Projective Spaces and Quasi-Cyclic Codes[1]

T. Aaron Gulliver and Vijay K. Bhargava[2]

Abstract

A family of double circulant quasi-cyclic codes is constructed from the incidence matrices of difference sets associated with hyperplanes in projective space. A subset of these codes leads to a class of doubly-even self-orthogonal codes, and two classes of self-dual codes.

Keywords: quasi-cyclic codes, self-dual codes, incidence matrices

1 Introduction

A binary $[n, k]$ linear code C is a k-dimensional vector subspace of $GF(2)^n$, where $GF(2)$ is the field of 2 elements. The elements of C are called codewords and the Hamming weight of a codeword is the number of non-zero coordinates. An $[n, k, d]$ code is an $[n, k]$ code with minimum (non-zero) Hamming weight d. The weight enumerator $W_C(y)$ of a code C is given by $W_C(y) = \sum_{i=0}^{n} A_i y^i$ where A_i is the number of codewords of weight i in C. The numbers $A_0, \cdots, A_n$ are called the weight distribution of C.

Two codes are equivalent if one can be obtained from the other by a permutation of coordinates. An automorphism of C is a permutation of the

[1]This work was supported in part by the Natural Sciences and Engineering Research Council of Canada.

[2]T. Aaron Gulliver is with the Department of Electrical and Electronic Engineering, University of Canterbury, Christchurch, New Zealand, gulliver@elec.canterbury.ac.nz. Vijay K. Bhargava is with the Department of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, MS 8610, Victoria, B.C., Canada V8W 3P6, bhargava@sirius.uvic.ca

coordinates of C which preserves C. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in GF(2)^n | \ x \cdot y = 0 \forall y \in C\}$. C is *self-orthogonal* if $C \subseteq C^{\perp}$, and *self-dual* if $C = C^{\perp}$. A code is *doubly-even* if all codewords have weight divisible by four, and *singly-even* if all weights are even and there is at least one codeword of weight $\equiv 2 \pmod 4$. A self-dual code is *extremal* if it has the largest possible minimum weight for that length. A code C is *formally self-dual* if the codes C and $C^{\perp}$ have identical weight distributions. Self-dual codes are formally self-dual, but there are formally self-dual codes which are not self-dual. A formally self-dual code is *divisible* if there exists a positive integer $\delta > 1$ such that δ divides all non-zero weights in the code. Formally self-dual codes with $\delta = 2$ are called *formally self-dual even.*

Let V be an $(n+1)$-dimensional vector space over the field $GF(q)$ of q elements. The *projective space* $PG(n,q)$ is the set of all vector subspaces of V [2]. An i-flat is a subspace of dimension $i+1$. The 0-flats are therefore points, and the 1-flats are lines. The $(n-1)$-flats are called hyperplanes. It is well known that the points and hyperplanes of $PG(n,q)$ form a symmetric block design with [3]

$$v = \frac{q^{n+1}-1}{q-1}, k = \frac{q^n-1}{q-1}, \lambda = \frac{q^{n-1}-1}{q-1}. \tag{1}$$

Singer [4] showed that this design corresponds to a cyclic difference set. Let R denote the incidence matrix of this difference set. It is well known that R is an orthogonal circulant matrix, i.e., $RR^T = I$ over GF(2). An $m \times m$ circulant matrix R is defined as

$$R = \begin{bmatrix} r_0 & r_1 & r_2 & \cdots & r_{m-1} \\ r_{m-1} & r_0 & r_1 & \cdots & r_{m-2} \\ r_{m-2} & r_{m-1} & r_0 & \cdots & r_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ r_1 & r_2 & r_3 & \cdots & r_0 \end{bmatrix}, \tag{2}$$

where each successive row is a right cyclic shift of the previous one. The algebra of $m \times m$ circulant matrices over GF(2) is isomorphic to the algebra of polynomials in the ring $f[x]/(x^m-1)$ if R is mapped onto the polynomial, $r(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{m-1} x^{m-1}$, formed from the entries in the first row of R [1].

A code is called *quasi-cyclic* (QC) if there is some integer p such that every cyclic shift of a codeword by p positions is again a codeword [1, ch.

16, p. 506]. The blocklength, n, of a QC code must be a multiple of p, with p the least positive integer for which the code is invariant under a cyclic shift by p positions. By rearranging the columns of the generator matrix, many QC codes can be transformed into an equivalent code with generator matrix

$$G' = [R_0;\ R_1;\ R_2;\ \ldots;\ R_{p-1}], \tag{3}$$

where R_i is an $m \times m$ circulant matrix, so that $n = mp$. The $r_i(x)$ associated with this QC code are called the *defining polynomials* [5]. If $p = 2$, the code is called *double circulant* (DC). A DC code C is equivalent to its dual $C^{\perp}$ [1], so that all DC codes are formally self-dual.

If the defining polynomials $r_i(x)$ contain a common factor which is also a factor of $x^m - 1$, then the QC code is called *degenerate* [5]. Define the *order* of the QC code defined in (3) as [6]

$$h(x) = \frac{x^m - 1}{(x^m - 1, r_0(x), r_1(x), \cdots, r_{p-1}(x))}. \tag{4}$$

The dimension K of the QC code is equal to the degree of $h(x)$. If $\deg(h(x)) \equiv K < m$, a generator matrix can be constructed by deleting $r = m - K$ rows of (3). These are called r-degenerate QC codes.

In this paper, we construct DC codes from the incidence matrices of the difference sets associated with $PG(n, q)$. It is shown that these codes are majority logic decodable. Further, self-dual and self-orthogonal codes are obtained from a subset of these codes.

2 Codes with $n = 2$

Singer [4] was the first to show that a projective plane ($n = 2$) of order q exists whenever q is a prime power. The design parameters are

$$v = q^2 + q + 1, k = q + 1, \lambda = 1. \tag{5}$$

The incidence matrix of the corresponding cyclic difference set has dimensions $v \times v$ and k 1's in each row. For $q = 2$, the difference set is (0,1,3), so

the 7×7 incidence matrix is

$$R_7 = \begin{matrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{matrix} \tag{6}$$

Appending to this a 7×7 identity matrix gives a generator matrix for a [14,7] DC code C_7 of the form

$$G_7 = [I_7; R_7]\,. \tag{7}$$

The weight distribution of C_7 is

Weight	Count
0	1
4	14
6	49
8	49
10	14
14	1

This distribution corresponds to that of the unique [14,7,4] self-dual code [7]. However, C_7 is not self-dual, since the rows of (6) are not orthogonal. The parity check matrix is

$$H_7 = [R_7^T; I_7]\,. \tag{8}$$

The weight distribution of H_7 is the same as that of G_7, so that C_7 is a formally self-dual even code. In fact, for q even, the rows of G always have even weight, so these codes are all formally self-dual even. Further, the columns of G have odd weight so the codes contain the all-ones codeword and $A_i = A_{n-i}$ for all i.

Consider the rows of H_7 with a leading 1

$$\left(\begin{array}{ccccccc|ccccccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

They form 3 orthogonal parity checks on bit 0 (leftmost). This is due to the fact that $\lambda = 1$, so that any two rows of R_7^T have a common 1 in only one position. Along with bit 0 alone, these form a set of 4 equations, so that with a majority vote, a single bit error in position 0 can be corrected. Due to the circulant nature of H_7, a set of 3 orthogonal parity checks can easily be formed on all 7 information bits in C_7. Thus all single bit error patterns in the information bits can be corrected. In addition, all double error patterns can be detected ($d = 4$).

The $[N, K, d]$ DC codes for $n = 2$ can be characterized in terms of the properties of the incidence matrix

$$\begin{aligned} N &= 2(q^2 + q + 1), \\ K &= q^2 + q + 1, \\ d &= q + 2, \end{aligned}$$

for q a prime power. The corresponding class of PG codes has $d = q + 1$ and are based solely on the incidence matrices [8]. Since the DC codes only have even weight codewords (due to the addition of the identity matrix), d must be $q + 2$ as shown above.

The first few codes are listed in Table 1. From this table, it is clear

Table 1: (v, k, λ) Difference Set DC Codes

(v, k, λ)	d
(7,3,1)	4
(13,4,1)	5
(21,5,1)	6
(31,6,1)	7
(57,8,1)	9
(73,9,1)	10
(91,10,1)	11
(133,12,1)	13
(183,14,1)	15
(273,17,1)	18
(307,18,1)	19
(381,20,1)	21

that the codes are asymptotically poor (but can easily be decoded). For example, consider the (31,6,1) cyclic difference set (0,1,3,8,12,18). If this set is used to denote the non-zero coefficients in $r_{31}(x)$, then $r(x) = 1 +$

$x + x^3 + x^8 + x^{12} + x^{18}$. The rows of H_{31} with a leading 1 are

1000000000000100000100010000101	1000000000000000000000000000000
1100000000000010000010001000010	0100000000000000000000000000000
1011000000000000100000100010000	0001000000000000000000000000000
1000010110000000000001000001000	0000000010000000000000000000000
1000100001011000000000000100000	0000000000001000000000000000000
1000001000100001011000000000000	0000000000000000001000000000000

These rows all have a 1 in the first location and no other location has more than one. Thus C_{31} is three error correcting, with $q + 2 = 7$ orthogonal parity checks (the 6 above and bit 0 alone). The best known minimum distance for a [62,31] binary linear code is $d = 12$, and a DC code exists with this minimum distance [9] (but is not majority logic decodable). Therefore the maximum possible number of correctable errors is 2 more than that for C_{31}.

Consider now the codes with q odd. For $q = 3$, the incidence matrix of the (13,4,1) cyclic difference set is

$$R_{13} = \begin{matrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{matrix}$$

The corresponding [26,13] DC code C_{13} with generator matrix

$$G_{13} = [I_{13}; R_{13}], \tag{9}$$

has weight distribution

Weight	Count
0	1
5	13
8	390
9	780
12	2340
13	2510
16	1313
17	780
20	52
21	13

The minimum distance is $q+2=5$, as expected, but there are only $k=13$ codewords with this weight, corresponding to the rows of G_{13}. Clearly if we *expurgate* all codewords of odd weight, we obtain a [26,12] code with minimum distance 8 and weights divisible by 4. To illustrate this, consider the sum of two adjacent rows of G_{13}, which produces a codeword of weight $2(q+1)=8$. This codeword is orthogonal to all other pairs of adjacent codewords, as shown in the matrix G'_{13}.

$$G'_{13} = \left[\begin{array}{cccccccccccccc}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 &
\end{array}\right.$$

$$\left.\begin{array}{cccccccccccccc}
1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0
\end{array}\right] \cdots$$

The codewords of C'_{13} (the code with generator matrix G'_{13}) must be the codewords of even weight in C_{13}, because G'_{13} is formed of 12 linearly independent even weight codewords of C_{13}. Note that C'_{13} is a 1-degenerate

QC code, since $x + 1$ divides both defining polynomials of G'_{13}, so that $K = 12 = q^2 + q$.

If the rows of the generator matrix of a self-orthogonal code have weight divisible by 4, the code is doubly-even [1]. Since every row of G'_{13} is self-orthogonal and has weight 8, C'_{13} is a doubly-even self-orthogonal code and has weight distribution

Weight	Count
0	1
8	390
12	2340
16	1313
20	52

Since the blocklength N is even, and all codewords have even weight, the rows of G'_{13} are orthogonal to the all-ones word. Thus C_{13} can be extended to a self-dual [26,13] code C^*_{13} by appending this word. The code C^*_{13} has weight distribution

Weight	Count
0	1
6	52
8	390
10	1313
12	2340
14	2340
16	1313
20	52
26	1

which as expected corresponds to the unique extremal self-dual code of length 26 [7]. Another construction of this code based on circulant matrices is given in [10].

For $q = 5$, the [62,31] code C_{31} has weight distribution

Weight	Count
0	1
7	31
12	4030
15	89590
16	259625
19	3977920
20	8492450
23	55602065
24	90578280
27	260449600
28	325217900
31	433503412
32	420190275
35	260449600
36	195332612
39	55602065
40	31874200
43	3977920
44	1775990
47	89590
48	16275
52	186
55	31
62	1

Expurgating the odd weight codewords again gives a doubly-even self-orthogonal code C'_{31} with $d = 2(q+1) = 12$. Appending the all-ones codeword, as done for $q = 3$, to C'_{31} gives a self-dual code with weight distribution

Weight	Count
0	1
10	186
12	4030
14	16275
16	259625
18	1775990
20	8492450
22	31874200
24	90578280
26	195332612
28	325217900
30	420190275
32	420190275
34	325217900
36	195332612
38	90578280
40	31874200
42	8492450
44	1775990
46	259625
48	16275
50	4030
52	186
62	1

Note that in this case, adding the all-ones codeword reduces the minimum distance from 12 to 10, because of the weight 52 codeword in G'_{31}. These results lead to the following theorem.

Theorem 1 *For all odd q, the double circulant code constructed from the incidence matrix of a (v, k, λ) cyclic difference set related to $PG(2, q)$ has parameters $[2(q^2+q+1), q^2+q+1, q+2]$. Expurgating the odd weight codewords results in a doubly-even $[2(q^2+q+1), q^2+q, 2(q+1)]$ self-orthogonal code. Appending the all-ones codeword to this self-orthogonal code results in a self-dual $[2(q^2+q+1), q^2+q+1]$ code with $d \leq 2(q+1)$.*

Proof. The parameters of the double circulant code C can be determined from the properties of the incidence matrix. Consider now the even weight codewords in C. A generator matrix for the resulting code C' can be

constructed by taking q^2+q adjacent pairs of codewords in C (as was done in the preceding examples). Since the weight of every row of G is $q+2$, the rows of G' have weight $2(q+1)$, and this is a multiple of 4.

To show that C' is self-orthogonal, consider the rows of G' associated with the incidence matrix. For two adjacent rows of G', one row of G appears twice, along with two distinct rows of G. Since every distinct pair of rows in G has one 1 in common, the number of common 1's between the two adjacent rows in G' due to the row of G which appears twice is $(q+1)-2$. The number of common 1's between these two rows of G' due to the distinct rows from G is one, and the number of common 1's from the identity matrix in G is one. Thus the total number of common 1's between two adjacent rows of G' is $q+1$, which is even. For two non-adjacent rows in G', there are either 2 or 4 common 1's, depending on where the common ones between adjacent rows of G lie. Thus the rows of G' are orthogonal, and since the weight of each row is divisible by 4, C' is doubly-even.

To determine the minimum distance of C', consider the formally self-dual codes C and $C^{\perp}$. The minimum distance of C' can be obtained by considering the even combinations of rows of G. Since these codewords are self-orthogonal, they also appear as the even weight codewords in $C^{\perp}$. Therefore, if there is a even weight codeword c of weight d in C then c must be a combination of at most $d/2$ rows of G or H. The reason for this is as follows. Let $wt-r(c)$ and $wt-l(c)$ be the Hamming weights of the right and left halves of c, respectively. If there is codeword c such that $wt-l(c)=d/2+1$ and $wt-r(c)=d/2-1$, then c is combination of $d/2-1$ rows of G, and c must be a combination of $d/2-1$ rows of H, since $wt-r(c)=d/2-1$. Thus it is only necessary to consider even combinations of up to $d/2=q+1$ rows of G to determine d. Any sum of $2 \leq x \leq q+1$ rows in the incidence matrix must have weight at least $2(q+1)$ from the matrix properties, and since the sum of two rows of G has weight $2(q+1)$, $d=2(q+1)$.

Extension to a self-dual code requires the addition of the all-ones codeword. Since the rows of G' are even and N is even, there can be no words of odd weight. Further, since the rows of G' have even weight, they are orthogonal to the all-ones codeword. Thus C^* has parameters $[2m, m]$, and so is a self-dual code. □

Consider again the [26,13] DC code C_{13} with generator matrix (9). This code can be *lengthened* by adding the all ones codeword and adding an overall parity check. The resulting code, C_{14}, is a *bordered double circulant* code which has a generator matrix the form

$$G_{14} = \left[\begin{array}{ccc} & 0\ 1\ \cdots\ 1 & \\ & 1 & \\ I_{14} & \vdots & R_{13} \\ & 1 & \end{array}\right].$$

The rows of G_{14} are self-orthogonal, since each pair of rows of R_{13} has a common one in only one column, and the overall parity check provides another common 1. G_{14} is then a self-dual code, and has weight distribution

Weight	Count
0	1
6	26
8	442
10	1560
12	3653
14	5020
16	3653
18	1560
20	442
22	26
28	1

which corresponds to a unique extremal self-dual [28,14] code given in [7].

This code can be extended to a class of $[N, K, d]$ bordered self-dual DC codes with parameters

$$\begin{aligned} N &= 2(q^2+q+2), \\ K &= q^2+q+2, \\ d &= q+3, \end{aligned}$$

for q an odd prime power. For example, the next code in the class is a [64,32,8] code ($q = 5$).

3 Codes with $\lambda \neq 1$

Besides the codes considered in the previous section, there are numerous codes with $\lambda \neq 1$. For $q = 2$, these codes are characterized in terms of the

incidence matrices of cyclic difference sets with the following parameters

$$v = 2^{n+1} - 1, k = 2^n - 1, \lambda = 2^{n-1} - 1. \tag{10}$$

We have already seen the code with $n = 2$, so consider the code with $n = 3$. The parameters in this case are $(v, k, \lambda) = (31, 15, 7)$. This code has $d = 4$, and so has a very poor minimum distance.

For $n = 3$, the difference sets have the following parameters

$$v = q^3 + q^2 + q + 1, k = q^2 + q + 1, \lambda = q + 1. \tag{11}$$

For $q = 2$, the difference set parameters are (15,7,3). The corresponding [30,15] DC code has $d = 4$ [11], which is half the maximum possible minimum distance [9].

Since the other codes in these classes have large dimensions, we were unable to determine their distance properties. However, we conjecture that in general the codes based on this DC construction have poor minimum distances.

4 Summary

A class of double circulant (DC) codes has been characterized in terms of the incidence matrices of cyclic difference sets associated with $PG(n, q)$. These codes are 1-step majority logic decodable since $\lambda = 1$. The codes for q even are formally self-dual even. The first codes for q odd have an odd weight symmetry [12], and it is conjectured that all codes in this class possess this property. It was shown that a class of doubly-even self-orthogonal codes, and two classes of self-dual codes, can be constructed from the DC codes for q odd.

Acknowledgement

The authors would like to thank Masaaki Harada and the anonymous reviewer for their helpful comments.

References

[1] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Co., New York, NY, 1977.

[2] P.J. Cameron and J.H. van Lint, *Designs, Graphs, Codes and Their Links*, London Math. Soc. Student Texts, No. 22, Cambridge University Press, New York, NY, 1991.

[3] M. Hall, Jr., *Combinatorial Theory*, Blaisdell Publishing Co., Waltham, MA, 1967.

[4] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Society*, vol. 43, pp. 377-385, 1938.

[5] P.P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes," *Designs, Codes and Crypt.*, vol. 2, pp. 81-91, 1992.

[6] G.E. Séguin and G. Drolet, "The theory of 1-generator quasi-cyclic codes," preprint, Royal Military College of Canada, Kingston, ON, June 1990.

[7] J.H. Conway and N.J.A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 1319-1333, Nov. 1990.

[8] E.R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw Hill, 1969.

[9] T.A. Gulliver and V.K. Bhargava, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, pp. 552-555, May 1991.

[10] V.K. Bhargava and J.M Stein, "(v, k, λ) configurations and self-dual codes," *Inform. and Contr.*, vol. 28, pp. 352-355, 1975.

[11] V.K. Bhargava, S.E. Tavares and S.G.S. Shiva, "Difference sets of the Hadamard type and quasi-cyclic codes," *Inform. and Contr.*, vol. 26, pp. 341-350, 1974.

[12] V.K. Bhargava, "Odd weight symmetry in some binary codes", *IEEE Trans. Inform. Theory*, vol. 23, pp 518-520, July 1977.