Difference Sets of the Hadamard Type and Quasi-Cyclic Codes*

V. K. BHARGAVA†, S. E. TAVARES

Department of Electrical Engineering, Queen's University, Kingston, Ontario

AND

S. G. S. SHIVA

Department of Electrical Engineering, University of Ottawa, Ottawa, Ontario

For every twin prime and prime power \( p \) where \( p = 3(4) \) we define a \((2p + 2, p + 1)\) binary code by a generator matrix of the form \( G = [I, S_p] \), where \( S_p \) is given in terms of the incidence matrix of a difference set of the Hadamard type. For \( p = 3(8) \) these codes are shown to be self-dual with weights divisible by four. For \( p = 7, 15, 23, 27, 31 \) and 35 the codes obtained are probably new and it is not known if they are related to cyclic codes. For \( p = 7, 15, 19 \) and 23 we present their weight distributions.

I. INTRODUCTION

For every twin prime and odd prime power \( p \equiv 3(4) \), \((2p + 2, p + 1)\) codes over \( GF(2) \) can be defined in a manner somewhat analogous to symmetry codes over \( GF(3) \) of Pless (1972). We define each code by a generator matrix of the form \( G = [I, S_p] \), where \( S_p \) is given in terms of the incidence matrix of a difference set of the Hadamard type. The matrix \( S_p \) is intimately associated with the construction of Hadamard matrices (Wallis, Street and Wallis, 1972).

* This research was supported in part by the National Research Council of Canada.
† Present address: Centre for Information Processing, Dept. of Elect. Communication Engineering, Indian Institute of Science, Bangalore, India.
‡ It has been pointed out to the authors by Dr. I. F. Blake of the University of Waterloo that the results of this paper still hold if \( p = r^m(r^m + 2) \) where \( r^m \) and \((r^m + 2)\) are both prime powers. If \( m = 1 \), \( p \) reduces to a “twin prime.”

Copyright © 1974 by Academic Press, Inc. All rights of reproduction in any form reserved.
The code generated by \( G = [I, S] \) will be referred to as \( C(p) \). The dual code \( C^*(p) \) consists of all vectors \( \bar{v} \) such that \( \bar{u} \cdot \bar{v} = 0 \) for all \( \bar{u} \in C(p) \). \( C(p) \) is self-dual if \( C(p) = C^*(p) \). For every twin prime and odd prime power \( p = 3(8) \), the \((2p + 2, p + 1)\) codes are shown to be self-dual with weights divisible by four. If \( p = 3(8) \) is a prime, then these codes are the extended codes of Karlin (1969). More recently MacWilliams and Karlin (1974) have shown that these codes are in fact the binary images of the \((p + 1, (p + 1)/2)\) extended quadratic residue codes over \( GF(4) \).

For \( p = 7, 15, 23, 27, 31 \) and 35 the codes obtained are probably new and it is not known if they are related to cyclic codes. For \( p = 7, 15, 19 \) and 23 we present their weight distributions.

II. DIFFERENCE SETS OF THE HADAMARD TYPE

To make the statement of our results precise we need some definitions and results from Combinatorics. For a complete study of these concepts we refer the reader to Hall (1967) or Baumert (1971).

**Definition.** A set of \( k \) residues \( D = \{a_1, \ldots, a_k\} \) modulo \( v \) is called a \((v, k, \lambda)\) difference set if for every \( d \equiv 0 \pmod{v} \) there are exactly \( \lambda \) ordered pairs \((a_i, a_j), a_i, a_j \in D\) such that \( a_i - a_j \equiv d \pmod{v} \). By a complementary difference set \( D^* \) we mean a \((v - 1, v - k, v - 2k + \lambda)\) difference set such that \( D + D^* = \{0, 1, \ldots, v - 1\} \).

**Definition.** A subset \( D = \{x_1, \ldots, x_k\} \) of elements of an additive Abelian group \( G \) of order \( v \) is called a \((v, k, \lambda)\) group difference set if for every \( y \neq 0 \in G \) there are exactly \( \lambda \) ordered pairs \((x_i, x_j)\) such that \( x_i - x_j = y \).

**Definition.** The incidence matrix \( A = (a_{ij}) \) of a \((v, k, \lambda)\) group difference set \( D \) is defined by ordering the elements of the group \( G = \{g_{ij}\} \) (or the integers modulo \( v \)) as \( g_1, g_2, \ldots, g_v \) and defining

\[
a_{ij} = \begin{cases} 1, & g_i - g_j \in D \\ 0, & \text{otherwise} \end{cases}
\]

The following theorem will play an important role in this paper:

**Theorem 2.1.** If \( A \) is the incidence matrix of a \((v, k, \lambda)\) difference set then \( A \) satisfies
(i) $AA^T = (k - \lambda) I + \lambda J$
(ii) $AJ = JA = kJ$

where every element of the $v \times v$ matrix $J$ is plus one.

**Proof.** See Baumert (1971)

Difference sets whose parameters $(v, k, \lambda) = (4t - 1, 2t - 1, t - 1)$ or its complement $(v, k^*, \lambda^*) = (4t - 1, 2t, t)$ are called Hadamard difference sets. In this paper we are concerned with the following two families of the Hadamard difference sets:

(a) quadratic residues in $GF(p^r)$, $v = p^r = 4t - 1$,

(b) twin primes, $v = p(p + 2)$ where $p$ and $p + 2$ are both prime numbers. Necessarily $p(p + 2) = 3(4)$.

These difference sets are listed in the book of Baumert (1971) and therefore we have omitted the details for constructing them.

### III. The Codes

We follow the notation of Pless (1972). For a twin prime or prime power $p = 3(4)$ the $(2p + 2, p + 1)$ code is specified by a generator matrix $G = [I, S_p]$ where $I$ is the $(p + 1) \times (p + 1)$ identity matrix and $S_p$ is as described below.

We define $S_p$ to be a $(p + 1) \times (p + 1)$ matrix $s_{ij}$, $i, j = 0, 1, \ldots, p - 1$ such that $s_{0,0} = 0$ and for $i, j \neq \infty$, $s_{i,0} = s_{0,j} = 1$. The remaining "core" or "finite part" of the matrix is the incidence matrix $A$ of a difference set of the Hadamard type.

It can be shown that (Baumert, 1971), if $p$ is a prime or twin prime, the incidence matrix $A$ is a circulant matrix. In this situation the corresponding difference set is also called a "cyclic" difference set. The algebra of $m \times m$ circulant matrices over $GF(q)$ is isomorphic to that of polynomials mod $x^m - 1$ over $GF(q)$ with the following one-to-one correspondence:

$$C = \begin{bmatrix} c_0 & c_1 & \cdots & c_{m-1} \\ c_{m-1} & c_0 & \cdots & c_{m-2} \\ \cdots & \cdots & \cdots & \cdots \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix} \leftrightarrow c(x) = c_0 + c_1x + \cdots + c_{m-1}x^{m-1}$$

Thus we shall often speak of the circulant $C$ as being specified by the "associated" polynomial $c(x)$. 
Let \( j = (1, 1, \ldots, 1) \) be a row of \( p \) ones. Then the matrix \( S_p \) is

\[
S_p = \begin{bmatrix}
0 & j \\
j^T & A
\end{bmatrix}.
\]

**Lemma 3.1.** Let \( p \) be a twin prime or prime power such that \( p \equiv 3(8) \) and let \( A \) be the incidence matrix of the \((p, (p + 1)/2, (p + 1)/4)\) Hadamard difference set. Then over \( GF(2) \)

(i) \( AA^T = I + J \), mod 2,

(ii) \( Aj^T = \phi^T, jA^T = \phi \), mod 2, where \( \phi = (0, 0, \ldots, 0) \) is a row of \( p \) zeros.

**Proof.** (i) From Theorem 2.1 with \( k = (p + 1)/2 \) and \( \lambda = (p + 1)/4 \)

\[
AA^T = \left( \frac{p + 1}{4} \right) I + \left( \frac{p + 1}{4} \right) J.
\]

Since \( p \equiv 3(8) \) it follows that

\[
AA^T = I + J \text{ over } GF(2).
\]

(ii) This is true since \((p + 1)/2\) is even. \( \quad \) Q.E.D.

With \( A \) the matrix of Lemma 3.1, we are now ready to prove the following:

**Theorem 3.1.** Let \( p \) be a twin prime or prime power such that \( p \equiv 3(8) \) and let \( S_p \) be as previously described, then the matrix \( S_p \) is orthogonal over \( GF(2) \), that is \( S_pS_p^T = I \).

**Proof.** Consider the matrix product

\[
S_p S_p^T = \begin{bmatrix}
0 & j \\
j^T & A
\end{bmatrix} \begin{bmatrix}
0 & j \\
j^T & A
\end{bmatrix}^T
\]

\[
= \begin{bmatrix}
j^T & jA^T \\
A^T & j^T j + AA^T
\end{bmatrix}.
\]

Thus from Lemma 3.1 and noting that \( j^T j = J \)

\[
S_p S_p^T = \begin{bmatrix}
1 & \phi \\
\phi^T & J + I + J
\end{bmatrix} = I \text{ over } GF(2).
\]

**Q.E.D.**

**Corollary 3.1.** For every twin prime and prime power \( p \), where \( p \equiv 3(8) \), \( C(p) \) is self-dual; hence the weight of any code word is divisible by four.
Proof. Note that each row in \( G = [I, S_p] \) has weight \( p + 1 \) or \( (p + 5)/2 \). Since \( p = 3(\mathbb{Z}) \) by assumption, both \( p + 1 \) and \( (p + 5)/2 \) are divisible by four. Thus the dot product of every row with itself over GF(2) is zero. Hence the row vectors of \( G \) are self-orthogonal. Since \( S_p S_p^T = I \), the rows of \( S_p \) are orthogonal to each other, hence the rows of \( G = [I, S_p] \) are orthogonal to each other. This proves that \( C(p) \) is self-dual.

The fact that the weights in \( C(p) \) are divisible by four is true by the formula \( ||\bar{u} + \bar{v}|| = ||\bar{u}|| + ||\bar{v}|| - 2 ||\bar{u} \cap \bar{v}||, \bar{u}, \bar{v} \in G \) and \( ||\bar{u} \cap \bar{v}|| \) is even. Here \( \bar{u} \cap \bar{v} \) is the vector which has a 1 at places where both \( \bar{u} \) and \( \bar{v} \) have a 1 and is 0 elsewhere.

Q.E.D.

Unless specified otherwise we shall take the “core” \( A \) of \( S_p \) to be the incidence matrix of a \((p, (p + 1)/2, (p + 1)/4)\) Hadamard difference set. The following lemma is of help in determining the minimum weight in \( C(p) \).

Lemma 3.2. (a) The weight of every vector in the basis \( G = [I, S_p] \) is \( p + 1 \) or \( (p + 5)/2 \). (b) The weight of any linear combination of two vectors in the basis \( G = [I, S_p] \) is \( (p + 5)/2 \). (c) The linear combination of any \( k \) rows in the basis \( G = [I, S_p] \) has weight exceeding \( k \).

Proof. (a) This is true by observation.

(b) Let \( \bar{u} \) and \( \bar{v} \in S_p \) and assume that \( ||\bar{u}|| = ||\bar{v}|| = (p + 3)/2 \). Then

\[
||\bar{u} + \bar{v}|| = ||\bar{u}|| + ||\bar{v}|| - 2 ||\bar{u} \cap \bar{v}||
= \frac{p + 3}{2} + \frac{p + 3}{2} - 2 \left( \frac{p + 1}{4} + 1 \right).
\]

(Since the core is the incidence matrix of a \((p, (p + 1)/2, (p + 1)/4)\) difference set, any two rows of the core must have \((p + 1)/4\) ones in common), i.e.,

\[
||\bar{u} + \bar{v}|| = \frac{p + 1}{2}.
\]

Thus the weight of the sum of two rows is

\[
2 + \frac{p + 1}{2} = \frac{p + 5}{2}.
\]

The case when either \( ||\bar{u}|| \) or \( ||\bar{v}|| = p + 1 \) can be treated similarly.

(c) This is true since \( S_p \) is nonsingular over GF(2).
IV. THE FIRST TEN CODES

We have a computer programme which determines the weight distribution of systematic rate $1/2$ quasi-cyclic codes and the steps in the code construction are as follows: (i) If $p$ is a twin prime or prime power then the core $A$ of $S_p$ is a circulant matrix. The corresponding difference set was obtained from the list of difference sets in Baumert (1971); (ii) The weight distribution of the $(2p, p, p)$ code generated by the matrix $G = [I, A]$ was computed; (iii) From the weight distribution of the $(2p, p)$ quasi-cyclic code, the weight distribution of the $(2p + 2, p + 1)$ code was determined. For $p = 31$ and 35 only the minimum distance could be computed. The case of prime powers needs special consideration.

**Case I.** Let $p = 3$. Here $D = \{0, 2\}$ is a $(3, 2, 1)$ cyclic difference set. The incidence matrix generates a $(6, 3), d = 3$ quasi-cyclic code with generator polynomial $a(x) = 5$ (in octal notation).

$C(3)$ corresponds to a $(8, 4), d = 4$ code. This code is equivalent to the extended Hamming code whose weight distribution is well known.

**Case II.** Let $p = 7$. Here $D = \{0, 3, 5, 6\}$ is a $(7, 4, 2)$ cyclic difference set. The $(14, 7), d = 3$ quasi-cyclic code is generated by $a(x) = 454$.

$C(7)$ corresponds to a $(16, 8)$ code having the following weight distribution;

- $A_0 = A_{16} = 1 = 1$
- $A_4 = A_{12} = 14 = 2 \times 7$
- $A_6 = A_{10} = 56 = 8 \times 7$
- $A_8 = 114 = 2 + 16 \times 7$

**Case III.** Let $p = 11$. Here $D = \{0, 2, 6, 7, 8, 10\}$ is a $(11, 6, 3)$ cyclic difference set. The $(22, 11), d = 7$ quasi-cyclic code is generated by $a(x) = 5072$.

$C(11)$ corresponds to a $(24, 12), d = 8$ code. This code is equivalent to the well-known extended Golay code whose weight distribution is known.

**Case IV.** Let $p = 15$, a twin prime. Here $D = \{0, 1, 2, 4, 5, 8, 10\}$ is a $(15, 7, 3)$ cyclic difference set. The $(30, 15), d = 4$ quasicyclic code is generated by $a(x) = 7312$. However, if we add a 1 in position 14 to make the total weight even, then $a(x) = 73121$ generates a $(30, 15), d = 7$ quasi-cyclic

---

2 A $(2m, m)$ rate $1/2$ quasi-cyclic code in the systematic form has a generator matrix $G = [I, C]$, where $C$ is a $m \times m$ circulant and is said to be generated by $C$ or equivalently by the associated polynomial $c(x)$. 
code. This corresponds to a (32, 16) code, having the following weight distribution:

\[
\begin{align*}
A_0 &= A_{32} = 1 = 1 \\
A_8 &= A_{24} = 380 = 25 \times 15 + 1 \times 5 \\
A_{10} &= A_{22} = 1,920 = 128 \times 15 \\
A_{12} &= A_{20} = 7,168 = 477 \times 15 + 2 \times 5 + 1 \times 3 \\
A_{14} &= A_{18} = 13,440 = 896 \times 15 \\
A_{16} &= 19,718 = 1,312 \times 15 + 6 \times 5 + 2 \times 3 + 2
\end{align*}
\]

It is known that there is no (32, 16) extended cyclic code with the above weight distribution (Goethals, 1965). However, there is a (32, 16) quasi-cyclic code generated by \( c(x) = 40276 \) which has the above mentioned weight distribution.

**Case V.** Let \( p = 19 \). Here \( D = \{0, 2, 3, 8, 10, 12, 13, 14, 15, 18\} \) is a \((19, 10, 5)\) cyclic difference set. The \((38, 19), d = 7\) quasi-cyclic code is generated by \( a(x) = 5412744 \).

\( C(19) \) corresponds to a \((40, 20)\) code having the following weight distribution.

\[
\begin{align*}
A_0 &= A_{40} = 1 = 1 \\
A_8 &= A_{32} = 285 = 3 \times 5 \times 19 \\
A_{12} &= A_{28} = 21,280 = 2^6 \times 5 \times 7 \times 19 \\
A_{16} &= A_{24} = 239,970 = 2 \times 3 \times 5 \times 421 \times 19 \\
A_{20} &= 525,504 = 2^6 \times 13,829 \times 19
\end{align*}
\]

**Case VI.** Let \( p = 23 \). Here \( D = \{0, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\} \) is a \((23, 12, 6)\) cyclic difference set. The \((46, 23), d = 7\) quasi-cyclic code is generated by \( a(x) = 41231536 \).

\( C(23) \) corresponds to a \((48, 24)\) code having the following weight distribution:

\[
\begin{align*}
A_0 &= A_{48} = 1 = 1 \\
A_8 &= A_{40} = 759 = 3 \times 11 \times 23 \\
A_{12} &= A_{36} = 7,130 = 2 \times 5 \times 31 \times 23 \\
A_{14} &= A_{34} = 49,128 = 2^3 \times 3 \times 89 \times 23 \\
A_{16} &= A_{32} = 286,143 = 3 \times 11 \times 13 \times 29 \times 23 \\
A_{18} &= A_{30} = 900,680 = 2^3 \times 5 \times 11 \times 89 \times 23
\end{align*}
\]
\[ A_{20} = A_{28} = 1,926,342 = 2 \times 3^4 \times 11 \times 47 \times 23 \]
\[ A_{22} = A_{26} = 3,242,448 = 2^4 \times 3^2 \times 11 \times 89 \times 23 \]
\[ A_{24} = 3,951,954 = 2 + 2^4 \times 10,739 \times 23 \]

Case VII. Let \( p = 3^3 = 27 \). In \( GF(3^3) \) with \( x^3 = x + 2 \)

\[ D = \{0, x, x + 2, 2x^2 + x + 2, x^2 + 2x + 2, x + 1, x^2 + x + 2, 2, 2x^2, 2x^2 + x, 2x^2 + 2x + 2, x^2 + 1, 2x^2 + 2x, 2x^2 + 1\} \]

is a (27, 14, 7) group difference set. The incidence matrix is given by

\[
A = \begin{bmatrix}
P & Q & R \\
R & P & Q \\
Q & R & P 
\end{bmatrix}
\]

and each of \( P, Q \) and \( R \) is comprised of nine \( 3 \times 3 \) circulants which are given by:

\[
P = \begin{bmatrix}
p_1 & p_2 & p_3 \\
p_3 & p_1 & p_2 \\
p_2 & p_3 & p_1
\end{bmatrix}
\]

with \( p_1 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \), \( p_2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \), and \( p_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \),

\[
Q = \begin{bmatrix}
q_1 & q_2 & q_3 \\
q_3 & q_1 & q_2 \\
q_2 & q_3 & q_1
\end{bmatrix}
\]

with \( q_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \), \( q_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \), and \( q_3 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \),

and

\[
R = \begin{bmatrix}
r_1 & r_2 & r_3 \\
r_3 & r_1 & r_2 \\
r_2 & r_3 & r_1
\end{bmatrix}
\]

with \( r_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \), \( r_2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \), and \( r_3 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \).

C(27) corresponds to a (56, 28) code. Since the incidence matrix is no longer a “simple” circulant we cannot use our computer program. The possible values for the minimum \( d = 8 \) or 12. We have ruled out the possibility of \( d = 4 \) by simple hand computations.

Case VIII. Let \( q = 31 \). Here \( D = \{0, 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30\} \) is a (31, 16, 8) cyclic difference set. The \( (62, 31), d = 7 \) quasi-cyclic code is generated by \( a(x) = 44416507554 \).

C(31) corresponds to a (64, 32), \( d = 8 \) code.
Case IX. Let \( q = 35 \) a twin prime. Here \( D = \{2, 5, 6, 8, 10, 15, 18, 19, 20, 22, 23, 24, 25, 26, 30, 31, 32, 34\} \) is a \((35, 18, 9)\) cyclic difference set. The \((70, 35), d = 11\) quasi-cyclic code is generated by \( a(x) = 115204737072 \). \( C(35) \) corresponds to a \((72, 36), d = 12\) code.

Remark 4.1. The \((72, 36)\) extended quadratic residue code over \( GF(2) \) also has minimum distance 12 and weights divisible by four. However the (circulant) orthogonal complement of weight 14 and order 35 for this code found by Karlin (1969) is not seen to be equivalent so far to the (circulant) orthogonal complement of weight 18 and order 35 that we have reported above. The equivalences tried so far as those reported by Tavares, Bhargava and Shiva (1974).

Case X. Let \( p = 43 \). Here \( D = \{0, 2, 3, 5, 7, 8, 12, 18, 19, 20, 22, 26, 27, 28, 29, 30, 32, 33, 34, 37, 39, 42\} \) is a \((43, 22, 11)\) cyclic difference set. The \((86, 43), d = 15\) quasi-cyclic code is generated by

\[
a(x) = 553040721756244.
\]

\( C(43) \) corresponds to a \((88, 44), d = 16\) code of MacWilliams and Karlin (1974).

Acknowledgments

We are very grateful to Mr. Jack Stein for his expert programming. We acknowledge helpful discussions with Dr. Jennifer Wallis, Mr. Maurice Karlin and Dr. F. J. MacWilliams.

Received: July 30, 1973; Revised: June 11, 1974

References


Pless, V. (1972), Symmetry codes over $GF(3)$ and new five-designs, *J. Combinatorial Theory* 12, 119.
