Linear Circulant Matrices Over A Finite Field

C. H. Cooke
Department of Mathematics
Old Dominion University
Norfolk, VA 23529, U.S.A.

(Received August 2003; revised and accepted April 2004)

Abstract—Rings of polynomials \( R_N = \mathbb{Z}_p[x]/x^N - 1 \) which are isomorphic to \( \mathbb{Z}_p^N \) are studied, where \( p \) is prime and \( N \) is an integer. If \( I \) is an ideal in \( R_N \), the code \( K \) whose vectors constitute the isomorphic image of \( I \) is a linear cyclic code. If \( I \) is a principle ideal and \( K \) contains only the trivial cycle \( \{0\} \) and one nontrivial cycle of maximal least period \( N \), then the code words of \( K/\{0\} \) obtained by removing the zero vector can be arranged in an order which constitutes a linear circulant matrix, \( C \). The distribution of the elements of \( C \) is such that it forms the cyclic core of a generalized Hadamard matrix over the additive group of \( \mathbb{Z}_p \).

A necessary condition that \( C = K/\{0\} \) be linear circulant is that for each row vector \( v \) of \( C \), the periodic infinite sequence \( a(v) \) produced by cycling the elements of \( v \) be period invariant under an arbitrary permutation of the elements of the first period. The necessary and sufficient condition that \( C \) be linear circulant is that the dual ideal generated by the parity check polynomial \( h(x) \) of \( K \) be maximal (a nontrivial, prime ideal of \( R_N \)), with \( N = p^k - 1 \) and \( k = \deg(h(x)) \). © 2004 Elsevier Ltd. All rights reserved.

1. INTRODUCTION

This paper represents an exposition of the connections between the following abstract constructs: polynomial ideals over a finite field [1]; linear cyclic codes [2]; linear difference equations [3]; linear circulant matrices [4], Butson Hadamard matrices [5] over a multiplicative cyclic group, generally having complex elements; and generalized Hadamard matrices over an additive Abelian group [6].

These concepts have evoked much interest in the literature, often in isolated realms. The intent here is to bring these ideas together in a way that shows clearly their complex and thought-provoking inter-relationships. What is actually seen is a combinatorial equivalence between certain specific subclasses of the above six constructs.

For those unfamiliar with the subject, classical Hadamard matrices are orthogonal matrices whose elements are square roots of unity. A natural generalization of the concept is Hadamard matrices whose elements are drawn from an Abelian group. For the case in which matrix dimension is \( q \) and elements are drawn from the cyclic group of \( p^k \) roots of unity, these generalized Hadamard matrices \( BH(p, q) \) are called Butson Hadamard matrices [5]. Later the concept of generalized Hadamard matrices \( H(p, p^k) \) over groups, which can be either multiplicative or additive, was formulated [6]. Examples of the two types will be given in Section 6.
2. SOME REMARKS ON LINEAR CYCLIC CODES

Let \( g(x) \) and \( h(x) \) be polynomials over the Galois field \( \mathbb{Z}_p \), which satisfy

\[
g(x)h(x) = x^N - 1,
\]

where \( h(x) \) is of degree \( k \) and \( g(x) \) is of degree \( N - k \). Let \( N \) be the length of code words in the linear cyclic code, \( K = K(g) \), generated by the polynomial \( g(x) \). \( K \) can be generated also using a linear difference equation determined by the coefficients of the parity check polynomial \( h(x) \), referred to here as the dual polynomial of \( g(x) \).

The vector \( g = [g_0 g_1 g_2 \ldots g_{n-k-1} oo \ldots o] \) indicates the codeword formed by the coefficients of \( g(x) \). Likewise, \( a(g) = [g_1 g_1 g_1 \ldots] \) denotes the infinite sequence of period \( N \) formed by cycling the elements of \( g \). \( N \) is not necessarily the least period of \( a(g) \). When the least period is \( N \), the sequence is called an \( M \)-sequence. The sequence is further called an \( M \)-invariant sequence, if the least period is \( N \), and sequences \( a(g^*) \) also have least period, \( N \), where \( g^* \) is an arbitrary permutation of the elements of vector \( g \). Thus, \( M \)-invariance means invariance of the least period under permutations. Necessary and sufficient conditions for \( M \)-invariance are obtained in reference [7].

It is well known [2] that the code \( K(g) \) is a cyclic linear subspace of \( \mathbb{Z}_p^N \). A cyclic code has the property that \( xc(x) \) is a codeword whenever \( c(x) \) is a codeword. The finite sequence \( C = \{c(x)| xc(x)| \ldots x^{T-1}c(x) \} \) is said to form a cycle of least period, \( T \), provided \( x^j c(x) = c(x) \) holds when \( j = T \), but not for integers \( 0 < j < T \). In particular, this means the sequence \( a(c) \) is periodic, of least period \( T \). A cycle is called maximal if and only if its least period is \( T = N \). Cyclic code \( K = \bigcup_{j=1}^S C_J \) is thus a finite union of its disjoint cycles.

3. MAXIMAL LINEAR CODES

Code \( K(g) \) is called maximal linear cyclic iff it is the union of the zero code word and a solitary maximal cycle, \( C^* \), formed by cycling \( g(x) \). \( K(g) \) also can be generated from the parity check polynomial, \( h(x) \), by considering code vectors obtained [3] by truncating after \( N \) terms distinct solutions of the linear difference equation \( \sum_{j=0}^k h_{k-j} v_{i+j} = 0 \).

Certainly, special conditions are required of \( N \) and \( g(x) \) in order for \( K \) to be maximal linear. As a minimum, it is necessary that there exist a prime \( p \) for which \( N = p^k - 1 \). This assures that the union of the zero code word and any possible maximal cycle generated by \( g(x) \) contains enough code words to fill out a linear space, without need for generation of other cycles.

Conditions that \( g(x) \) generate a maximal cycle are also required. A sufficient condition is that the code word \( g \) produces an \( M \)-invariant sequence \( a(g) \). The only maximal linear cyclic codes which are known to the author are the cyclic Hadamard codes [4]. Therefore, the \( M \)-sequence, \( a(g) \), in addition to being \( M \)-invariant, is required to have present each nonzero element of \( \mathbb{Z}_p \), with multiplicity, \( \lambda \), and the zero element, with multiplicity \( \lambda - 1 \), as well as \( \text{g.c.d.} \{\lambda, \lambda - 1, N\} = 1 \), where \( \lambda = p^{k-1} \). Of course, \( (p - 1)\lambda + \lambda - 1 = N \).

An interesting question, which for some time was puzzling to the author, is: can one do without the presence of some of the elements of \( GF(p) \), as \( M \)-invariance does not necessarily require it? As it turns out, the answer is no. A linear circulant must have present all nonzero elements of \( \mathbb{Z}_p \), or it cannot be both linear and nonzero.

Another question concerns distribution as regards element multiplicity within a row of a linear circulant, \( C \).

1. Since \( CU\{0\} \), is a linear space, for each row in which the unit element appears in the first position, \( C \) must contain a row \( i_j \) with element \( j \) in the first position, obtained upon multiplying row 1 by value(s) \( j = 1, 2, \ldots p - 1 \).

2. Likewise, after excepting the \( p - 1 \) rows previously enumerated, for each row remaining which has a nonzero element, \( k \), in column 1, a multiply by the inverse of \( k \) produces
another row not previously enumerated which has a unit first element. Each such "1" row implies the presence of a second group of \( p - 1 \) rows each with distinct nonzero first position. Continuing in this fashion, we see by induction that the element multiplicities for the first column satisfy the distribution equation

\[
D(\lambda, \lambda_0) = (p - 1)\lambda + \lambda_0 = N,
\tag{D}
\]

where the distribution of multiplicities of zero and nonzero elements of \( Z_p \) which occur in column 1 is, respectively, \( \lambda_0, \lambda \).

3. As \( C \) is a maximal period circulant, it can be generated by cycling the first row, in which case each nonzero element which appears in column one must also appear in row 1. By similar arguments applied to the other columns, each row and each column of a linear circulant with elements over \( Z_p \) must have the element distribution of equation (D) above.

**REMARK.** Distribution (D) is a necessary for a linear circulant. There are solutions of (D) for which the corresponding matrix is not a linear circulant. In the case where \( \lambda_0 = \lambda - 1 \) and \( C \) is a linear circulant matrix, \( C \) is the cyclic core of a generalized Hadamard matrix \( H = H(p, p\lambda) \) of dimension \( N + 1 \), over the additive group of \( Z_p \). \( H \) is formed by affixing to the cyclic core, \( C \), an extra row and column of zeros.

Moreover, \( H \) is the Hadamard exponent of a standard form Butson Hadamard matrix \( B = B(p, p\lambda) \), whose elements are \( p^{th} \) roots of unity. The connection is \( B = x^H \), where \( x \) is a primitive \( p^{th} \) root of unity, and the notation signifies matrix elements which satisfy \( b_{ij} = x^{h_{ij}} \). The distribution \( D(\lambda, \lambda - 1) \) now becomes the condition which assures that \( B \) is an orthogonal matrix. The additional zero appended in the first position assures that \( B \) is a Hadamard matrix in standard form.

4. **PRIME IDEALS AND MAXIMAL LINEAR CYCLIC CODES**

An ideal in the polynomial quotient ring \( R_N = Z_p[x]/x^N - 1 \) is a set of polynomials, \( I \), of degree \( d < N \), which is

(a) closed under addition and scalar multiplication of the elements within \( I \), as well as
(b) closed under multiplication by an arbitrary ring element, which may or may not be in \( I \).

Thus, the isomorphic image of \( I \) in \( Z_p^N \) is a linear cycle code, \( K(g) \), of length \( N \), where the polynomials \( g(x) \) of degree \( N - k \), and \( h(x) \) of degree \( k \), are dual divisors of zero: \( g(x)h(x) = x^N - 1 \). Moreover, \( I \) is the principle ideal \( (g(x)) \) generated by element \( g(x) \).

If \( h(x) \) is an irreducible primitive polynomial in \( Gf(p^k) \), then \( (h(x)) \) is a maximal (prime) ideal. (Otherwise, one arrives at a contradiction that \( h(x) \) is irreducible.) According to Zierler [1], if \( h(x) \) is primitive irreducible, each nonzero solution of the linear difference equation \( \sum_{j=0}^k h_{k-j}v_{i+j} = 0 \) has maximal least period \( N = p^k - 1 \).

Moreover, each cyclic translate of a nonzero solution is one of the other nonzero solutions. There are \( N + 1 \) distinct such solutions, each of which when truncated after \( N \) elements form a code word of \( K(g) \). (The parity check polynomial of code \( K(g) \) is \( h(x) \).) The code words of \( K(g) \) constitute a maximal linear code, since each nonzero codeword is a cyclic permutation of every other. Hence, there is a permutation matrix, \( P \), such that the matrix \( C = PK/(0) \) is a maximal linear circulant.

Conversely, if \( h(x) \) is not primitive, \( K(g) \) has more than one nontrivial cycle, so a linear circulant is impossible. Likewise, if \( N \) does not satisfy the above condition, \( K(g) \) will have too many code words for a single nontrivial cycle of period \( N \). By such arguments, one arrives at the result.

**Theorem 1.** *There is a maximal linear circulant matrix, \( C \), of dimension \( N \), with elements in the field \( Gf(p) \), if and only if there is a nontrivial prime ideal \( \langle h(x) \rangle \) in the ring of quotients \( R_N = Z_p[x]/x^N - 1 \).*
\[ \frac{Z_p[x]}{x^N - 1}, \] where \( h(x) \) is an irreducible primitive polynomial of degree \( k \) in \( \Gamma f(p^k) \), and \( N = p^k - 1 \).

**Corollary 1.** The maximal linear circulant of Theorem 1 is the cyclic core of a generalized Hadamard matrix \( H(p, p\lambda) \), where \( \lambda \) is the multiplicity of each nonzero element which appears in a row of \( C \). In turn, \( H \) is the Hadamard exponent of a Butson Hadamard matrix \( BH(p, p^k) \) whose elements are \( p^k \) roots of unity.

### 5. EXAMPLES OF CIRCULANT MATRICES

In this section the discussion of Sections 1–4 is clarified by recap and numerical examples, in what could be called a slide presentation format.

Matrix \( B = C(W) \) of dimension \( N \) is a circulant matrix means the following.

(a) \( B \) is generated from a vector \( W \) of length \( N \) by row wrap-a-round.
(b) Elements satisfy where \( b(i+1, j+1) = b(i, j) \), \( i, j = 0, 1, 2, N - 1 \), with \( (k) \) the mod \( N \) evaluation of \( k \), as a least nonnegative residue.

\( B \) is a linear circulant iff the rows of \( B \) together with the zero vector constitute a linear vector space over some field, \( \mathbb{F} \). The field of interest is \( \mathbb{Z}_p = \{0, 1, 2, \ldots, p - 1\} \).

**Distribution of Elements**

Circulant \( B = C(W) \) is called nondefective iff every nonnegative least residue of \( \mathbb{Z}_p \) is present among the components of \( W \).

\( C(W) \) is called a Hadamard (\( H \)-circulant) iff the respective multiplicity of zero and nonzero components of \( W \) is \( \lambda - 1, \lambda \) with \( N = P\lambda - 1 \). \( \lambda \) is an integer.

\( C(W) \) is a perfectly nondefective Hadamard (\( PH \)-circulant) iff, additionally, \( \lambda > 1 \). If \( \lambda = 1 \), \( C(W) \) is called Hadamard defective (HD-circulant).

**Maximality**

Circulant \( C(W) \) is called maximal iff the infinite sequence \( a(W) = \{W|W|W|\ldots\} \) generated by cycling the elements of \( W \) has least period \( T = N \). The row vectors of a maximal circulant form a single cycle of period \( N \).

**Theorem 2.** Every \( H \) or \( PH \) Circulant \( C(V), \dim(V) = N \), has least period \( T = N \).

**Proof.** Every \( H \) or \( PH \) Circulant \( C(W) \) has a companion \( M \)-invariant sequence \( a(W) \) of least period \( N \), where \( N = \dim(W) \). See Theorem 3 in the sequel.

**Example 1.**

\[
B = \begin{pmatrix}
1 & 2 & 3 & 4 \\
4 & 1 & 2 & 3 \\
3 & 4 & 1 & 2 \\
2 & 3 & 4 & 1
\end{pmatrix}
\]

Here, \( W = [1 \ 2 \ 3 \ 4] \), \( N = T = 4 \), and \( B(W) \) is maximal, Hadamard defective, but \( B \) is not a linear circulant. \( B \) is a nonlinear, cyclic Hadamard core. Attaching an extra first row and first column of zeroes will give a generalized Hadamard matrix \( H(5, 5) \) over an additive group.

**Example 2.**

\[
C = \begin{pmatrix}
1 & 2 & 1 & 2 \\
2 & 1 & 2 & 1 \\
1 & 2 & 1 & 2 \\
2 & 1 & 2 & 1
\end{pmatrix}
\]
$C$ is not maximal, since the infinite sequence $a(W)$ generated by cycling the elements of $W = [1 \ 2 \ 1 \ 2]$ has least period $P = 2 < N = 4$. Permutation $W_1 = [1 \ 2 \ 2 \ 1] \Rightarrow C(W_1)$ is period maximal. Sequence $a(W)$ is not period invariant under permutations of $W$.

**Example 3.**

$$D = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$ $D$ is a maximal, $PH$ nondefective, linear circulant, over $Z_2$.

**Examples 4 and 5.** Associated Hadamard matrices.

$$E = GH(2,4) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad F = H(2,4) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$ $E$ is a generalized Hadamard matrix over the binary additive group $G = \{0, 1\}$, with mod 2 addition. $D$ is called the linear cyclic core of $E$.

$E$ is the Hadamard exponent of Butson Hadamard matrix $F$, written as $F = (-1)^E$, where $F_{i,j} = (-1)^{E_{i,j}}$. Butson Hadamard matrices have elements which are $p^{th}$ roots of unity and in the present example is denoted as $F = BH(P, P\lambda)$. It is $GH$ over the multiplicative group $\{1, -1\}$.

**M-Sequences and M-Invariance**

When the least period of sequence $a(W)$ is exactly $N$, $a(W)$ is called an $M$-sequence, and the companion circulant $C(W)$ has maximal period.

When the period of $a(W)$ is invariant under arbitrary permutations of $W$, $a(W)$ is called $M$-invariant. A nonconstant $M$-invariant sequence has maximal period.

**Characterization of M-Invariance**

**Theorem 3.** (See [7].)

Let $V = [v_0 \ v_1 \ \ldots \ v_{N-1}]$ be a vector of least nonnegative residues over $Z_p$. If $j$ is a least nonnegative residue, let $\lambda_j$ be the multiplicity of $j$, as a member of the set of elements of $V$. If $j$ is not an element of $V$, define the multiplicity of $j$ to be zero. Let $\zeta = [\lambda_0, \lambda_1, \ldots, \lambda_{p-1}]$ be the corresponding vector of multiplicities of the elements of $V$, which satisfy compatibility conditions (I),(II)

$$\text{Condition (I)} \quad \sum_{j=0}^{P-1} \lambda_j = N, \quad \text{Condition (II) g.c.d.} \quad (\zeta, N) = q.$$ There exists a vector $V$ whose components satisfy the compatibility Conditions (I),(II), such that the infinite sequence $a(V)$ is $M$-invariant, if and only if $q = 1$.

**Lemma 1.** A sufficient condition that $a(V)$ be $M$-invariant is that the multiplicity vector $\zeta$ have components $\lambda_0 = \lambda - 1$ and $\lambda_j = \lambda > 0$, $j = 1, 2, \ldots, P - 1$, where $P$ is prime, $N = P\lambda - 1$, and vector $V$ over $Z_p$ has $\dim(V) = N$. Thus, every $H$ or $PH$-circulant $C(V)$ has $M$-invariant companion $a(V)$.

Proof follows from Theorem 2.

**Lemma 2.** A necessary condition that nondefective maximal circulant $C(V)$ over $Z_p$ be a linear circulant is that the distribution of the elements of an arbitrary row or column satisfy $(P - 1)\lambda + \lambda_0 = N$, where $\lambda_0, \lambda$ signify respective multiplicities of zero and nonzero residues of $Z_p$.

Proof. Use maximality, linearity of the vector space $CU\{0\}$, and wrap-around.
Remarks.

1. Theorems 2 and 3 give only sufficient conditions for obtaining a maximal period circulant $C(V)$ over $\mathbb{Z}_p$.
2. Not every maximal period circulant has an companion sequence $a(V)$ which is $M$-invariant.
   Rearranging $W = [1 \ 2 \ 1 \ 2]$ as $W_1 = [1 \ 1 \ 2 \ 2]$ gives a maximal period sequence $a(W_1)$ which is not period invariant.
3. Lemma 2 implies that a linear, $PH$-maximal circulant must satisfy $N = P\lambda - 1$.
4. As it turns out, every maximal period linear circulant $C(V)$ is also $M$-invariant, provided generating vector $V$ has no zero component in multiplicity vector $\zeta(V)$.

Theorem 4. See Theorem 1.

Maximal period $PH$-circulant $C(V)$ over $\mathbb{Z}_p$ is a linear circulant if and only if

(a) $N = P\lambda - 1$, where $P$ is prime, $K = \text{Rank}(C(V))$, $\lambda = P^{K-1}$, and $K > 0$.
(b) The components of Vector $V$ form the coefficients of a polynomial

$$g(x) = \sum_{j=0}^{N-1} V_j x^j$$

of degree $K$, such that $x^N - 1 = g(x)h(x)$.
(c) $h(x)$ is a primitive polynomial in $GF(P^K)$ of degree $N - k$, and each maximal period sequence $a(V^*)$ generated by an arbitrary row $V^*$ of $C(V)$ is a solution of the linear difference equation

$$\sum_{j=0}^{N-K} h_{N-K-j} V_j = 0$$

of order $N - K$.

Remark 5. Theorem 3 implies every linear $PH$-circulant over $\mathbb{Z}_p$ of dimension $N = P\lambda - 1$ forms the linear cyclic core of a Butson Hadamard matrix $BH(P, P\lambda)$ of dimension $N + 1 = P^K$, where $\lambda = P^{K-1}$ is the multiplicity of the nonzero elements in each row and column of the cyclic core $C(V)$.

Example 6. Binary arithmetic $g(x) = x + 1$ difference equation

$$C(V) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad V_{j+2} + V_{j+1} + V_j = 0,$$

$$h(x) = 1 + x + x^2. \quad g(x)h(x) = x^3 - 1, \text{ mod } 2,$$

$[1 \ 1 \ 1]$ is the only independent null vector of $C(V)$, and it is orthogonal to each row of $C(V)$.

Remark 6. A defective circulant can be maximal but not linear—a well-chosen linear row combination can generate a row with an arbitrary missing residue.

Remark 7. A circulant which is not maximal cannot be linear, as repeated vectors are not permissible in a linear space.

Remark 8. If the dimension is not $N = P\lambda - 1$, a linear circulant core does not exist. In certain cases the corresponding Hadamard matrix is known not to exist, even if $N = P\lambda - 1$. When $\lambda = 1$ the $H$-circulant is nonlinear.
EXAMPLE 7. Mod 3 arithmetic

\[ g(x) = x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1, \quad h(x) = x^2 + x + 2, \quad g(x)h(x) = x^8 - 1, \mod(3), \]

\[ C(V) = \begin{bmatrix}
1 & 1 & 2 & 0 & 2 & 2 & 1 & 0 \\
0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \\
1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 \\
2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 \\
2 & 2 & 1 & 0 & 1 & 1 & 2 & 0 \\
0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 \\
2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 \\
1 & 2 & 0 & 2 & 2 & 1 & 0 & 1
\end{bmatrix}. \]

Difference equation: \( V_{j+2} + 2V_{j+1} + 2V_j = 0, \mod(3) \) \( N = 8, K = 2, \lambda = 3, P = 3. \)

REFERENCES