholarship.

1988-1991 Southeast Asia Scholarship & Rhode Island Scholarship.

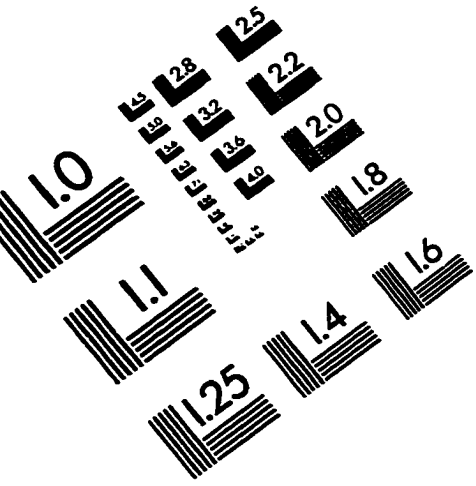
Publications: Heng, Iem H. and Cooke, Charlie H.
Error Correcting Codes Associated with Complex Hadamard Matrices,
Applied Mathematics Letters, Vol. 11, No. 4, pp. 77-80, 1998.

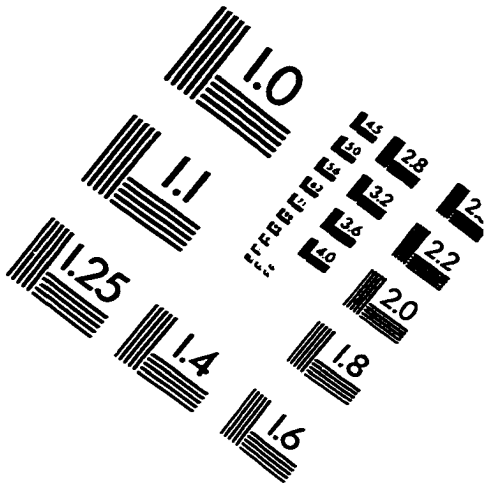
Cooke, Charlie H. and Heng, Iem (1997).
Polynomial Construction of Complex Hadamard Matrices with Cyclic core,
Applied Mathematics Letters, (In-Press).

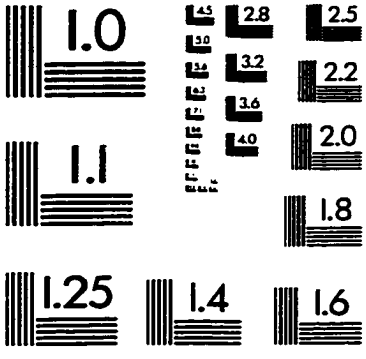
Cooke, Charlie H. and Heng, Iem (1998).
On the Non-Existence of Some Generalized Hadamard Matrices,
Aust. J. Comb., (In-Press).

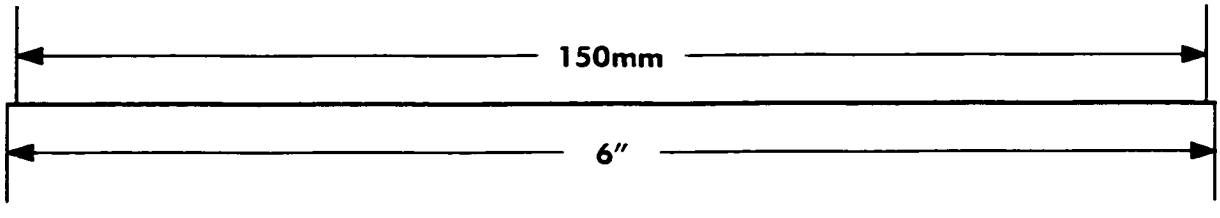
This dissertation was printed with **LATEK.**

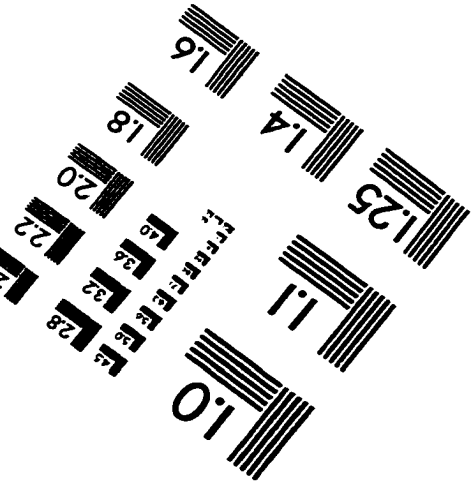
IMAGE EVALUATION
TEST TARGET (QA-3)

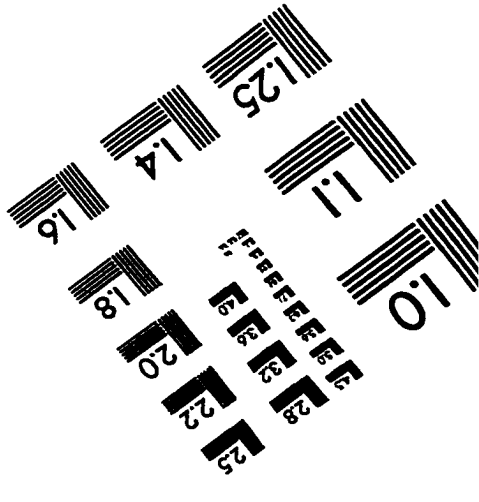












APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989