CODES CONSTRUCTED FROM NON-SYMMETRIC ASSOCIATION SCHEMES

Jon Lark Kim

Department of Mathematics
Seoul National University
Seoul, 151-742, Korea
e-mail:jlkim@math.snu.ac.kr

June 23, 1997

Abstract. We construct binary codes $\mathcal{C}$ and $\mathcal{C}'$ from non-symmetric association schemes $\mathfrak{X}$ of class 2 with order $n \equiv 3 \pmod 4$. We prove a necessary and sufficient condition for $\mathcal{C}$ or $\mathcal{C}'$ constructed from $\mathfrak{X}$ to be doubly-even self-dual or singly-even non-self-dual. We also prove that $\mathcal{C}$ is the extension of $\mathcal{C}'$ when $n \equiv 3 \pmod 8$. In the last section we construct Hamming and Golay codes and other codes by this method, and give a conjecture that if there exists a non-symmetric association scheme of class 2 with order 35, then the code constructed by this method is a doubly-even self-dual $[72, 36, 16]$ code, which has been an open problem.

§1. Introduction

It is well known that association schemes play an important role in coding theory, providing many of the sharpest bounds on the size of a code. The purpose of this paper is to construct binary $\mathcal{C}$ and $\mathcal{C}'$ codes from non-symmetric association schemes $\mathfrak{X}$ of class 2 with order $n \equiv 3 \pmod 4$. Many codes turn out to be double circulant or quasi-cyclic codes. We will show in section 2 a necessary and sufficient condition for $\mathcal{C}$ or $\mathcal{C}'$ constructed from $\mathfrak{X}$ to be doubly-even self-dual or singly-even non-self-dual. We also prove that $\mathcal{C}$ is the extended code of $\mathcal{C}'$ when $n \equiv 3 \pmod 8$. In section 3 we give examples which include $[8, 4, 4]$ Hamming code, $[24, 12, 8]$ Golay code and some quasi-cyclic codes. Finally we conjecture that if there exists a non-symmetric association scheme of class 2 with order 35, then the code constructed by this method is a doubly-even self-dual $[72, 36, 16]$ code.

In this section we give basic definitions concerning codes and association schemes.

1.1. Codes

For basic definitions about codes, we refer to [4,6,9]. A *binary* $[n, k]$ *linear code* $\mathcal{C}$ is a k-dimensional vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the Galois field of 2 elements. We call the elements of $\mathcal{C}$ *codewords* and the (Hamming) *weight* of a codeword is defined as the number of non-zero coordinates. An $[n, k, d]$ *code* is an $[n, k]$ code with minimum weight d among all the codewords in $\mathcal{C}$. In this paper, we only consider binary codes.

Two codes are *equivalent* if one can be obtained from the other by a permutation of coordinates. An *automorphism* of $\mathcal{C}$ is a permutation of the coordinates of $\mathcal{C}$ which preserves $\mathcal{C}$. It is easy to check that all automorphisms of $\mathcal{C}$ form a group.

The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_2^n \,|\, x \cdot y = 0, \text{ for all } y \in \mathcal{C}\},$$

where $x \cdot y$ is calculated via (mod 2).

We continue our definitions.

Definition 1.1. A code $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C}$ is a subcode of $\mathcal{C}^\perp$, and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. A code is *doubly-even* if all codewords have weight divisible by 4, 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 minimum weight for that length. The *intersection* of codewords $u = (u_1, \cdots, u_n)$ and $v = (v_1, \cdots, v_n)$ is

$$u * v = (u_1 v_1, \cdots, u_n v_n).$$

Now we define double circulant codes.

Definition 1.2. Let $\mathcal{D}_p$ be a code with generator matrix of the form $[I, R]$, where I is the identity matrix and R is a circulant matrix. By a circulant matrix we mean a matrix of the form

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_{m-1} & a_0 & \cdots & a_{m-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{bmatrix},$$

where a_i's are 0 or 1. This code $\mathcal{D}_p$ is called *pure double circulant.*

Similarly let $\mathcal{D}_b$ be a code with generator matrix of the form

$$\left[\begin{array}{c|cccc} & 0 & 1 & \cdots & 1 \\ & 1 & & & \\ I_{n+1} & \vdots & & R' & \\ & 1 & & & \end{array}\right],$$

where R' is again a circulant matrix. This code $\mathcal{D}_b$ is called *bordered double circulant.* $\mathcal{D}_p$ and $\mathcal{D}_b$ are called *double circulant* codes. Many codes we will construct in section 2 are double circulant codes.

Brualdi and Pless [2] constructed a self-dual code of length $2n+2$ from a singly-even self-dual code of length n via shadows. By using this result, Gulliver and

Harada [4] have shown that a bordered double circulant self-dual code is equivalent to an extended code of a pure double circulant self-dual code $[I\ R]$, where the extension is given via the generator matrix

$$G' = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 1 & 1 & & & & & & \\ \vdots & \vdots & & I_n & & & R & \\ 1 & 1 & & & & & & \end{bmatrix}. \tag{1.1}$$

We remark that we will prove in Theorem 4 in section 2 a similar result as Gulliver and Harada did above even though R may not be circulant. Moreover they [4] proved that the weight enumerator of a bordered double circulant self-dual code is obtained from those of a pure double circulant self-dual code and its shadow.

Definition 1.3. A binary code is called *quasi-cyclic* if there is some integer s such that every cyclic shift of a codeword by s places is again a codeword.

Remark 1. It is easy to see that a cyclic code is a quasi-cyclic code with $s = 1$. By taking the columns of $[I, R]$ in some order, where R is circulant, we see that $\mathcal{D}_p$ is equal to a quasi-cyclic code with $s = 2$.

It is well known that any binary QR code $\mathcal{Q}$ with one coordinate deleted, or any extened code $\widehat{\mathcal{Q}}$ is equal to a quasi-cyclic code with $s = 2$ [6]. We note that many good codes are quasi-cyclic codes and that some long double circulant(or quasi-cyclic) code $\mathcal{D}_p$ meet the Gilbert-Varshamov bound [5].

In [6], they defined an equivalent double circulant code $\mathcal{B}$ with $\mathcal{D}_b$ as follows.

Let $q = 4m - 1$ is a prime of the form $8k + 3$. Then $\mathcal{B}$ is defined as the $[8m = 2q + 2, q + 1]$ binary code with generator matrix

$$M = \begin{array}{c} \begin{array}{ccccccccc} & & & & r_\infty & r_0 & r_1 & \cdots & r_{q-1} \end{array} \\ \begin{bmatrix} 1 & & & & 0 & & & & \\ \vdots & & I & & \vdots & & A & & \\ 1 & & & & 0 & & & & \\ 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \end{array}, \tag{1.2}$$

where A is a circulant matrix which in the first row has a 1 in position r_i iff $i = 0$ or i is a quadratic residue mod q, 0 otherwise, i.e.

$$a(x) = 1 + \sum_{r \in Q} x^r,$$

where Q is the set of all quadratic residues in $\mathbb{F}_q^*$.

Remark 2. It was shown that $\mathcal{B}$ is a doubly-even self-dual code [6, p.508]. Furthermore in [3] there is a square root bound for the minimum distance d of $\mathcal{B}$.

$$(d-1)^2 - (d-1) + 1 \geq 2q + 1,$$

which was a research problem proposed in [6, p509]. Our construction is primarily motivated by (1.2) (see (2.2).

1.2. Association schemes

We follow definitions and notations in [1].

Let X be a set of cardinality n and let $R_i (i = 0, 1, \cdots, d)$ be subsets of $X \times X$ satisfying the followings;

(i) $R_0 = \{(x, x) | x \in X\}$,

(ii) $X \times X = R_0 \cup R_1 \cup \cdots \cup R_d$, $R_i \cap R_j = \phi$ if $i \neq j$,

(iii) $R_i^T = R_i'$ for some $i' \in \{0, 1, \cdots, d\}$,
where $R_i^T = \{(x, y) | (y, x) \in R_i\}$,

(iv) For $i, j, k \in \{0, 1, \cdots, d\}$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is constant whenever $(x, y) \in R_k$.

Such a configuration $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is called an *association scheme* of class d on X.

We denote the constant in (iv) by p_{ij}^k and call them the *intersection numbers* of $\mathfrak{X}$. We call the cardinality $n = |X|$ of X the *order* of $\mathfrak{X}$.

In addition, if
(v) $p_{ij}^k = p_{ji}^k$, for all i, j, k,
then $\mathfrak{X}$ is called *commutative.* On the other hand, if
(iv) $i' = i$,
then $\mathfrak{X}$ is called *symmetric* or of *Bose-Mesner type.*

The *i-th adjacency matrix* A_i of $\mathfrak{X}$ is defined to be the matrix of degree $|X|$ whose rows and columns are indexed by the elements of X and whose (x, y) entries are

$$(A_i)_{xy} = \begin{cases} 1 \text{ if } (x, y) \in R_i, \\ 0 \text{ otherwise.} \end{cases}$$

Then A_i is a $(0, 1)$-matrix. We can easily show that the conditions $(i), \cdots, (vi)$ are equivalent to the following $(i)', \cdots, (vi)'$;

$(i)'$ $A_0 = I$, the identity matrix,

$(ii)'$ $A_0 + A_1 + \cdots + A_d = J$, the matrix whose entries are all 1,

$(iii)'$ $A_i^T = A_{i'}$ for some $i' \in \{0, 1, \cdots, d\}$,
where A_i^T is the transpose of A_i,

$(iv)'$ $A_i A_j = \displaystyle\sum_{k=0}^{d} p_{ij}^k A_k$ for all i, j,

$(v)'$ $A_i A_j = A_j A_i$ for all i, j,

$(vi)'$ $A_i^T = A_i$ for all i.

Let's set $k_i = p_{ii'}^0$. Then k_i is the valency of A_i. Hence it is clear that

$$\begin{aligned} &k_0 = 1, \\ &|X| = k_0 + k_1 + \cdots + k_d, \\ &A_i J = k_i J,\ \ J A_i = k_{i'} J. \end{aligned} \tag{1.3}$$

Moreover we will use the following formula in Lemma 3 in §2

$$k_i k_j = \sum_{t=0}^{d} p_{ij}^t k_t, \text{ for all } i, j \in \{0, 1, \cdots, d\}. \tag{1.4}$$

If $(A)_{ij} = 1$ implies $(A)_{ij} = 0$, then A is called *directed* since the adjacency matrix A induces a directed graph whose adjacency matrix is A. If $(A)_{ij} = (A)_{ji}$ and $(A)_{ii} = 0$, then A is called *non-directed.*

Remark 3 [7]. It is easy to see that each of the adjacency matrices except A_0 is either directed or non-directed.

§2. Codes constructed from non-symmetric association schemes

For classification of association schemes of small orders ≤ 15, we refer to [7,10]. In this section, we will construct doubly-even selfi-dual codes or singly-even non-self-dual codes from a non-symmetric association scheme $\mathfrak{X}$ of class 2 with order n. Many of them will be bordered or pure double circulant codes, but not necessarily.

Fact [7]. Let $\mathfrak{X} = (X, \{R_0, R_i (i = 1, 2)\})$ be a non-symmetric association scheme of class 2 with order n, which is the cardinality of the set X. Then we have

$$n \equiv 3 \pmod 4.$$

Hence we can assume that n is odd if $\mathfrak{X}$ is a non-symmetric association scheme of class 2. Throughout this paper, we denote $\mathfrak{X}$ by a non-symmetric association scheme of class 2 with odd order n, and let I(identity matrix), A_1 and A_2 be the adjacency matrices of R_0, R_1, and R_2, respectively. Let k_1 be the valency of A_1 and k_2 be the valency of A_2. Then we see that $k_1 = k_2$ in Lemma 3.

To prove Theorem 1, we need several Lemmas.

Lemma 1. *Suppose that there exists a non-symmetric association scheme $\mathfrak{X}$ of class 2. Then $p_{12}^1 = p_{12}^2$.*

Proof. Let k_i be the valency of A_i where $i = 1, 2$. Since $\mathfrak{X}$ is non-symmetric, we have $A_2 = A_1^T$. Let

$$A_1 A_2 = k_1 A_0 + p_{12}^1 A_1 + p_{12}^2 A_2.$$

Then since $(A_1A_2)^T = A_1A_2$ and $A_2 = A_1^T$, it follows that

$$p_{12}^1 = p_{12}^2. \quad \square$$

Similarly we can show that

$$p_{21}^1 = p_{21}^2.$$

Then we can prove the more in the following Lemma.

Lemma 2. *For a non-symmetric association scheme $\mathfrak{X}$ of class 2 with $k_1 = k_2$, we obtain*

$$p_{ij}^k = p_{ji}^k \qquad \text{for all } i, j, k \in \{0, 1, 2\}.$$

Proof. Put $a = p_{12}^1 = p_{12}^2$ and $b = p_{21}^1 = p_{21}^2$. Let k_i be the valency of A_i. Now by Lemma 1, we know

$$\begin{aligned} A_1A_2 &= k_1I + aA_1 + aA_2, \\ A_2A_1 &= k_2I + bA_1 + bA_2. \end{aligned}$$

Noting that $I + A_1 + A_2 = J$, we can show that

$$\begin{aligned} A_1^2 &= A_1(J - I - A_2) \\ &= k_1J - A_1 - (k_1I + aA_1 + aA_2) \\ &= (k_1 - 1 - a)A_1 + (k_1 - a)A_2 \text{ by inserting again } J = I + A_1 + A_2. \end{aligned} \tag{2.1}$$

Hence we have

$$\begin{aligned} A_2A_1 &= (J - I - A_1)A_1 \\ &= k_1J - A_1 - A_1^2 \text{ since } JA_1 = k_2J = k_1J \\ &= k_1J - A_1 - (k_1 - 1 - a)A_1 - (k_1 - a)A_2 \\ &= k_1I + k_1A_1 + k_1A_2 - A_1 - (k_1 - 1 - a)A_1 - (k_1 - a)A_2 \\ &= k_1I + aA_1 + aA_2. \end{aligned}$$

Hence $A_1A_2 = A_2A_1$, as desired. Moreover in the process of proof we have shown

$$p_{12}^1 = p_{21}^1, \qquad p_{12}^2 = p_{21}^2$$

The other cases are trivial. This completes the proof. $\square$

Note that we also obtain as in (2.1) the following equations.

$$\begin{aligned} A_1^2 &= (J - I - A_2)A_1 \\ &= k_2J - A_1 - (k_2I + bA_1 + bA_2) \\ &= (k_2 - 1 - b)A_1 + (k_2 - b)A_2 \text{ by inserting again } J = I + A_1 + A_2. \end{aligned}$$

Hence we get

$$k_1 - a = k_2 - b,$$

which will be used in the proof of the Lemma 3.

Lemma 3. *For a non-symmetric association scheme of class 2 with order n, we have*

$$k_1 = k_2 \text{ and } n = 4p_{12}^1 + 3.$$

Proof. We recall the formula (1.4), i.e.

$$k_i k_j = \sum_{t=0}^{d} p_{ij}^t k_t \text{ for all } i, j \in \{0, 1, \cdots, d\}.$$

Put $i = j = 1,\ a = p_{12}^1$. We note from (2.1)

$$p_{11}^0 = 0,\ p_{11}^1 = (k_1 - 1 - a),\ p_{11}^2 = (k_1 - a).$$

Then we obtain

$$\begin{aligned} k_1^2 &= p_{11}^0 k_0 + p_{11}^1 k_1 + p_{11}^2 k_2 \\ &= 0 \times 1 + (k_1 - a - 1)k_1 + (k_1 - a)k_2. \end{aligned}$$

Similarly we get

$$k_2^2 = 0 \times 1 + (k_2 - b)k_1 + (k_2 - 1 - b)k_2.$$

Hence by substracting these two equations and using $k_1 - a = k_2 - b$, we see that

$$k_1 = k_2.$$

So we have, by inserting $k_1 = k_2$ into the former equation of the two equations,

$$k_1 = 2a + 1.$$

Since $2k_1 + 1 = n$, it follows that

$$n = 4a + 3 = 4p_{12}^1 + 3. \quad \square$$

From Lemma 2 and Lemma 3, we have proven the following useful result.

Corollary 1. *Suppose $\mathfrak{X}$ is a non-symmetric association scheme of class 2. Then $\mathfrak{X}$ is commutative.*

Proof. By Lemma 3 we know that $\mathfrak{X}$ satisfies $k_1 = k_2$. To prove that $\mathfrak{X}$ is commutative, we must show

$$p_{ij}^k = p_{ji}^k \qquad \text{for all } i, j, k \in \{0, 1, 2\}.$$

However this follows from Lemma 2. $\square$

The following is obtained esaily from Lemma3.

Corollary 2. *For a non-symmetric association scheme of class 2 with order* $n \equiv 3 \pmod 4$ *it follows that* $n \equiv 3 \pmod 8$ *if and only if* p^1_{12} *is even.*

2.1. Construction

This Corollary 2 will be used in the proof of Theorem 1. Now letting $a = p^1_{12} = p^2_{12} = p^1_{21} = p^2_{21}$ and $k = k_1 = k_2$, we can write

$$A_1A_2 = kI + aA_1 + aA_2.$$

Put

$$B_i = I + A_i,$$

and

$$M_i = \begin{bmatrix} 1 & & & & 0 & & & \\ \vdots & & I & & \vdots & & B_i & \\ 1 & & & & 0 & & & \\ 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{bmatrix}, \tag{2.2}$$

$$M'_i = \begin{bmatrix} \quad I \quad , \quad A_i \quad \end{bmatrix}. \tag{2.3}$$

So we can construct a code $\mathcal{C}(\mathfrak{X})$ $(\mathcal{C}'(\mathfrak{X}))$ with a generator matrix $M_i(M'_i)$. When B_i (A_i) is circulant, this code $\mathcal{C}(\mathfrak{X})$ $(\mathcal{C}'(\mathfrak{X}))$ will be bordered (pure) double circulant. However in general B_i is not circulant(see section 3). This makes difference from double circulant codes. $\mathcal{C}(\mathfrak{X})$ will be mainly studied in this paper since $\mathcal{C}(\mathfrak{X})$ gives rise to a doubly-even self-dual code while $\mathcal{C}'(\mathfrak{X})$ gives a singly-even code(not self-dual). After proving Theorem 1, we will also show that two codes with generator matrices M_1 and M_2 are equivalent when $n \equiv 3 \pmod 8$.

Now we can state and prove our main theorem.

Theorem 1. *Let* $\mathfrak{X}$ *be a non-symmetric association scheme of class 2 with order* n*. Then* $n \equiv 3 \pmod 8$ *if and only if the code* $\mathcal{C}(\mathfrak{X})$ *constructed from* $\mathfrak{X}$ *with a generator matrix* M_i *in (2.2) where* $i = 1, 2$ *is a doubly-even self-dual* $[2n+2, n+1]$ *code.*

Furthermore the code $\mathcal{C}'(\mathfrak{X})$ *constructed from* M'_i *in (2.3) is a self-dual* $[2n, n]$ *code.*

Proof. Suppose that $n \equiv 3 \pmod 8$ and let $a = p^1_{12}$. Then a is even by Corollary 2. Note that M is an $(n+1) \times (2n+2)$ matrix whose row rank is $(n+1)$. So $\mathcal{C}$ is a $[2n+2, n+1]$ code. From the definition of an associaton scheme, it follows that

$$A_1^T = A_2, A_2^T = A_1$$
$$I + A_1 + A_2 = J.$$

Without loss of generality, we may assume that $i = 1$ and consider M_1. Putting $B = B_1 = I + A_1$, and $M = M_1$, we have

$$\begin{aligned} BB^T &= (I + A_1)(I + A_1^T) \\ &= (I + A_1)(I + A_2) \\ &= I + A_1 + A_2 + A_1A_2 \\ &= J + A_1A_2. \end{aligned}$$

Since a is p^i_{12}, we get

$$A_1A_2 = kI + aA_1 + aA_2.$$

So we have

$$BB^t = J + kI + aA_1 + aA_2. \tag{2.4}$$

Then the diagonal elements of BB^T are even since k is odd, and off-diagonal elements of BB^t are odd since a is even. Hence we have

$$BB^T \equiv I + J \pmod 2.$$

By noting M and equation (2.4), we can conclude that the weight of u, except the bottom row of M is $k + 3$, which is also even and the weight of the bottom row of M is even since $n + 1$ is even. Hence the weight of $u * v$ of any two distinct rows of M is $a + 2$ or $k + 1$ which are even. These imply that $\mathcal{C}$ is self-dual. In addition, every row of M has weight $n + 1$ or $k + 3 = \frac{n-3}{2} + 4$ both of which are divisible by 4. Hence it follows by induction that any codeword of $\mathcal{C}$ is divisible by 4. Consequently $\mathcal{C}$ is a doubly-even self-dual code.

Conversely suppose that $\mathcal{C}$ is doubly-even self-dual. Then $\mathcal{C}$ must satisfy (2.4). Hence for off-diagonal elements of BB^t to be odd, the value of a is even.

To prove that $\mathcal{C}'$ is self-dual, we note

$$A_1A_2 \equiv I \pmod 8 \quad \text{since } a \text{ is even.}$$

Hence each row of M'_i has even weight $k + 1$, and $u * v$ of two distinct rows u, v of M_i also has even weight. Therefore $\mathcal{C}'$ is self-dual. This completes the proof. □

Similarily we can prove the following theorem.

Theorem 1′. *Let $\mathfrak{X}$ be a non-symmetric association scheme of class 2 with order n. Then $n \equiv 7 \pmod 8$ if and only if the code $\mathcal{C}'(\mathfrak{X})$ constructed from $\mathfrak{X}$ with a generator matrix M'_i, where $i = 1, 2$ is a singly-even (not self-dual) $[2n, n]$ code.*

Proof. (⇒) Let $a = p^1_{12}$. Then a is odd by Corollary 2. Note that M'_i is an n by $2n$ matrix. So $\mathcal{C}'(\mathfrak{X})$ is an $[2n, n]$ code. From the definition, we have

$$\begin{aligned} A_1^T &= A_2, A_2^T = A_1 \\ I + A_1 &+ A_2 = J. \end{aligned}$$

Like Theorem 1, we may assume that $i = 1$, and consider M_1. Then since a is p^i_{12}, we get

$$A_1 A_1^T = A_1 A_2 = kI + aA_1 + aA_2. \tag{2.4$'$}$$

Then the diagonal elements of $A_1 A_1^T$ are odd since k is odd, and off-diagonal elements of $A_1 A_1^T$ are odd since a is odd.

By noting M', we know that the weight of any row u of M' is $k+1$ which is even and that $\mathrm{wt}(u * v) = a \not\equiv 0 \pmod 2$. This means $\mathcal{C}'(\mathfrak{X})$ is not self-dual. However we have

$$\begin{aligned} \mathrm{wt}(u+v) &= 2(k+1) - 2a \\ &= 4a + 4 - 2a \text{ by Lemma 3 and } 2k+1 = n \\ &= 2a + 4 \\ &\equiv 2 \pmod 4 \text{ since } a \text{ is odd.} \end{aligned}$$

Therefore $\mathcal{C}'(\mathfrak{X})$ is a singly-even code.

($\Leftarrow$) Conversely suppose that $\mathcal{C}'(\mathfrak{X})$ is singly-even. Then $\mathcal{C}'(\mathfrak{X})$ must satisfy (2.4$'$). Hence $\mathrm{wt}(u+v) = 2a + 4 \equiv 2 (\mathrm{mod}\ 4)$ implies that a is odd. By Corollary 2 this completes the proof. $\square$

Lemma 4 [4]**.** *Let $\mathcal{C}$ and $\mathcal{C}'$ be self-dual $[2n, n]$ codes with generator matrices of the form $[I_n, A]$ and $[I_n, A^T]$, respectively, where A is an n by n $(0,1)$-matrix and A^T is the transpose of A. Then $\mathcal{C}$ and $\mathcal{C}'$ are equivalent.*

Proof. Since $\mathcal{C}$ is self-dual, the parity check matrix $H = [A^T \ I_n]$ of $\mathcal{C}$ is also a generator matrix of $\mathcal{C}$. Thus there is a permutation of coordinates exchanging the left half and the right half of H and hence $\mathcal{C}$ is equivalent to $\mathcal{C}'$. $\square$

By using Theorem 1 and Lemma 4, we can prove the following.

Corollary 3. *If $n \equiv 3$ (mod 8), then the code $\mathcal{C}_1(\mathfrak{X})$ with generator matrix M_1 is equivalent to the code $\mathcal{C}_2(\mathfrak{X})$ with generator matrix M_2.*

Proof of sketch. The proof is similar to that of Lemma 4. Noting Theorem 1, we know that $\mathcal{C}_1$ and $\mathcal{C}_2$ are doubly-even self-dual. Also note that

$$B_1^T = (I + A_1)^T = I + A_1^T = I + A_2 = B_2.$$

Then consider the parity check matrix of M_1. $\square$

Remark 4. It is worth noting that Theorem 1 is somewhat different from the result [6, p501] which says that if M is of the form in (1.2), where we note B_i in (2.2) is replaced by a circulant matrix T, then the code generated by M is self-dual if and only if $TT^T \equiv I + J (\mathrm{mod}\ 2)$. This is because we are considering both circulant matrices(e.g. $n = 3, 11, 19$) and non-circulant matrices(e.g. $n = 27$).

Theorem 2. *Let $\mathfrak{X}, M$ and $\mathcal{C}(\mathfrak{X})$ be defined above. Let $n \equiv 3 \pmod 4$. Then the weight of any row, except the bottom row z of M and the weight of sum $u+v$ of any rows u, v of M are always $k+3$, where k is the valency of an adjacency matrix of $\mathfrak{X}$. Furthermore the weight of $u+v+z$ is also $k+3$.*

Proof. Put $B = I + A_1$. Let u, v be distinct rows of B. Then $2(k+1)$ is the total number of 1's appearing in u and v, and $(a+1)$ is the number of 1's appearing in $u * v$. Hence the weight of the sum of distinct rows of M, except the bottom row z of M, is $2(k+1) - 2(a+1) + 2 = k+3$, where 2 are added since the left side of M is the identity matrix. Moreover each row of B has valency of $k+1$. So the weight of any row codeword, except the bottom row of M, is $(k+1)+2$.

It is obvious to see that the weight of the bottom row z of M is greater than $k+3$ since $\mathrm{wt}(z) = n+1 = 2k+2 > k+3$. Let w be any row of M distinct from z of M. Then $\mathrm{wt}(w+z) = (n+1) - (k+2) = k+3$ since $2k+1 = n$.

Let's prove the last sentence of the theorem. In the process of the above proof, we can show that if u, v are distinct rows of B, then the weight of $u+v$ in B is $2k - 2a$. Therefore if we consider u, v as rows of M, then the weight of $u+v+z$ is $(n+1) - (2k-2a) + 2 = 2a+4 = k+3$. This completes the proof. $\square$

Lemma 5 [3]**.** *Let $q \equiv 3 (mod\ 8)$ be an odd prime power. Let*

$$M(q) = \begin{bmatrix} 1 & & & & 0 & & & \\ \vdots & & I_q & & \vdots & & S & \\ 1 & & & & 0 & & & \\ 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 \end{bmatrix},$$

where

$$(S)_{ij} = \begin{cases} 1 & \text{if } (j-i) \text{ is a square(possibly } 0), \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

Then the code $C(q)$ generated by $M(q)$ is a doubly-even self-dual quasi-cyclic code. Also the following holds. holds.

$$\begin{aligned} SS^t &= \Big(\frac{q+1}{4}\Big)I + \Big(\frac{q+1}{4}\Big)J \\ &\equiv I + J\ (mod\ 2). \end{aligned}$$

We note that the code $C(q)$ is a generalization of the code $\mathcal{B}$ in (1.2) and the square root bound in Remark 2 also holds for the code $C(q)$. The second statement of this Lemma follows from a classical theorem on difference sets. What we need here is the case when q is an odd prime(not power). In this case we can prove the existence of a non-symmetric association scheme of class 2 with odd prime order $n \equiv 3(\mathrm{mod}\ 8)$.

Theorem 3. *If $|X| = n \equiv 3 \pmod 8$ is an odd prime, then there exists a non-symmetric association scheme $\mathfrak{X}$ of two classes $\{R_1, R_2\}$, one, say A_1, of whose adjacency matrices can be taken as*

$$(A_1)_{ij} = \begin{cases} 1 & \text{if } (j-i) \text{ is a nonzero square,} \\ 0 & \text{otherwise.} \end{cases}$$

Moreover the code $\mathcal{C}(\mathfrak{X})$ constructed from this $\mathfrak{X}$ is a doubly-even self-dual quasi-cyclic code, which is bordered double circulant.

Proof. Set $A_1 = S - I$, where S is given by (2.5) and $q = n$. Then since there are $\frac{q-1}{2}$ quadratic residues in $\mathbb{F}_q^*$ and -1 is a non-residue when $q \equiv 3 \pmod 8$, we can choose A_2 such that A_1 is a circualnt matrix and $A_1^T = A_2$ and,

$$I + A_1 + A_2 = I + S - I + S_I^T - I = J. \tag{2.6}$$

We let $\mathfrak{X} = \{R_0, R_1, R_2\}$ be the association scheme corresponding to the adjacency matrices I, A_1, A_2, respectively. Then

$$\begin{aligned} A_1A_2 &= (S - I)(S^T - I) \\ &= SS^T - S - S^T + I \\ &= \left(\frac{q+1}{4}\right)I + \left(\frac{q+1}{4}\right)J - S - S^T + I \quad \text{by Lemma 5} \\ &= \left(\frac{q-3}{4}\right)I + \left(\frac{q+1}{4}\right)J - A_1 - A_2 \\ &= \left(\frac{2q-2}{4}\right)I + \left(\frac{q-3}{4}\right)A_1 + \left(\frac{q-3}{4}\right)A_2 \quad \text{by (2.6)} \\ &= \left(\frac{2q-2}{4}\right)I + 2mA_1 + 2mA_2 \quad (\because q = 8m+3) \end{aligned}$$

Similarly we can show that A_2A_1, A_1A_1 and A_2A_2 are of the form $a_0I + a_1A_1 + a_2A_2$ (a_0, a_1, a_2 are nonnegative integer), which justifies that $\mathfrak{X}$ is an association scheme. Furthermore by Theorem 1 and last equation of A_1A_2 we can conclude that $\mathcal{C}(\mathfrak{X})$ is a doubly-even self-dual code, which is bordered doubly circulant quasi-cyclic since S is a circulant matrix. $\square$

However the condition that $n \equiv 3 \pmod 8$ is an odd prime is not necessary for the existence of a non-symmetric association scheme of class 2. For example, if $n = 7$ or $n = 15$, then there exits a non-symmetric association scheme of class 2. These codes will be considered in the following section 3.

The next thoerem describes the relationship between $\mathcal{C}(\mathfrak{X})$ and $\mathcal{C}'(\mathfrak{X})$ constructed from a non-symmetric association scheme of class 2 with order $n \equiv 3 \pmod 8$.

Theorem 4. *Let $\mathfrak{X}$ be a non-symmetric association scheme of class 2 with order $n \equiv 3 \pmod 8$. Then the code $\mathcal{C}(\mathfrak{X})$ is equivalent to the extension of $\mathcal{C}'(\mathfrak{X})$, where the extension is given in (1.1).*

Proof.

$$
\begin{aligned}
\widehat{M'_1} &= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 1 & 1 & & & & & & \\ \vdots & \vdots & & I_n & & & A_1 & \\ 1 & 1 & & & & & & \end{bmatrix} \\
&\simeq \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 1 & & & & 1 & & & \\ \vdots & & I_n & & \vdots & & A_1 & \\ 1 & & & & 1 & & & \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & & & & 1 & & & \\ \vdots & & I_n & & \vdots & & A_1 + J_n & \\ 0 & & & & 1 & & & \end{bmatrix} \\
&\simeq \begin{bmatrix} 0 & 0 & 0 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & & & & 0 & & & \\ \vdots & & I_n & & \vdots & & I + A_2 & \\ 1 & & & & 0 & & & \end{bmatrix} \\
&= M_2 \simeq M_1 \quad \text{by Corollary 3} \quad \square
\end{aligned}
$$

We end this secton by remarking that although when $n \equiv 7 \pmod 8$ the code $\mathcal{C}(\mathfrak{X})$ constructed from $\mathfrak{X}$ is not in general singly-even, $\mathcal{C}'(\mathfrak{X})$ is singly-even. Furthermore $\mathcal{C}'(\mathfrak{X})$ need not be pure double circulant(e.g. $n = 15$). We illustrate our theorems by considering examples in the following section.

§3. Examples

Now we can give examples.

Example 1. Case of $n = 3$. The fact is that there are two (inequivalent) association schemes of order 3. One of these is of non-symmetric type and has 2 classes. Its adjacency matrices are

$$
A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.
$$

Then by letting $B = I + A_1$, we can construct a code $\mathcal{H}$ with generator matrix

$$
M = \left[\begin{array}{c|ccc|c|ccc} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ - & - & - & - & - & - & - & - \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].
$$

We first check that $k=1, a=0$. Hence from Theorem 1 it follows that this code $\mathcal{H}$ is doubly-even self-dual and so the minimum distance is 4. Therefore this is an extended Hamming $[8,4,4]$ code, as expected.

Example 2. Case of $n=7$. There exits a unique non-symmetric association scheme of class 2 [7,10]. The following is an adjacency matrix

$$A_1 = \begin{bmatrix} 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1\\ 1&0&1&0&0&0&1\\ 1&1&0&1&0&0&0 \end{bmatrix}.$$

By using a computer program, we can compute the weight enumerator of this code $\mathcal{C}'(\mathfrak{X})$,

$$w(x,y) = x^{14} + 14x^{10}y^4 + 49x^8y^6 + 49x^6y^8 + 14x^4y^{10} + y^{14}. \tag{3.1}$$

Hence this $[14,7]$ code has minimum distance 4 and singly-even by Theorem $1'$. It is known in [8] that there exists a self-orthogonal $[14,7,4]$ code of type D_{14} with the same weight enumerator as (3.1).

Example 3. Case of $n=11$. It is known that there are four (inequivalent) association schemes of order 11 [10]. One of these is of non-symmetric type and has 2 classes. These adjacency matrices are

$$A_1 = \begin{array}{c} \begin{array}{ccccccccccc} 0&1&2&3&4&5&6&7&8&9&10 \end{array} \\ \left[\begin{array}{ccccccccccc}
&1&&1&1&1&&&&1& \\
&&1&&1&1&1&&&&1 \\
1&&&1&&1&1&1&&& \\
&1&&&1&&1&1&1&& \\
&&1&&&1&&1&1&1& \\
&&&1&&&1&&1&1&1 \\
1&&&&1&&&1&&1&1 \\
1&1&&&&1&&&1&&1 \\
1&1&1&&&&1&&&1& \\
&1&1&1&&&&1&&&1 \\
1&&1&1&1&&&&1&&
\end{array}\right] \end{array}, \quad A_2 = \begin{array}{c} \begin{array}{ccccccccccc} 0&1&2&3&4&5&6&7&8&9&10 \end{array} \\ \left[\begin{array}{ccccccccccc}
&&1&&&&1&1&1&&1 \\
1&&&1&&&&1&1&1& \\
&1&&&1&&&&1&1&1 \\
1&&1&&&1&&&&1&1 \\
1&1&&1&&&1&&&&1 \\
1&1&1&&1&&&1&&& \\
&1&1&1&&1&&&1&& \\
&&1&1&1&&1&&&1& \\
&&&1&1&1&&1&&&1 \\
1&&&&1&1&1&&1&& \\
&1&&&&1&1&1&&1&
\end{array}\right] \end{array}.$$

Then by letting $B = I + A_1$, we construct a code $\mathcal{G}$ with generator matrix

$$G = \begin{array}{c} \begin{array}{c|ccccccccccc|c|ccccccccccc} \infty&0&1&2&3&4&5&6&7&8&9&10&\infty&0&1&2&3&4&5&6&7&8&9&10 \end{array} \\ \left[\begin{array}{c|ccccccccccc|c|ccccccccccc}
1&1&&&&&&&&&&&&1&1&&1&1&1&&&&1& \\
1&&1&&&&&&&&&&&&1&1&&1&1&1&&&&1 \\
1&&&1&&&&&&&&&&1&&1&1&&1&1&1&&& \\
1&&&&1&&&&&&&&&&1&&1&1&&1&1&1&& \\
1&&&&&1&&&&&&&&&&1&&1&1&&1&1&1& \\
1&&&&&&1&&&&&&&&&&1&&1&1&&1&1&1 \\
1&&&&&&&1&&&&&&1&&&&1&&1&1&&1&1 \\
1&&&&&&&&1&&&&&1&1&&&&1&&1&1&&1 \\
1&&&&&&&&&1&&&&1&1&1&&&&1&&1&1& \\
1&&&&&&&&&&1&&&&1&1&1&&&&1&&1&1 \\
1&&&&&&&&&&&1&&1&&1&1&1&&&&1&&1 \\
\hline
&&&&&&&&&&&&1&1&1&1&1&1&1&1&1&1&1&1
\end{array}\right] \end{array} \begin{array}{c} \\ 0\\1\\2\\3\\4\\5\\6\\7\\8\\9\\10\\ \\11 \end{array}.$$

It is routine to check that $k = 5, a = 2$. Then as Example 1, it follows from Theorem 1 that this code $\mathcal{G}$ is self-dual. By Theorem 2, the minimum distance d of $\mathcal{G}$ is less than or equal to 8. Since this is equivalent to a double circulant code $C(11)$ in Lemma 5 with $q = 11$, we can show by the Remark 2 that $d \geq 7$. However noting that any codeword has even weight, we can conclude that the minimum distance is 8, whence we have proven that this is an extended $[24, 12, 8]$ Golay code.

If we construct the code $\mathcal{C}'(\mathfrak{X})$, then we obtain a self-dual $[22, 11, 6]$ code by Theorem 1. Their weight enumerator is displayed.

$$\begin{aligned} w(x, y) =& x^{22} + 77x^{16}y^6 + 330x^{14}y^8 + 616x^{12}y^{10} \\ &+ 616x^{10}y^{12} + 330x^8y^{14} + 77x^6y^{16} + y^{22}. \end{aligned}$$

The extension of $\mathcal{C}'(\mathfrak{X})$ has the same weight distribution as the $[24, 12, 8]$ Golay code by Thoerem 4.

Example 4. Case of $n = 15$. It is known that there is a unique non-symmetric association scheme of class 2 [10]. By ussing one of adjacency matrix of this order we can construct the code $\mathcal{C}'(\mathfrak{X})$ with generator matrix

$$G = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&0&0&0 \\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&1&1&1&0&0&1&0 \\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&0&1&1&0&0&1&0&1 \\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&0&0&1&0&1&1 \\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&0&0&1&0&1&1&1 \\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&1&0&1&1&1&0 \\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&1&1&0&1&1&1&0&0 \\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&1&0&0&0&0&1&1&1&0&0&1 \\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&1&1&0&1&0&1&1&0&1&0&0 \\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&1&1&0&1&0&0&0&1&1&0&1&0 \\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&1&0&0&0&0&0&1&1&0&1 \\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&1&0&0&0&1&0&0&0&1&1&0 \\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&1&0&0&0&1&0&1&0&0&0&1&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&0&1&1&1&0&1&0&0&0&1 \\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&0&1&1&0&1&1&0&1&0&0&0
\end{bmatrix}.$$

By using a computer program, we can compute the weight enumerator of this code $\mathcal{C}'(\mathfrak{X})$,

$$\begin{aligned} w(x, y) =& x^{30} + 21x^{26}y^4 + 28x^{24}y^6 + 534x^{22}y^8 + 1617x^{20}y^{10} + 4634x^{18}y^{12} \\ &+ 9549x^{14}y^{16} + 9549x^{14}y^{16} + 4634x^{12}y^{18} \\ &+ 1617x^{10}y^{20} + 534x^8y^{22} + 28x^6y^{24} + 21x^4y^{26} + y^{30}. \end{aligned}$$

Hence this code is a singly-even $[30, 15, 4]$ code by Theorem $1'$. Although Theorem 4 applies only to $n \equiv 3 \pmod 8$ we note that if we extend this $[30, 15, 4]$ code $\mathcal{C}'(\mathfrak{X})$ by construction (1.1), then the weight distribution of this extended $[32, 16, 4]$ code is the same as the code $\mathcal{C}(\mathfrak{X})$ by a computer program.

Example 5. Case of $n = 19$. Since $n \equiv 3 (\text{mod } 8)$, we can construct a non-symmetric association scheme of class 2 by Theorem 3. The code $\mathcal{C}(\mathfrak{X})$ is the same as the extremal quasi-cyclic $[40, 20, 8]$ code $C(19)$ in Lemma 5.

Example 6. Case of $n = 23, 31$. Let A_{11} and A_{15} be adjacency matrices of non-symmetric association scheme of order 11, 15, respectively. Then we can construct adjacency matrices of order 23 and 31 as follows:

$$A_{23} = \begin{bmatrix} 0 & \bar{1} & \bar{0} \\ \bar{0} & A_{11} & B \\ \bar{1} & J+B & A_{11} \end{bmatrix},$$

where B is a left-wise circulant matrix with its first row $\bar{1} + v_1$, where v_1 is the first row of A_{11}. Similarly we can construct an adjacency matrix of order 31 by replacing A_{11} by A_{15}. Since these orders are congruent to 7 (mod 8), we get singly-even non-self-dual codes. We can show that there are codewords of weight 4 in code $\mathcal{C}'(\mathfrak{X})$ with $n = 23$ by a computer program, and it is not difficult to show that there is no codeword of weight 2 by hand. Therefore the minimum distance of code $\mathcal{C}'(\mathfrak{X})$ with $n = 23$ is 4, which is small compared with $n = 11, 19$.

Example 7. Case of $n = 27$. We observe that the incidence matrix appearing in [11] gives rise to an adjacency matrix by modifying diagonal entries as all 0. Then the adjacency matrix is given by

$$A = \begin{bmatrix} P & Q & R \\ R & P & Q \\ Q & R & P \end{bmatrix},$$

where each of P, Q and R is comprised of nine 3×3 circulants which are given by

$$P = \begin{bmatrix} p_1 & p_2 & p_3 \\ p_3 & p_1 & p_2 \\ p_2 & p_3 & p_1 \end{bmatrix}, \quad \text{with } p_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, p_2 = J, \text{ and } p_3 = \text{zero matrix}$$

$$Q = \begin{bmatrix} q_1 & q_2 & q_3 \\ q_3 & q_1 & q_2 \\ q_2 & q_3 & q_1 \end{bmatrix}, \quad \text{with } q_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, q_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \text{ and } q_3 = q_2,$$

$$R = \begin{bmatrix} r_1 & r_2 & r_3 \\ r_3 & r_1 & r_2 \\ r_2 & r_3 & r_1 \end{bmatrix}, \quad \text{with } r_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, r_2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \text{ and } r_3 = r_2.$$

It takes much longer time to compute the minimum distance of the code $\mathcal{C}(\mathfrak{X})$ by our computer program. However we could compute the weight enumerator of this code as the following.

$$\begin{aligned} w(x,y) =& x^{56} + 8190x^{44}y^{12} + 622314x^{40}y^{16} + 11699688x^{36}y^{20} \\ &+ 64909845x^{32}y^{24} + 113955380x^{28}y^{28} + 64909845x^{24}y^{32} \\ &+ 11699688x^{20}y^{36} + 622314x^{16}y^{40} + 8190x^{12}y^{44} + y^{56}. \end{aligned}$$

Hence the code $\mathcal{C}(\mathfrak{X})$ is an extremal doubly-even self-dual $[56, 28, 12]$ code.

So far we have shown that if $n \equiv 3 \pmod 8$, where $n \leq 27$ then we can construct extremal doubly-even self-dual codes $\mathcal{C}(\mathfrak{X})$ by this construction. This consideration gives the follwing argument.

Example 8. Case of $n = 35$. This case is probably interesting. We don't know whether there exists a non-symmetric association scheme of class 2 with order 35. However since $n \equiv 3 \pmod 8$, if there exists such an association scheme then the code $\mathcal{C}(\mathfrak{X})$ is doubly-even self-dual $[72, 36, d]$ code. So far it has been an open problem whether there exists a doubly-even self-dual $[72, 36, 16]$ code. We suggest that this code is a good example to look into.

Another interesting case is $n = 51$ which is congruent to 3 (mod 8). It is known in [6] that there is an extremal doubly-even self-dual QR $[104, 52, 20]$ code. We also conjecture that if there exists a non-symmetric association scheme of class 2 with order 51, then the code $\mathcal{C}(\mathfrak{X})$ will have the same minimum distance 20 as the $[104, 52, 20]$ code.

References

[1] E. Bannai, T. Ito, *Algebraic Combiniatorics I : Association schemes*, Benjamin/Cummings, Menlo Park, CA, 1984.

[2] R. A. Brualdi, V. S. Pless, *Weight enumerators of self-dual codes*, IEEE Trans. Inform. Thoery **IT-37** (1991), 1222-1225.

[3] R. Calderbank, *A square root bound on the minimum weight in quasi-cyclic codes*, IEEE Trans. Inform. Thoery **IT-29** (1983), 332-337.

[4] T. A. Gulliver, M. Harada, *Weight enumerators of double circulant codes and new extremal self-dual codes*, Des. Codes and Cryptogr. **11** (1997), 141-150.

[5] T. Kasami, *A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2*, IEEE Trans. Inform. Thoery **IT-20** (1974), 679.

[6] F. J. MacWilliams, N. J. A. Sloane, *The Theory of error-correcting Codes*, North-Holland, 1993.

[7] E. Nomiyama, *Classification of association schemes with at most ten vertices*, Kyushu J. Math **49** (1995), 163-195.

[8] V. Pless, *A classification of self-orthogonal codes over GF(2)*, Discrete Math. **3** (1972), 209-246.

[9] S. Roman, *Coding and Information Theory(GTM 134)*, Springer-Verlag, 1992.

[10] K. See, S. Y. Song, *Association schemes of small order*, preprint (1997).

[11] S. G. S. Shiva, V. K. Bhargava, S. E. Tavares, *Difference sets of the Hadamard types and quasi-cyclic codes*, Information and Control **26** (1974), 348.