Old Dominion University
ODU Digital Commons

Mathematics & Statistics Faculty Publications | Mathematics & Statistics

1999

Polynomial Construction of Complex Hadamard Matrices with Cyclic Core

C. H. Cooke
Old Dominion University

I. Heng
Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/mathstat_fac_pubs

 Part of the Applied Mathematics Commons

Repository Citation

Cooke, C. H. and Heng, I., "Polynomial Construction of Complex Hadamard Matrices with Cyclic Core" (1999). *Mathematics & Statistics Faculty Publications*. 131.
https://digitalcommons.odu.edu/mathstat_fac_pubs/131

Original Publication Citation

Cooke, C. H., & Heng, I. (1999). Polynomial construction of complex Hadamard matrices with cyclic core. *Applied Mathematics Letters, 12*(1), 87-93. doi:10.1016/s0893-9659(98)00131-1

This Article is brought to you for free and open access by the Mathematics & Statistics at ODU Digital Commons. It has been accepted for inclusion in Mathematics & Statistics Faculty Publications by an authorized administrator of ODU Digital Commons. For more information, please contact digitalcommons@odu.edu.

PERGAMON

Applied Mathematics Letters 12 (1999) 87–93

Applied Mathematics Letters

Polynomial Construction of Complex Hadamard Matrices with Cyclic Core

C. H. COOKE AND I. HENG
Department of Mathematics and Statistics
Old Dominion University
Norfolk, VA 23529, U.S.A.

(Received and accepted November 1997)

Abstract—Conditions are given which are necessary and sufficient to ensure invariance of an M-sequence under periodic rearrangement. In conjunction with a certain uniformity property of polynomial coefficients, these conditions yield a simple method by which complex Hadamard matrices with cyclic core can be constructed. In such cases, a real p-ary linear cyclic error correcting code may be associated with the complex Hadamard matrix. © 1998 Elsevier Science Ltd. All rights reserved.

Keywords—Complex Hadamard matrix, Maximal period circulant, M-invariant sequence, Cyclic error-correcting code, Hadamard exponent.

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, 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 [1] shows how to construct from an appropriately chosen relative difference set, a cyclic matrix E_c 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 [1]. 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 references [2,3].

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 paper is to supply proof that this approach is generally applicable. In order to do so, it will first be necessary to develop 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.

0893-9659/98/$—see front matter © 1998 Elsevier Science Ltd. All rights reserved.
PII: S0893-9659(98)00131-1

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

M-SEQUENCES

Let V be an arbitrary vector of length N whose elements are in the finite field Gf(p), where p is a prime. Let the elements of vector V constitute the first period of an infinite sequence $a(V)$ which is periodic of period N.

Although by definition $a(V)$ has period N, smaller periods are conceivable. 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, the sequence $a(V)$ is called **M-invariant** under periodic rearrangement. In the sequel, the property of M-invariance is shown useful in constructing Hadamard matrices with cyclic core.

Classicly, for $N+1 = p^u$, an m-sequence is a solution of a linear difference equation of order u, which has least period N [4,5]. When the approach is taken of starting with vector V, and cycling to produce a sequence of period N, it may happen that the sequence satisfies a linear difference equation of order larger than u. Thus, every m-sequence is also an M-sequence, but the converse does not hold.

Let $V = [v_0 v_1 \dots v_{N-1}]$ be a particular vector over Gf(p). If j is a residue in Gf(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. Define a vector of multiplicities associated with V as $\zeta = (\lambda_j : j = 0, 1, 2, \dots, p-1)$.

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

THEOREM I. *Let $\zeta = [\lambda_0 \lambda_1 \dots \lambda_{p-1}]$ be a vector whose components are nonnegative integers which satisfy compatibility relations (I) and (II):*

$$\text{(I)} \qquad \sum_{j=0}^{p-1} \lambda_j = N;$$

$$\text{(II)} \qquad g.c.d.\,(\zeta, N) = q.$$

There exists a vector $V = [v_0 v_1 \dots v_{N-1}]$, $N > 1$, whose set of components contains the residues from Gf(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 nonnegative integer components satisfying (I) and (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 nonnegative integers ${\lambda_j}^0 = \lambda_j/q$, $j = 0, 1, \dots, p-1$, 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 each can be divided into subsets ${S_j}^i : i = 1, 2, \dots, q$ of cardinality ${\lambda_j}^0$. For $i = 1, 2, \dots q$, 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^* whose length is N by sequentially placing all elements of the group Q_i after the elements of Q_{i-1}, for $i = 2, 3, \dots, q$.

As it is clear that $a(V^*)$ is periodic of period L, $a(V)$ cannot 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) and (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 $\lambda_j = Q\lambda_j{}^0$, $j = 0, 1, \ldots, p-1$. Therefore, $g.c.d.(\zeta, N) = Q$, with $1 < Q < N$. This contradicts $q = 1$. Hence, the assumption that $a(V)$ is not M-invariant is false.

COMMENTS. Suppose V is of length N and its associated vector ζ of multiplicities has nonnegative integral components which satisfy (I) and (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 which are not M-invariant exist.

HADAMARD MATRICES AND GENERALIZED HADAMARD CODES

Hadamard matrices $H(p, q)$, of index p, are matrices of dimension $q \times q$, whose elements are p^{th} roots of unity and whose rows are orthogonal; precisely $HH^{CT} = qI$. For the case $p = 2$, the elements are ± 1, and the matrix is referred to as a classical Hadamard matrix. References [4,6–9] deal with theory and applications of classical Hadamard matrices, chiefly in the context of designs and codes.

For $p > 2$, the elements of a Hadamard matrix are numbers on the unit circle, and the terminology used is that of a complex, or generalized Hadamard matrix. References [1–3,10–12] are concerned with structure and properties of generalized Hadamard matrices.

Butson [10] proves that for primes $p > 2$, a necessary condition for existence of $H(p, q)$ is that $p \mid q$ (p divides q). Here, attention 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 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 elements of the Hadamard exponent matrix lie in the Galois field Gf(p), and its row vectors constitute the codewords of what shall be called a generalized Hadamard code. Depending upon the value of the integer t, either a linear group code or a nonlinear code may emerge. Several examples of generalized Hadamard codes are given in references [2,3].

A PROPERTY OF VECTORS OVER C_p. The problem of establishing the value $d(K)$, which represents the minimum Hamming distance between the codewords of a generalized Hadamard code K, is now reviewed.

Let $C_p = \{1, x, x^2, \ldots, x^{p-1}\}$ 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 $Q = \{a_i - b_i, \bmod p : i = 1, 2, \ldots, N\}$, and let n_q be the multiplicity of element q of Gf(p) which appears in Q.

PROPERTY U

Vector Q is said to satisfy **Property** U iff each element q of Gf(p) appears in Q exactly t times ($n_q = t$, $q = 0, 1, \ldots, p-1$).

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

LEMMA I. ORTHOGONALITY OF VECTORS OVER C_p. *For fixed primes p, arbitrary vectors A, B of length $N = pt$, whose elements are from C_p, are orthogonal iff the vector Q satisfies Property U, where Q is the collection of* mod p *differences between the Hadamard exponents associated with A, B.*

COMMENT 1. Lemma I above can be inferred from assertions of Butson [1], for which he provides no proof, but which he maintains are clearly valid. See also [2].

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 I. *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.

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 [1] 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.

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 nonzero codewords of a linear cyclic code K, if and only if there is polynomial $g(x)$ with coefficients in Gf(p), which is a proper divisor of $x^N - 1$ and which generates K [4,13]. In order to have N nonzero 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 [13], 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) [5]. A sufficient condition is that, in addition, a certain subset [1] 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 coefficients of the vector $[0, g(x)]$ be uniformly distributed over Gf(p): each residue $0, 1, \ldots, p-1$ 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 given in the sequel.

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 $h(x) \mid x^N - 1$, the ideal generated by $g(x)$, mod $x^N - 1$, will be a cyclic code K [4,13]. Moreover, Property U guarantees the nonzero 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 indicate that $\{0,1,6\}$ is the relative difference set, mod 8, which instead could be used to generate the cyclic core [10], certainly more intricately than by calculating the codewords associated with $g(x)$ using the cyclic shift operation.

POLYNOMIAL CONSTRUCTION OF COMPLEX HADAMARD MATRICES POSSESSING CYCLIC CORE

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

(1) *vector $\bar{C}=[0,c_0,c_1,\ldots,c_{N-1}]$ satisfies Property U,*
(2) *$g(x)h(x)=x^N-1$, 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 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 ${Z_p}^N$ [4,13], 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 I, 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 II. *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 $[0,g(x)]$ satisfies Property U,* mod p, *where p is prime.*

PROOF. It is clear that the lines of proof in Theorem II 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 $\{f_i(x): i=2,3,\ldots,N+1\}$. (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 [1], $h(x)$ is irreducible [5].

COMPUTER-AIDED CONSTRUCTION OF POLYNOMIAL PAIRS

In this section, there are given some results from computer-aided construction of the polynomial pairs $(g(x),h(x))$ which satisfy Theorem II. Table 1 shows typical irreducible $h(x)$, whose companion $g(x)$ (see Table 2) satisfies Property U.

Interestingly enough, analysis of the type represented by Table 1 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 1. 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 $x^4+x^3+x^2+2x+2$ $x^4+2x^3+x^2+x+2$
3^5	x^5+2x+1 x^5+2x^4+1 x^5+x^4+2x+1 x^5+2x^4+x+1 $x^5+x^3+2x^2+1$ $x^5+2x^3+x^2+1$ $x^5+x^4+2x^3+1$ x^5+x^3+x+1 $x^5+x^4+x^2+1$ $x^5+x^4+2x^3+x^2+x+1$ $x^5+2x^4+x^3+x^2+x+1$ $x^5+x^4+x^3+2x^2+x+1$ $x^5+x^4+x^3+x^2+2x+1$

Table 2. Coefficients of generating polynomials.

$N=p^n-1$	$g(x)=a_0+a_1x+\cdots+a_nx^n$
8	11202210 12202110
26	22201221202001110211210100 20212210222001012112011100 21112102022001222120101100 22020121112001101021222100
80	11112012112120202211020110012222021002000222 10212212101011220102200211012001000 12122011122220202112010210022122022002000212 10222111101012210201200112101100100 10011012110021020122101011112220112120002002 20212200120102112020222211102212100 10021011120022010221101012122120122220002001 20222100110201122020212112102111000 12211100220100101022102121101111210120002112 22001102002020112012122022221202100 11221200210200101021102222101212220220002211 21001201002020122011112021211101100

REFERENCES

1. J.A. Butson, Relations among generalized Hadamard matrices, *Can. J. Math.* **15**, 42–48, (1963).
2. C.H. Cooke and I. Heng, The Hadamard matroid and generalized Hadamard codes, In *Tenth Cumberland Conference on Graph Theory, Combinatorics, and Computing*, Emory University, Atlanta, GA, May 16–18, 1997.
3. C.H. Cooke and I. Heng, Error correcting codes associated with complex Hadamard matrices, *Appl. Math. Lett.* **11** (4), 77–80, (1998).
4. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, Ninth edition, North-Holland, Amsterdam, (1996).
5. N. Zierler, Linear recurring sequences, *J. Soc. Indust. Appl. Math.* **7** (1), 31–48, (1959).
6. E.F. Assmus and J.D. Key, *Designs and Their Codes*, Cambridge University Press, New York, (1992).
7. J.H. Beder, Conjectures about Hadamard matrices, In *R.C. Bose Memorial Conference on Statistical Design and Related Combinatorics*, Colorado State University, June 7–11, 1995.
8. A. Hedayat and W.D. Wallis, Hadamard matrices and their applications, *Annals of Statistics* **6** (6), 1184–1238, (1978).
9. K. Vijayan, Hadamard matrices and submatrices, *J. Australian Mathematical Society* **22**, 469–475, (1976).
10. J.A. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.* **13**, 894–898, (1962).
11. C.H. Cooke, The Hadamard matroid and an anomaly in its single element extensions, *JCMAA* **38** (7), 115–120, (1997).
12. S.S. Shrikhande, Generalized Hadamard matrices and orthogonal arrays of strength two, *Can. J. Math.* **16**, 736–740, (1964).
13. J. Adamek, *Foundations of Coding*, John Wiley, New York, (1991).