AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **32** (2005), Pages 61–78

A new method for constructing T-matrices*

Mingyuan Xia

School of Mathematics and Statistics
Central China Normal University
Wuhan, Hubei 430079
P.R. China

Tianbing Xia

School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522
Australia

Jennifer Seberry

School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522
Australia

Guoxin Zuo

School of Mathematics and Statistics
Central China Normal University
Wuhan, Hubei 430079
P.R. China

Abstract

For every prime power $q \equiv 3 \pmod 8$ we prove the existence of $(q; x, 0, y, y)$-partitions of $GF(q)$ with $q = x^2 + 2y^2$ for some x, y, which are very useful for constructing SDS, T-matrices and Hadamard matrices. We discuss the transformations of $(q; x, 0, y, y)$-partitions and, by using the partitions, construct generalized cyclotomic classes which have properties similar to those of classical cyclotomic classes. Thus we provide a new construction for T-matrices of order q^2.

* Research supported by NSF of China (No. 10071029)

1 Introduction

In 1965 L. Baumert and M. Hall, Jr [1] found a construction of Hadamard matrices of order $12n$ from known Williamson matrices of order n. Indeed, they gave the first example of T-matrices of order 3. Many attempts were made to generalize this array, but none were successful until in 1971 L.R. Welch found a Baumert-Hall array of order 5. In 1972, Joan Cooper and Jennifer Seberry Wallis [4] gave the first definition of $T-$matrices. R.J. Turyn [11] proposed the notion of 4δ codes and Turyn's sequences, using Golay sequences, he constructed an infinite class of T-matrices of order $2^i 10^j 26^k + 1$ for $i, j, k \geq 0$. Since Turyn's sequences are very restrictive and very few are known, Turyn, then J. Seberry, C.H. Yang, C. Koukouvinos, etc. investigated base sequences instead and found a large number of existent cases (for details see [10]). In 1984 M.Y. Xia [12] proposed the idea of C-partitions on an Abelian group, and then an infinite family of C-partitions on $GF(q^2)$ with q prime power $\equiv 3 \pmod 8$ was found [14]. Now the construction of C-partitions in this paper is more general and yields many new T-matrices and Hadamard matrices.

Let G be an Abelian group of order v. We denote the group operation by multiplication. Subsets $D_1, \cdots, D_r$ of G are called r-$\{v; |D_1|, \cdots, |D_r|; \lambda\}$ supplementary difference sets(SDS), if for every nonidentity element g in G, there are exactly λ elements (d, d') in $D_1 \times D_1$, or $D_2 \times D_2, \cdots$, or $D_r \times D_r$ such that $gd' = d$.

It is convenient to use the group ring $Z[G]$ of the group G over the ring Z of rational integers with the addition and multiplication. Here the elements of $Z[G]$ are of the form

$$a_1 g_1 + a_2 g_2 + \cdots + a_v g_v, a_i \in Z, g_i \in G.$$

In $Z[G]$ the addition $+$ is given by the rule

$$(\sum_g a(g)g) + (\sum_g b(g)g) = \sum_g (a(g) + b(g))g.$$

The multiplication in $Z[G]$ is given by the rule

$$(\sum_g a(g)g)(\sum_h b(h)h) = \sum_k \left(\sum_{gh=k} a(g)b(h) \right) k.$$

For any subset A of G, we define an element

$$\sum_{g \in A} g \in Z[G],$$

and by abusing the notation we will denote it by A.

Let $A, B \subset G$ and t be an integer. We define

$$B^{(t)} = \sum_{b \in B} b^t \in Z[G], \quad AB^{(-1)} = \sum_{a \in A, b \in B} ab^{-1} \in Z[G]$$

and denote

$$\triangle A = AA^{(-1)}, \triangle(A, B) = AB^{(-1)} + BA^{(-1)}.$$

If $A = \emptyset$, we define

$$\triangle\emptyset = 0,\ \triangle\,(\emptyset, B) = 0.$$

With this convention $D_1, \cdots, D_r$ being r-$\{v; |D_1|, \cdots, |D_r|; \lambda\}$ SDS are equivalent to

$$\sum_{i=1}^{r} \triangle D_i = \left(\sum_{i=1}^{r} |D_i| - \lambda\right) + \lambda G.$$

If $r = 1$ the single SDS becomes a difference set(DS) in the usual sense. When $|D_1| = \cdots = |D_r| = k$, we denote r-$\{v; |D_1|, \cdots, |D_r|; \lambda\}$ by r-$\{v; k; \lambda\}$.

In the following we assume p is an odd prime, $r > 0$, and

$$q = p^r = 8m + 3 = x^2 + 2y^2 \tag{1}$$

with $x \equiv 1 \equiv y \pmod 2$.

In this paper we propose the notion of $(q; x, 0, y, y)$-partition of $GF(q)$ and prove its existence for some x, y satisfying (1). It provides a very useful method for constructing SDS, Hadamard matrices and T-matrices. Y. Q. Chen [3] constructed a partition of $GF(q^2)$. Then [15] generalized it from $GF(q^2)$ to $GF(q)$ with q prime power $\equiv 1 \pmod 4$. Now we extend it to the case q prime power $\equiv 3 \pmod 8$.

The rest of the paper is organized as follows. In section 2, we will partition the group $GF(q)$ into 8 subsets with certain desirable properties. In section 3, we use the partition obtained in Section 2 to define the generalized cyclotomic classes and discuss their properties. In section 4, by using generalized cyclotomic classes, we will construct 4-$\{q; (q-1)/2; q(q-2)\}SDS$, Hadamard matrices of order $4q^2$. In section 5 we show that there are lots of T-matrices of order q^2.

Before we proceed further, we list the notations that will be used throughout this paper:

q: a power of an odd prime p as in (1);
$GF(q)$: the Galois field with q elements;
$GF(q)^*$: the multiplicative group of $GF(q)$;
S: the set of all nonzero squares of $GF(q)$;
N: the set of all non squares of $GF(q)$;
δ: a generator of $GF(q)^*$;
$\mathrm{Tr}\, q^n$: the absolute trace from $GF(q^n)$ to $GF(p)$;
$\mathrm{Tr}\, q^n/q$: the relative trace from $GF(q^n)$ to $GF(q)$;
$\langle i, j\rangle$: the cyclotomy number.

Recall that the absolute trace $\mathrm{Tr}\, q^n$ of an element $g \in GF(q^n)$ is defined as

$$\mathrm{Tr}\, q^n(g) = \sum_{j=0}^{rn-1} g^{p^j} \in GF(p).$$

For the detailed discussion of absolute and relative trace maps of finite fields, we refer the reader to textbooks such as [6], [7] and [8]. The characters of the group $GF(q^n)$ are given by the following (see [9]). Let ξ be a fixed primitive pth root of unity, $\alpha, \beta \in GF(q^n)$, define a group homomorphism

$$\chi_\alpha : GF(q^n) \to C^*,$$
$$\chi_\alpha(\beta) = \xi^{\mathrm{Tr}\, q^n(\alpha\beta)},$$

where C^* is the multiplicative group of nonzero complex numbers. These group homomorphisms can be easily extended to ring homomorphisms from $Z[GF(q^n)]$ to C. In order to show $A = B$ in $Z[GF(q^n)]$ by using the Fourier inversion formula, we need only to verify $\chi_\alpha(A) = \chi_\alpha(B)$ for every $\alpha \in GF(q^n)$.

2 $(q; x, 0, y, y)$-Partitions

Let w be a solution of the irreducible polynomial $x^2 + 1$ over $GF(q)$. Then the set of all elements $\alpha w + \beta, \alpha, \beta \in GF(q)$, is $GF(q^2)$. It is well known that there is an element $g = \alpha w + \beta, \alpha, \beta \in GF(q)$, such that

$$GF(q^2)^* = \{g^k : k = 0, 1, \cdots, q^2 - 2\}.$$

Let g be such an element and put

$$E_i = \left\{g^{8(2m+1)j+i} : j = 0, 1, \cdots, 4m\right\}, i = 0, 1, \cdots, 16m + 7.$$

It is easy to show that

$$E_0 = \left\{\delta^{2k} : k = 0, 1, \cdots, 4m\right\} = S,$$

and

$$E_{8m+4} = \left\{\delta^{2k+1} : k = 0, 1, \cdots, 4m\right\} = N.$$

For any $i, 1 \le i < 16m + 8, i \ne 8m + 4$, write $g^i = \alpha w + \beta$, then $\alpha \ne 0$ and

$$\begin{aligned} E_i = g^i E_0 &= \left\{\alpha\delta^{2k} w + \beta\delta^{2k} : j = 0, 1, \cdots, 4m\right\} \\ &= \left\{\alpha\delta^{2k} w + \alpha^{-1}\beta\alpha\delta^{2k} : j = 0, 1, \cdots, 4m\right\} \\ &\triangleq \left\{(\alpha\delta^{2k}, \alpha^{-1}\beta(\alpha\delta^{2k})) : j = 0, 1, \cdots, 4m\right\}. \end{aligned}$$

So we can represent E_i by $\{(\eta, \gamma\eta) : \eta \in S\}$ or $\{(\eta, \gamma\eta) : \eta \in N\}$ according to $\alpha \in S$ or $\alpha \in N$. For convenience, we denote

$$E_0 = (0, S), \quad E_{8m+4} = (0, N)$$

and

$$\begin{aligned} \{(\eta, \gamma\eta) : \eta \in S\} &= (S, \gamma S), \\ \{(\eta, \gamma\eta) : \eta \in N\} &= (N, \gamma N). \end{aligned}$$

The partition given in the following theorem is the basis of the paper. It provides a useful method for constructing SDS, Hadamard matrices and T-matrices.

Theorem 1 *There exist eight subsets, $X_1, \cdots, X_8$, of $GF(q)$, q and m satisfy (1), such that*

$$\begin{aligned} |X_1| = |X_2| &= m, && (2)\\ \{|X_3|, |X_4|\} &= \left\{m + \frac{1}{2}(1+y), m + \frac{1}{2}(1-y)\right\} = \{|X_7|, |X_8|\}, && (3)\\ \{|X_5|, |X_6|\} &= \left\{m + \frac{1}{2}(1+x), m + \frac{1}{2}(1-x)\right\}, && (4)\\ X_1 + \cdots + X_8 &= GF(q), && (5)\\ V &= MU, && (6) \end{aligned}$$

for some x, y satisfying (1), where

$$\begin{aligned} V &= (X_1N + X_2S, X_1S + X_2N, \cdots, X_7N + X_8S, X_7S + X_8N)', && (7)\\ U &= (X_1, \cdots, X_8)' && (8) \end{aligned}$$

and

$$M = \begin{pmatrix} |X_1|{-}1 & |X_2|{-}1 & |X_3|{-}1 & |X_4|{-}1 & |X_5|{-}1 & |X_6|{-}1 & |X_7|{-}1 & |X_8|{-}1 \\ |X_2| & |X_1| & |X_4| & |X_3| & |X_6| & |X_5| & |X_8| & |X_7| \\ |X_4| & |X_3| & |X_1| & |X_2| & |X_7| & |X_8| & |X_6| & |X_5| \\ |X_3| & |X_4| & |X_2| & |X_1| & |X_8| & |X_7| & |X_5| & |X_6| \\ |X_6| & |X_5| & |X_8| & |X_7| & |X_1| & |X_2| & |X_3| & |X_4| \\ |X_5| & |X_6| & |X_7| & |X_8| & |X_2| & |X_1| & |X_4| & |X_3| \\ |X_8| & |X_7| & |X_5| & |X_6| & |X_4| & |X_3| & |X_1| & |X_2| \\ |X_7| & |X_8| & |X_6| & |X_5| & |X_3| & |X_4| & |X_2| & |X_1| \end{pmatrix}. \quad (9)$$

We call the partition satisfying (2)–(9) a $(q; x, 0, y, y)$-partition.

Proof. Put

$$C_i = \left\{g^k : k \equiv i \pmod 8\right\}, \quad i = 0, 1, \cdots, 7,$$

where g is a generator of $GF(q^2)$. It is clear that

$$C_i = \bigcup_{j=0}^{2m} E_{8j+i}, \quad i = 0, 1, \cdots, 7.$$

Particularly, C_0 and $C_4 = g^{8m+4}C_0$ can be written in the forms

$$\begin{aligned} C_0 &= (0, S) \cup \{(S, \gamma S), \gamma \in X_1\} \cup \{(N, \gamma N), \gamma \in X_2\}, && (10)\\ C_4 &= (0, N) \cup \{(N, \gamma N), \gamma \in X_1\} \cup \{(S, \gamma S), \gamma \in X_2\} && (11) \end{aligned}$$

for some subsets X_1 and X_2 of $GF(q)$. Obviously,

$$|X_1| + |X_2| = 2m. \quad (12)$$

For any $i, 1 \le i \le 2m$, write $g^{8i} = \alpha w + \beta (\in E_{8i})$ and $\alpha \neq 0$ for sure. Now

$$(g^{8i})^{8m+3} = g^{(16m+8)(4i-1)+8(2m+1-i)} \in E_{8(2m+1-i)}$$

and

$$(\alpha w+\beta)^{8m+3}=\alpha w^{8m+3}+\beta=-\alpha w+\beta,$$

so $\alpha(-\alpha)\in N$ and $\alpha^{-1}\beta+(-\alpha)^{-1}\beta=0$. Therefore $\gamma=\alpha^{-1}\beta\in X_i$ if and only if $-\gamma\in X_{3-i}, i=1,2$. These facts, together with (12), show that

$$|X_1|=|X_2|=m \tag{13}$$

and

$$0\notin X_1\cup X_2. \tag{14}$$

Now take

$$X_5=\left\{-\gamma^{-1}:\gamma\in(X_1\cap N)\cup(X_2\cap S)\right\}, \tag{15}$$

$$X_6=\{0\}\cup\left\{-\gamma^{-1}:\gamma\in(X_1\cap S)\cup(X_2\cap N)\right\}. \tag{16}$$

Since $\{C_2,C_6\}=\{g^{4m+2}C_0,g^{12m+6}C_0\}$ and $\{E_{4m+2},E_{12m+6}\}=\{(S,0),(N,0)\}$, so

$$\{C_2,C_6\}=\left\{\bigcup_{\gamma\in X_5}(S,\gamma S)\cup(\bigcup_{\gamma\in X_6}(N,\gamma N)),\bigcup_{\gamma\in X_5}(N,\gamma N)\cup(\bigcup_{\gamma\in X_6}(S,\gamma S))\right\}.$$

Without loss of generality, we can write

$$C_2 = \{(S,\gamma S),\gamma\in X_5\}\cup\{(N,\gamma N),\gamma\in X_6\}, \tag{17}$$

$$C_6 = \{(N,\gamma N),\gamma\in X_5\}\cup\{(S,\gamma S),\gamma\in X_6\}. \tag{18}$$

Clearly

$$|X_5|+|X_6|=2m+1. \tag{19}$$

Since

$$\{E_{2m+1},E_{6m+3},E_{10m+5},E_{14m+7}\}=\{(S,-S),(N,N),(N,-N),(S,S)\},$$

it follows that

$$1,-1\notin X_1\cup X_2.$$

Define

$$\begin{aligned}
X_3 &= \{-1\}\cup\{-(\gamma-1)^{-1}(\gamma+1):\gamma\in(X_1\cap(S+1))\cup(X_2\cap(N+1))\},\\
X_4 &= \{-(\gamma-1)^{-1}(\gamma+1):\gamma\in(X_1\cap(N+1))\cup(X_2\cap(S+1))\},\\
X_7 &= \{(\gamma+1)^{-1}(\gamma-1):\gamma\in(X_1\cap(N-1))\cup(X_2\cap(S-1))\},\\
X_8 &= \{1\}\cup\{(\gamma+1)^{-1}(\gamma-1):\gamma\in(X_1\cap(S-1))\cup(X_2\cap(N-1))\}.
\end{aligned}$$

Similarly to (17) and (18), without loss of generality, we can write

$$
\begin{aligned}
C_1 &= \{(S,\gamma S),\gamma\in X_3\}\cup\{(N,\gamma N),\gamma\in X_4\}, && (20)\\
C_3 &= \{(S,\gamma S),\gamma\in X_7\}\cup\{(N,\gamma N),\gamma\in X_8\}, && (21)\\
C_5 &= \{(N,\gamma N),\gamma\in X_3\}\cup\{(S,\gamma S),\gamma\in X_4\}, && (22)\\
C_7 &= \{(N,\gamma N),\gamma\in X_7\}\cup\{(S,\gamma S),\gamma\in X_8\}. && (23)
\end{aligned}
$$

Obviously,

$$|X_3|+|X_4|=|X_7|+|X_8|=2m+1. \tag{24}$$

From [16] we know that

$$\sum_{i=1}^{4}(|X_{2i-1}|-|X_{2i}|)^2 \;=\; 2(|X_3|-|X_4|)^2+(|X_5|-|X_6|)^2=q.$$

Therefore,

$$(|X_5|-|X_6|)^2=x^2 \quad\text{and}\quad (|X_3|-|X_4|)^2=(|X_7|-|X_8|)^2=y^2 \tag{25}$$

for some x and y. Consequently, by (13), (19), (24) and (25), we have

$$
\begin{aligned}
\{|X_5|,|X_6|\} &= \left\{m+\frac{1}{2}(1+x),m+\frac{1}{2}(1-x)\right\},\\
\{|X_3|,|X_4|\} &= \{|X_7|,|X_8|\}=\left\{m+\frac{1}{2}(1+y),m+\frac{1}{2}(1-y)\right\}.
\end{aligned}
$$

Since

$$
\begin{aligned}
&\{(S,\gamma S),\gamma\in X_1\cup X_3\cup X_5\cup X_7\}\cup\{(N,\gamma N),\gamma\in X_2\cup X_4\cup X_6\cup X_8\}\\
&=\bigcup_{i=1}^{2m}E_{8i}\cup(\bigcup_{i=1}^{3}\bigcup_{j=0}^{2m}E_{8j+i}),
\end{aligned}
$$

it follows that

$$|X_1\cup X_2\cup X_3\cup X_4\cup X_5\cup X_6\cup X_7\cup X_8|=8m+3,$$

i.e.

$$X_1+X_2+X_3+X_4+X_5+X_6+X_7+X_8=GF(q).$$

Now we are going to prove (6).

For any $h=\alpha w+\beta\neq 0,\alpha,\beta\in GF(q)$, it is clear that

$$\{hC_0,\cdots,hC_7\} \;=\; \{C_0,\cdots,C_7\}.$$

Note that

$$(\alpha,\beta)(\alpha',\beta')=(\alpha w+\beta)(\alpha' w+\beta')=(\alpha\beta'+\beta\alpha',\beta\beta'-\alpha\alpha'),$$

we have

$$\begin{aligned} hC_0 &= (\alpha S, \beta S) \cup \{(\alpha\gamma+\beta)S, (\beta\gamma-\alpha)S), \gamma \in X_1\} \\ &\quad \cup\{((\alpha\gamma+\beta)N, (\beta\gamma-\alpha)N), \gamma \in X_2\}, \\ hC_4 &= (\alpha N, \beta N) \cup \{(\alpha\gamma+\beta)N, (\beta\gamma-\alpha)N), \gamma \in X_1\} \\ &\quad \cup\{((\alpha\gamma+\beta)S, (\beta\gamma-\alpha)S), \gamma \in X_2\}. \end{aligned} \tag{26}$$

For any $\gamma_0 \in X_1$, we can choose $\alpha, \beta \in GF(q)$ such that $\alpha \in S$ and $\alpha^{-1}\beta = -\gamma_0 \in X_2$.

In (26) the term

$$(\alpha S, \beta S) = (S, -\gamma_0 S) \in C_4;$$

it follows that

$$hC_0 = C_4 \quad \text{and} \quad hC_4 = C_0.$$

Then in (26) the term

$$((\alpha\gamma_0+\beta)S, (\beta\gamma_0-\alpha)S) = (0, -(1+\gamma_0^2)S)$$

should be equal to $(0, N)$, i.e., $1+\gamma_0^2 \in S$. Now

$$\begin{aligned} hC_0 &= (S, -\gamma_0 S) \cup (0, N) \cup \{((\gamma-\gamma_0)S, -(1+\gamma\gamma_0)S), \gamma \in X_1, \gamma \neq \gamma_0\} \\ &\quad \cup\{((\gamma-\gamma_0)N, -(1+\gamma\gamma_0)N), \gamma \in X_2\} \\ &= (0, N) \cup (S, -\gamma_0 S) \cup \{(S, -\gamma^{-1}(1+\gamma_0^2+\gamma_0\gamma)S), \gamma \in R_1\} \\ &\quad \cup\{(N, -\gamma^{-1}(1+\gamma_0^2+\gamma_0\gamma)N, \gamma \in R_2\}, \end{aligned}$$

where

$$\begin{aligned} R_1 &= ((X_1-\gamma_0) \cap S) \cup ((X_2-\gamma_0) \cap N), \\ R_2 &= ((X_1-\gamma_0) \cap N) \cup ((X_2-\gamma_0) \cap S). \end{aligned}$$

Comparing expression (26) with (11), it follows that

$$|R_1| = |(X_1-\gamma_0) \cap S| + |(X_2-\gamma_0) \cap N| = |X_1| - 1, \tag{27}$$

$$|R_2| = |(X_1-\gamma_0) \cap N| + |(X_2-\gamma_0) \cap S| = |X_2|. \tag{28}$$

(27) and (28) mean that the coefficients of γ_0 in $X_1N + X_2S$ and $X_1S + X_2N$ are $|X_1| - 1$ and $|X_2|$ respectively.

Similarly, for $\gamma_0 \in X_1$, we can prove

$$hC_i = C_{i+4} \quad \text{and} \quad hC_{i+4} = C_i, i = 1, 2, 3.$$

Comparing the expression of hC_i with that of $C_{i+4} (i = 1, 2, 3)$, it follows that the coefficients of γ_0 in $X_3N + X_4S$, $X_3S + X_4N$, $X_5N + X_6S$, $X_5S + X_6N$, $X_7N + X_8S$ and $X_7S + X_8N$ are $|X_4|$, $|X_3|$, $|X_6|$, $|X_5|$, $|X_8|$ and $|X_7|$ respectively.

Similarly, repeating the procedure for $X_2, \cdots, X_8$, one can get (6). The theorem is proved. □

For any subset $E \subset GF(q), \beta, \gamma \in GF(q)$ and integer t, we write

$$\beta E + \gamma = \{\beta\alpha + \gamma : \alpha \in E\}, \quad E^{(t)} = \{\alpha^t : \alpha \in E\}$$

and as well as in $Z[GF(q)]$

$$\beta E + \gamma = \sum_{\alpha \in E} (\beta\alpha + \gamma), \quad E^{(t)} = \sum_{\alpha \in E} \alpha^t.$$

Theorem 2 *Suppose* $W = \{X_1, \cdots, X_8\}$ *is a* $(q; x, 0, y, y)$*-partition of* $GF(q), \beta, \gamma \in GF(q)$ *and* $\beta \neq 0$*. If* $\bar{W} = \{\bar{X}_1, \cdots, \bar{X}_8\}$ *is obtained from* W *under the following transformations:*

(a) $\bar{X}_i = X_i + r, \ i = 1, \cdots, 8,$

(b) $\bar{X}_i = X_i^{(p)}, \ i = 1, \cdots, 8,$

(c) $\bar{X}_i = \beta X_i, \ i = 1, \cdots, 8$ *for* $\beta \in S,$

(d) $\bar{X}_1 = \beta X_2, \bar{X}_2 = \beta X_1$ *and* $\bar{X}_i = \beta X_i, \ i = 3, \cdots, 8$ *for* $\beta \in N,$
then $\bar{W}$ *is also a* $(q; x, 0, y, y)$*-partition of* $GF(q)$*.*

The proof of Theorem 2 is trivial. We leave it to the reader.
Remark. In general, the representation $q = x^2 + 2y^2$ is not unique, and so the values of x and y in (1), (3) and (4) are not completely determined by Theorem 1. In this case there is a problem: Does there exist a $(q; x, 0, y, y)$-partition for every given pair (x, y) satisfying (1)?

Example 1 $q = 27 = 8 \times 3 + 3 = 3^2 + 2 \times 3^2 = 5^2 + 2 \times 1^2$*. Let* δ *be a root of the equation* $\delta^3 = \delta + 2$*. Then*

$$GF(3^3)^* = \{\delta^i : i = 0, 1, \cdots, 25\}.$$

Take

$$\begin{array}{ll} X_1 = \{\delta^5, \delta^{15}, \delta^{19}\}, & X_2 = \{\delta^2, \delta^6, \delta^{18}\}, \\ X_3 = \{\delta^4, \delta^{10}, \delta^{12}, \delta^{13}\}, & X_4 = \{\delta^{14}, \delta^{16}, \delta^{22}\}, \\ X_5 = \{\delta^7, \delta^8, \delta^{11}, \delta^{20}, \delta^{21}, \delta^{24}\}, & X_6 = \{0\}, \\ X_7 = \{\delta, \delta^3, \delta^9\}, & X_8 = \{\delta^0, \delta^{17}, \delta^{23}, \delta^{25}\}. \end{array}$$

It is easy to verify that $\{X_1, \cdots, X_8\}$ *is a* $(27; 5, 0, 1, 1)$*-partition.*

Remark. We can read off

$$|(X_{2i-1} - \alpha) \cap S| + |(X_{2i} - \alpha) \cap N|, \quad |(X_{2i-1} - \alpha) \cap N| + |(X_{2i} - \alpha) \cap S|$$

by simply finding the coefficients of $\alpha \in GF(q)$ in

$$X_{2i-1}N + X_{2i}S, X_{2i-1}S + X_{2i}N$$

respectively, $i = 1, 2, 3, 4$.

3 Generalized cyclotomic classes

In this section, by using $(q; x, 0, y, y)$-partitions, we will construct generalized cyclotomic classes, which have properties similar to those of classical cyclotomic classes.

For any $\alpha \in GF(q)^*$, we know that $\chi_\alpha(S)$ and $\chi_\alpha(N)$ only depend on the fact that α is in S or in N, and do not depend on the particular choice of the element α in S or N. If Q is either S or N, we will denote $\chi_\alpha(Q)$ by $\chi_S(Q)$ for any $\alpha \in S$ and $\chi_N(Q)$ for any $\beta \in N$. Define

$$a = \chi_S(S) = \chi_N(N), \quad b = \chi_S(N) = \chi_N(S).$$

The value of a and b can be computed from either the values of quadratic Gauss sums [6], [7], [8] or uniform cyclotomy [2]. They are

$$\{a, b\} = \left\{ -\frac{1}{2}(1 + \sqrt{-q}), -\frac{1}{2}(1 - \sqrt{-q}) \right\}.$$

Theorem 3 *Suppose $\{X_i, \ i = 1, \cdots, 8\}$ is a $(q; x, 0, y, y)$-partition of $GF(q)$, and $C_0, \cdots, C_7$ are subsets of $GF(q^2)$, given as in (10), (11) , (17), (18), (20), (21), (22) and (23) respectively. Then*

$$C_i C_j = \varepsilon_{j-i}(2m+1)(4m+1) + \sum_{k=0}^{7} < j-i, k > C_{i+k}, 0 \le i \le j \le 7, \tag{29}$$

where $\varepsilon_{j-i} = 1$ or 0 according as $j - i = 4$ or not, the table of $< i, j >$ $(0 \le i, j \le 7)$ reads as:

$$\begin{array}{cccccccc}
<0,0> & <0,1> & <0,2> & <0,1> & <0,4> & <0,1> & <0,2> & <0,1> \\
<1,0> & <1,0> & <1,2> & <0,1> & <0,1> & <0,1> & <0,1> & <0,7> \\
<2,0> & <0,1> & <2,0> & <1,7> & <0,2> & <0,1> & <0,2> & <1,2> \\
<1,0> & <0,1> & <0,1> & <1,0> & <0,1> & <1,7> & <1,2> & <0,1> \\
<0,0> & <1,0> & <2,0> & <1,0> & <0,0> & <1,0> & <2,0> & <1,0> \\
<1,0> & <0,1> & <1,7> & <1,2> & <0,1> & <1,0> & <0,1> & <0,1> \\
<2,0> & <1,7> & <0,2> & <0,1> & <0,2> & <1,2> & <2,0> & <0,1> \\
<1,0> & <1,2> & <0,1> & <0,1> & <0,1> & <0,1> & <1,7> & <1,0>
\end{array}$$

$$\begin{array}{ll}
<0,0>= m^2 + m, & <0,1>= m^2 + m - \frac{1}{4}(y^2 - 1), \\
<0,2>= m^2 - m + \frac{1}{2}(y^2 - 1), & <0,4>= m^2 + 3m + 1, \\
<1,0>= m^2 + \frac{1}{4}(y^2 - 1), & <1,2>= m^2 + m + \frac{1}{4}(1 + 2xy + y^2), \\
<1,7>= m^2 + m + \frac{1}{4}(1 - 2xy + y^2), & <2,0>= m^2 + m - \frac{1}{2}(y^2 - 1),
\end{array}$$

and $C_i = C_j$ as $i \equiv j \pmod 8$.

Proof. We calculate the character values of $C_i, i = 0, \cdots, 7$, as follows.

For any $\alpha_1, \alpha_2 \in GF(q)$, clearly,

$$\chi_{(\alpha_1,\alpha_2)}(C_{i+4}) = \overline{\chi_{(\alpha_1,\alpha_2)}(C_i)}, i = 0, 1, 2, 3.$$

It is enough to calculate the character values only for C_0, C_1, C_2 and C_3. Now

$$\begin{aligned}
\chi_{(\alpha_1,\alpha_2)}(C_0) &= \sum_{\beta\in S}\xi^{\mathrm{Tr}\,_{q^2}(\alpha_1\beta w+\alpha_2\beta)} + \sum_{\beta\in S,\gamma\in X_1}\xi^{\mathrm{Tr}\,_{q^2}((\alpha_1\gamma+\alpha_2)\beta w+\alpha_2\gamma\beta-\alpha_1\beta)} \\
&\quad + \sum_{\beta\in N,\gamma\in X_2}\xi^{\mathrm{Tr}\,_{q^2}((\alpha_1\gamma+\alpha_2)\beta w+\alpha_2\gamma\beta-\alpha_1\beta)} \\
&= \sum_{\beta\in S}\xi^{\mathrm{Tr}\,_q(\mathrm{Tr}\,_{q^2/q}(\alpha_1\beta w+\alpha_2\beta))} \\
&\quad + \sum_{\beta\in S,\gamma\in X_1}\xi^{\mathrm{Tr}\,_q(\mathrm{Tr}\,_{q^2/q}((\alpha_1\gamma+\alpha_2)\beta w+\alpha_2\gamma\beta-\alpha_1\beta))} \\
&\quad + \sum_{\beta\in N,\gamma\in X_2}\xi^{\mathrm{Tr}\,_q(\mathrm{Tr}\,_{q^2/q}((\alpha_1\gamma+\alpha_2)\beta w+\alpha_2\gamma\beta-\alpha_1\beta))} \\
&= \sum_{\beta\in S}\xi^{\mathrm{Tr}\,_q(2\alpha_2\beta)} + \sum_{\beta\in S,\gamma\in X_1}\xi^{\mathrm{Tr}\,_q(2(\alpha_2\gamma-\alpha_1)\beta)} + \sum_{\beta\in N,\gamma\in X_2}\xi^{\mathrm{Tr}\,_q(2(\alpha_2\gamma-\alpha_1)\beta)} \\
&= \chi_{2\alpha_2}(S) + \sum_{\gamma\in X_1}\chi_{2(\alpha_2\gamma-\alpha_1)}(S) + \sum_{\gamma\in X_2}\chi_{2(\alpha_2\gamma-\alpha_1)}(N).
\end{aligned}$$

If $\alpha_1=\alpha_2=0$,

$$\chi_{(0,0)}(C_0) = |C_0| = (2m+1)(4m+1) = (q^2-1)/8.$$

If $\alpha_2=0, \alpha_1\neq 0$,

$$\chi_{(\alpha_1,0)}(C_0) = 4m+1+|X_1|\chi_{\alpha_1}(S)+|X_2|\chi_{\alpha_1}(N) = 3m+1.$$

If $\alpha_2\in N$, we set $\alpha=\alpha_2^{-1}\alpha_1$, then

$$\begin{aligned}
\chi_{(\alpha_1,\alpha_2)}(C_0) &= a + \sum_{\gamma\in X_1}\chi_{\gamma-\alpha}(S) + \sum_{\gamma\in X_2}\chi_{\gamma-\alpha}(N) \\
&= a + \sum_{\gamma\in(X_1-\alpha)\cap S}\chi_\gamma(S) + \sum_{\gamma\in(X_1-\alpha)\cap N}\chi_\gamma(S) \\
&\quad + \sum_{\gamma\in(X_1-\alpha)\cap\{0\}}\chi_\gamma(S) + \sum_{\gamma\in(X_2-\alpha)\cap\{0\}}\chi_\gamma(N) \\
&\quad + \sum_{\gamma\in(X_2-\alpha)\cap S}\chi_\gamma(N) + \sum_{\gamma\in(X_2-\alpha)\cap N}\chi_\gamma(N) \\
&= (1+k_1)a + k_2 b + (4m+1)|((X_1\cup X_2)-\alpha)\cap\{0\}|,
\end{aligned}$$

where

$$\begin{aligned}
k_1 &= |(X_1-\alpha)\cap S| + |(X_2-\alpha)\cap N|, \\
k_2 &= |(X_1-\alpha)\cap N| + |(X_2-\alpha)\cap S|.
\end{aligned}$$

If $\alpha_2\in S$, let $\alpha=\alpha_2^{-1}\alpha_1$ again, we get

$$\chi_{(\alpha_1,\alpha_2)}(C_0) = (1+k_1)b + k_2 a + (4m+1)|((X_1\cup X_2)-\alpha)\cap\{0\}|.$$

Similarly, we have

$$\begin{aligned}\chi_{(0,0)}(C_i) &= (2m+1)(4m+1),\\ \chi_{(\alpha_1,0)}(C_i) &= |X_{2i+1}|\chi_{\alpha_1}(S)+|X_{2i+2}|\chi_{\alpha_1}(N),\\ \chi_{(\alpha_1,\alpha_2)}(C_i) &= \begin{cases} k_{2i+1}a+k_{2i+2}b+(4m+1)|((X_{2i+1}\bigcup X_{2i+2})-\alpha)\bigcap\{0\}|, & ;\alpha_2\in N,\\ k_{2i+1}b+k_{2i+2}a+(4m+1)|((X_{2i+1}\bigcup X_{2i+2})-\alpha)\bigcap\{0\}|, & ;\alpha_2\in S,\end{cases}\end{aligned}$$

where

$$\begin{aligned}k_{2i+1} &= |(X_{2i+1}-\alpha)\cap S|+|(X_{2i+2}-\alpha\cap N|,\\ k_{2i+2} &= |(X_{2i+1}-\alpha)\cap N|+|(X_{2i+2}-\alpha\cap S|,\end{aligned}$$

$i=1,2,3$.

We know that for any $\gamma\neq 0$

$$\begin{array}{ll}\chi_\gamma(S)+\chi_\gamma(N)=-1, & \chi_\gamma(S)\chi_\gamma(N)=2m+1,\\ \chi_\gamma^2(S)=-2m-1-\chi_\gamma(S), & \chi_\gamma^2(N)=-2m-1-\chi_\gamma(N).\end{array}$$

We denote the right hand side of (29) by R_{ij} and discuss the case $i=j=0$ at first. One can see that

$$|C_0C_0|=(2m+1)^2(4m+1)^2$$

and

$$|R_{00}|=\sum_{k=0}^{7}<0,k>|C_k|=(2m+1)(4m+1)\sum_{k=0}^{7}<0,k>=|C_0C_0|.$$

For $\alpha_1\neq 0$,

$$\chi_{(\alpha_1,0)}(C_0C_0)=\chi^2_{(\alpha_1,0)}(C_0)=(3m+1)^2$$

and

$$\begin{aligned}\chi_{(\alpha_1,0)}(R_{00}) &= (<0,0>+<0,4>)(3m+1)-<0,2>(|X_3|+|X_4|)\\ &\quad -<0,1>(|X_5|+|X_6|)-<0,3>(|X_7|+|X_8|)\\ &= \chi_{(\alpha,0)}(C_0C_0).\end{aligned}$$

For $\alpha_2\in N$,

$$\begin{aligned}&\chi_{(\alpha_1,\alpha_2)}(C_0C_0)=-(2m+1)(1+k_1-k_2)^2-(1+k_1)^2a-k_2^2b+\\ &(4m+1)[2(1+k_1)a+2k_2b+(4m+1)]|((X_1\cup X_2)-\alpha)\cap\{0\}|\end{aligned}$$

and

$$\begin{aligned}&\chi_{(\alpha_1,\alpha_2)}(R_{00})\\ &=<0,0>[-1-k_1-k_2+2(4m+1)|((X_1\cup X_2)-\alpha)\cap\{0\}|]+\\ &<0,1>[-k_3-k_4-k_7-k_8+2(4m+1)|((X_3\cup X_4\cup X_7\cup X_8)-\alpha)\cap\{0\}|]\\ &+<0,2>[-k_5-k_6+2(4m+1)|((X_5\cup X_6)-\alpha)\cap\{0\}|]\\ &+[<0,4>-<0,0>]\chi_{(\alpha_1,\alpha_2)}(C_4).\end{aligned}$$

If $\alpha = \alpha_2^{-1}\alpha_1 \in X_1 \bigcup X_2$, then

$$1 + k_1 = k_2 = m, \;\; k_{2i+1} + k_{2i+2} = 2m + 1, \;\; i = 1, 2, 3.$$

Hence,

$$\chi_{(\alpha_1,\alpha_2)}(C_0^2) = (3m + 1)^2 = \chi_{(\alpha_1,\alpha_2)}(R_{00}).$$

If $\alpha \in X_3$, then

$$\begin{array}{llll} k_1 = |X_3| - 1, & k_2 = |X_4|, & k_3 = |X_1|, & k_4 = |X_2|, \\ k_5 = |X_8|, & k_6 = |X_7|, & k_7 = |X_5|, & k_8 = |X_6|. \end{array}$$

Therefore

$$\chi_{(\alpha_1,\alpha_2)}(C_0^2) = -(2m + 1)y^2 - |X_3|^2 a - |X_4|^2 b = \chi_{(\alpha_1,\alpha_2)}(R_{00}).$$

If $\alpha \in X_4$, then

$$\begin{array}{llll} k_1 = |X_4| - 1, & k_2 = |X_3|, & k_3 = |X_2|, & k_4 = |X_1|, \\ k_5 = |X_7|, & k_6 = |X_8|, & k_7 = |X_6|, & k_8 = |X_5|. \end{array}$$

So

$$\chi_{(\alpha_1,\alpha_2)}(C_0^2) = -(2m + 1)y^2 - |X_4|^2 a - |X_3|^2 b = \chi_{(\alpha_1,\alpha_2)}(R_{00}).$$

By a similar discussion we can prove that

$$\chi_{(\alpha_1,\alpha_2)}(C_0^2) = \chi_{(\alpha_1,\alpha_2)}(R_{00})$$

is valid in all cases. Consequently, $C_0^2 = R_{00}$. The proof of the rest of the theorem is similar. □

Theorem 3 shows that the formulas of the left part of the table [5, p196] are still valid for $C_0, \cdots, C_7$ defined by (10), (11), (17), (18), (20), (21), (22), (23) respectively, which need not be cyclotomic sets. We call them generalized cyclotomic classes.

Corollary 1 *Under the same assumptions as Theorem 3, C_0, C_1, C_2 and C_3 are* 4-$\{q^2; (q^2 - 1)/8; (q^2 - 9)/16\}SDS$.

Proof. From Theorem 3 we have

$$\sum_{i=0}^{3} \triangle C_i = \sum_{i=0}^{3} C_i C_{i+4} = (7q^2 + 1)/16 + (q^2 - 9)/16 GF(q^2).$$

The proof is completed. □

Remark. It is easy to see that C_i, C_j, C_k and C_l are 4-$\{q^2; (q^2-1)/8; (q^2-9)/16\}SDS$ for any set $\{i, j, k, l\} \equiv \{0, 1, 2, 3\}$ (mod 4).

Example 2 *Let $q = 11$. Then $m = 1 = y, x = 3$.*

$$S = \{1, 3, 4, 5, 9\}, \quad N = \{2, 6, 7, 8, 10\}.$$

Take

$$\begin{array}{llll} X_1 = \{6\}, & X_2 = \{10\}, & X_3 = \{0, 1\}, & X_4 = \{9\}, \\ X_5 = \emptyset, & X_6 = \{2, 3, 8\}, & X_7 = \{7\}, & X_8 = \{4, 5\}. \end{array}$$

It is easy to verify that $X_1, \cdots, X_8$ satisfy (2)-(9). Define $C_0, \cdots, C_7$ as in (10), (11), (17), (18), (20)–(23):

$$\begin{array}{ll} C_0 = (0, S) \cup (S, 6S) \cup (N, -N), & C_4 = (0, N) \cup (N, 6N) \cup (S, -S), \\ C_1 = (S, 0) \cup (S, S) \cup (N, 9N), & C_5 = (N, 0) \cup (N, N) \cup (S, 9S), \\ C_2 = (N, 2N) \cup (N, 3N) \cup (N, 8N), & C_6 = (S, 2S) \cup (S, 3S) \cup (S, 8S), \\ C_3 = (S, 7S) \cup (N, 4N) \cup (N, 5N), & C_7 = (N, 7N) \cup (S, 4S) \cup (S, 5S). \end{array}$$

From Theorem 3 it follows that

$$\begin{array}{lll} < 0, 0 >=< 0, 1 >= 2, & < 0, 2 >= 0, & < 0, 4 >= 5, \\ < 1, 0 >=< 1, 7 >= 1, & < 1, 2 >= 4, & < 2, 0 >= 3. \end{array}$$

It is easy to show that $C_0, \cdots, C_7$ satisfy (29). However they are generalized cyclotomic classes, not cyclotomic sets.

4 Constructing SDS

In this section we will construct some SDS which can be used to form Hadamard matrices.

To construct SDS in $GF(q^2)$ we need the following lemmas.

Lemma 1 *In $GF(q^2)$ the following equations hold:*

(i) $\triangle E_i = (4m + 1) + 2m(E_i + E_{i+8m+4})$;

(ii) $\triangle(E_i, E_{i+8m+4}) = (4m + 1)(E_i + E_{i+8m+4})$;

(iii) $\triangle(E_i, E_j + E_{j+8m+4}) = GF(q^2)^* - (E_i + E_j + E_{i+8m+4} + E_{j+8m+4})$, $i \neq j$, $0 \leq i, j \leq 16m + 7$.

For the proof see [13].

Let $A = \{a_0, \cdots, a_{2t}\} \subset \{0, 1, \cdots, 16m + 7\}$ and $B = \{b_1, \cdots, b_{4m+1-t}\} \subset \{0, 1, \cdots, 8m + 3\}$. Suppose

$$|\{a (\mathrm{mod}\ 8m + 4) : a \in A\} \cup B| = 4m + 2 + t. \tag{30}$$

Write

$$C = \bigcup_{i=0}^{2t} E_{a_i}, \ \bar{C} = \bigcup_{i=0}^{2t} E_{a_i+8m+4}, \ H = \bigcup_{j=1}^{4m+1-t} (E_{b_j} \cup E_{b_j+8m+4}), \ D = C \cup H.$$

Lemma 2 *Under the condition (30) we have*

$$\begin{aligned}\triangle D &= 2(4m+1-t)(4m+1)+[(4m+1)^2-t^2]GF(q^2)^* \\ &\quad -(4m+1-t)(C+\bar{C})+\triangle C. \end{aligned} \tag{31}$$

Proof. (31) follows from Lemma 1 by direct calculation. □

From (31) we see that the expression of $\triangle D$ only depends on the set of A and does not depend on the particular choice of B.

Let $X_1, \cdots, X_8$ be a $(q; x, 0, y, y)$-partition of $GF(q)$,

$$B_i \subset GF(q)\backslash(X_{2i+1} \cup X_{2i+2}), \quad |B_i| = 3m+1, \quad i = 0,1,2,3, \tag{32}$$

$C_0, \cdots, C_7$ are given in Theorem 3. Set

$$H_i = \bigcup_{\gamma \in B_i} ((S, \gamma S) \cup (N, \gamma N)), \quad D_i = C_i \cup H_i, \quad i = 0,1,2,3. \tag{33}$$

Theorem 4 *D_0, D_1, D_2 and D_3 given in (33) are* $4\text{-}\{q^2; q(q-1)/2; q(q-2)\}$ *SDS.*

Proof. It is easy to show that (32) and (33) guarantee the validity of (30) for every i.

From Lemma 2 we have

$$\triangle D_i = 2(3m+1)(4m+1)+(3m+1)(5m+1)GF(q^2)-(3m+1)(C_i+C_{i+4})+\triangle C_i,$$

$i = 0,1,2,3$. The conclusion follows immediately from Theorem 3. □

Let e, f be integers such that $0 < e, f < 7$ and $\{e, f\} \equiv \{1, 3\} (\mathrm{mod}\ 4)$,

$$B_i \subset X_{2(i+f)+1} \cup X_{2(i+f)+2}, \quad |B_i| = m, \tag{34}$$

$$H_i = \bigcup_{\gamma \in B_i} ((S, \gamma S) \cup (N, \gamma N)), \quad D_i = C_i \cup C_{i+2} \cup C_{i+e} \cup H_i, \tag{35}$$

$i = 0,1,2,3$.

Theorem 5 *D_0, D_1, D_2 and D_3 given in (34) and (35) are* $4\text{-}\{q^2; q(q-1)/2, q(q-2)\}SDS$.

Proof. First, (34) and (35) ensure (30) for every $D_i, i = 0,1,2,3$.

Then, from Lemma 2 we have

$$\begin{aligned}\triangle D_i &= 2m(4m+1)+m(7m+2)GF(q^2)^*-m(GF(q^2)^*-C_{i+f}-C_{i+f+4}) \\ &\quad +\triangle\ (C_i+C_{i+2}+C_{i+e}).\end{aligned}$$

Hence

$$\begin{aligned}\sum_{i=0}^{3} \triangle D_i &= 8m(4m+1)+m(28m+5)GF(q^2)^*+\sum_{i=0}^{3}\triangle(C_i+C_{i+2}+C_{i+e}) \\ &= q^2+q(q-2)GF(q^2),\end{aligned}$$

where we used the following equations:

$$\begin{aligned}\triangle(C_i + C_{i+2} + C_{i+e}) &= 3(2m+1)(4m+1) + \sum_{j=0}^{3} \alpha_j (C_{i+j} + C_{i+j+4}),\\ \sum_{j=0}^{3} \alpha_j &= 36m^2 + 27m + 3.\end{aligned}$$

□

Remark. The $(1,-1)$ incidence matrices of D_0, D_1, D_2 and D_3 in Theorem 4 or Theorem 5 maybe used to construct an Hadamard matrix of order $4q^2$ with Goethals-Seidel or Wallis-Whiteman type [13].

5 Constructing T-matrices

T-matrices play an important role in composite Hadamard matrices.

Definition 1 *(T-matrices) $(0, \pm 1)$ matrices T_1, T_2, T_3 and T_4 of order t are called T-matrices if the following five conditions are satisfied:*

(a) They are pairwise commute;

(b) There is a monomial matrix R of order t, $R' = R$, $R^2 = I$, such that

$$(T_i R)' = T_i R, \ i = 1, 2, 3, 4;$$

(c) $T_i * T_j = 0, i \neq j, 1 \leq i, j \leq 4$, where $*$ denotes Hadamard product;

(d) $T_1 + T_2 + T_3 + T_4$ is a $(1, -1)$ matrix;

(e) $\sum_{i=1}^{4} T_i T_i' = tI$.

Let $C_0, \cdots, C_7$ be given as in (10), (11), (17), (18), (20)−(23) respectively. We know that for each i, $0 \leq i \leq 7$, there is a set A_i of numbers, such that

$$\begin{aligned}&|A_i| = 2m+1, \qquad A_i \subset \{0, 1, \cdots, 16m+7\},\\ &C_i = \textstyle\bigcup_{j \in A_i} E_j, \qquad i = 0, 1, \cdots, 7.\end{aligned}$$

It is clear that

$$\bigcup_{i=0}^{7} A_i = \{0, 1, \cdots, 16m+7\},$$

and for $i = 0, 1, 2, 3$,

$$A_i + 8m + 4 = \{a + 8m + 4 (\bmod\ 16m+8) : a \in A_i\} = A_{i+4}.$$

For each $i, 0 \leq i \leq 3$, choose a subset I_i of A_i such that $|I_i| = m$. Denote $A_i \backslash I_i$ by $\bar{I}_i$, $i = 0, 1, 2, 3$. Set

$$\begin{aligned}
D_0 &= \bigcup_{i \in I_3} (E_i \cup E_{i+8m+4}) \cup C_0 \cup C_1 \cup C_2, \\
D_2 &= \bigcup_{i \in I_1} (E_i \cup E_{i+8m+4}) \cup C_2 \cup C_3 \cup C_4, \\
D_1 &= \bigcup_{i \in I_0} (E_i \cup E_{i+8m+4}) \cup \left(\bigcup_{j \in \bar{I}_1} (E_j \cup E_{j+8m+4}) \right) \\
&\quad \cup \left(\bigcup_{k \in I_2} (E_k \cup E_{k+8m+4}) \right) \cup C_3, \\
D_3 &= \bigcup_{i \in \bar{I}_0} (E_i \cup E_{i+8m+4}) \cup \left(\bigcup_{j \in I_2} (E_j \cup E_{j+8m+4}) \right) \\
&\quad \cup \left(\bigcup_{k \in I_3} (E_k \cup E_{k+8m+4}) \right) \cup C_5. \qquad (36)
\end{aligned}$$

Theorem 6 *D_0, D_1, D_2 and D_3 defined in (36) are 4-$\{q^2; q(q-1)/2; q(q-2)\}SDS$.*

Proof. First, we see that, for each $D_i, 0 \leq i \leq 3$, (30) is valid. Then, from Lemma 2 it follows that

$$\begin{aligned}
\triangle D_0 &= 2m(4m+1) + m(7m+1)GF(q^2)^* + m(C_3 + C_7) + \triangle(C_0 + C_1 + C_2), \\
\triangle D_2 &= 2m(4m+1) + m(7m+1)GF(q^2)^* + m(C_1 + C_5) + \triangle(C_2 + C_3 + C_4), \\
\triangle D_1 &= 2(3m+1)(4m+1) + (3m+1)(5m+1)GF(q^2)^* - \\
&\quad (3m+1)(C_3 + C_7) + \triangle C_3, \\
\triangle D_3 &= 2(3m+1)(4m+1) + (3m+1)(5m+1)GF(q^2)^* - \\
&\quad (3m+1)(C_1 + C_5) + \triangle C_5.
\end{aligned}$$

From Theorem 3 it is easy to verify that

$$\sum_{i=0}^{3} \triangle D_i = q^2 + q(q-2)GF(q^2).$$

The theorem is proved. □

We have need to point out that every element of $GF(q^2)$ appears an even number of times in the system of D_0, D_1, D_2 and D_3 given in (36). Hence from Theorem 1 and Theorem 3 of [14] and Theorem 6 above we obtain the following theorem.

Theorem 7 *There exist T-matrices of order q^2 with q prime power $\equiv 3 \pmod 8$.*

It is worth pointing out that from [13], [15] and this paper one would know the state of the art concerning Hadamard matrices of order $4q^2$ (q prime power), namely, the only open case is $q \equiv 7 \bmod 8$.

References

[1] L. D. Baumert and M. Hall, Jr., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **71** (1965), 169–170.

[2] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy. *J. Number Theory* **14** (1982), 67–82.

[3] Y. Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields and their Applications* **3** (1997), 234–256.

[4] Joan Cooper and Jennifer Seberry Wallis, A construction for Hadamard arrays, *Bull. Austral. Math. Soc.* **7** (1972), 269–278.

[5] M. Hall, Jr., *Combinatorial Theory, 2nd ed.*, John Wiley & Sons, New York, 1986.

[6] D. Jungnickel, *Finite fields. Structure and arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[7] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, Berlin, 1986.

[8] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, Cambridge, 1994.

[9] A. Pott, *Finite Geometry and Character Theory*, Lec. Notes Math. 1601 (1995), Springer-Verlag, New York, Berlin.

[10] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, *Contemporary Design Theory*, Wiley, New York, 1992, 431–560.

[11] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four symbol sequences, pulse compression and surface wave codings, *J. Combin. Theory, Ser. A* **16** (1974), 313–333.

[12] M. Y. Xia, On supplementary difference sets and Hadamard marices, *Acta Math. Sci.* **4** (1984), 81–92 (Chinese).

[13] M. Y. Xia and G. Liu, A new family of supplementary difference sets and Hadamard matrices, *J. Stat. Plan. Inf.* **51** (1996), 283–291.

[14] M. Y. Xia and T. B. Xia, A family of C-partitions and T-matrices, *J. Combin. Designs* **7** (1999), 269–281.

[15] M. Y. Xia, T. B. Xia and J. Seberry, A new method for constructing Williamson matrices, *Des. Codes Cryptography* **35** (2005), 191–209.

[16] M. Y. Xia, T. B. Xia and J. Seberry, An infinite family of Goethals-Seidel arrays, *Discrete App. Math.* **145** (2005), 498–504.

(Received 1 Aug 2003)