A new method for constructing Williamson matrices

Keywords: Hadamard matrix, Williamson type Hadamard matrices, Partitions

Correspondent address:
Tianbing Xia
School of IT & CS
University of Wollongong
Northfields Ave., NSW 2522
Australia
Email: txia@uow.edu.au

A new method for constructing Williamson matrices *

Mingyuan Xia
Department of Mathematics,
Central China Normal University,
Wuhan, Hubei 430079, China
Email: xiamy@ccnu.edu.cn
Jennifer Seberry, Tianbing Xia
School of IT & CS,
University of Wollongong, NSW 2500, Australia
Email: [j.seberry, txia]@uow.edu.au

Abstract

For every prime power $q \equiv 1 \ (mod\ 4)$ we prove the existence of $(q; x, y)-$partitions of $GF(q)$ with $q = x^2 + 4y^2$ for some x, y, which are very useful for constructing SDS, DS and Hadamard matrices. We discussed the transformations of $(q; x, y)-$partitions and, by using the partitions, constructed generalized cyclotomic classes which have properties similar to those of classical cyclotomic classes. Thus we provided a new construction for Williamson matrices of order q^2.

1 Introduction

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

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

*The subject supported by the NSF of China (No. 10071029).

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

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

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 $A = \phi$, we define

$$\triangle\phi = 0, \quad \triangle(\phi, B) = 0.$$

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

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

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 paper we assume p is an odd prime,

$$q = p^r = 4m + 1 = x^2 + 4y^2 \tag{1}$$

with $x \equiv 1 (mod\, 4)$.

Turyn constructed $(4 \cdot 3^{2r}, 2 \cdot 3^{2r} - 3^r, 3^{2r} - 3^r)$ Hadamard difference sets [10]. Latter, M. Xia [14] constructed $(4q^2, 2q^2 - q, q^2 - q)$ Hadamard difference sets for $p \equiv 3(mod\, 4)$. Xiang and Chen gave a more transparent viewpoint of Xia's construction [16]. van Eupen and Tonchev found examples of $(2500, 1225, 600)$ difference sets in $Z_2^2 \times Z_5^4$ [4]. Inspired by these examples, Wilson and Xiang introduced a general method of constructing Hadamard difference sets and gave the construction of $(4p^4, 2p^4 - p^2, p^4 - p^2)$ DS for $p = 5, 13$ and 17 [12]. Finally, Chen [2] proved the existence of $(4p^4, 2p^4 - p^2, p^4 - p^2)$ DS for all odd primes p by using relative $(q + 1, 2, q, (q - 1)/2)$ DS and generalized the results of [3].

In this paper, we propose the notion of $(q;x,y)-$partition of $GF(q)$ and prove its existence for some x, y satisfying (1). It provides a very useful method for constructing SDS, DS and Williamson type Hadamard matrices. This is a generalization of the partition in [2] (Lemma 2.4) from $GF(q^2)$ to $GF(q)$. The partitions constructed by Chen are exactly the case: q is a complete square and $y=0$. When $p \equiv 3(mod\, 4)$, $(q;x,y)-$partitions constructed in this paper become $(q;x,0)-$partitions, which are consistent with the partitions in [2].

The rest of the paper is organized as follows. In section 2, we will partition the group $GF(q)$ into four subsets with certain desirable properties. In section 3, we use the partition obtained in Section 2 to give the generalized cyclotomic classes, and by using them to construct $4-\{q^2;k;\lambda\}$ SDS with $(k,\lambda)=((q^2-1)/4,(q^2-5)/4)$ and $(q(q-1)/2,q(q-2))$. In section 4, we consider the case: q is a complete square.

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

$$\begin{aligned}
q: &\quad \text{a power of an odd prime p},\\
GF(q): &\quad \text{the Galois field with } q \text{ elements},\\
GF(q)^*: &\quad \text{the multiplicative group of } GF(q)-\{0\},\\
S: &\quad \text{the set of all nonzero squares of } GF(q),\\
N: &\quad \text{the set of all nonsquares of } GF(q),\\
\delta: &\quad \text{a primitive element of } GF(q)^*,\\
Tr_{q^n}: &\quad \text{the absolute trace from } GF(q^n) \text{ to } GF(p),\\
Tr_{q^n/q}: &\quad \text{the relative trace from } GF(q^n) \text{ to } GF(q).
\end{aligned}$$

In this paper for every $g \in GF(q^n)$ we define

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

For the detailed discussion of absolute and relative trace maps of finite fields, we refer 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, α, $\beta \in GF(q^n)$, define a group homomorphism

$$\begin{aligned}
&\chi_\alpha: \ GF(q^n) \to C^*,\\
&\chi_\alpha(\beta)=\xi^{Tr_{q^n}(\alpha\beta)}.
\end{aligned}$$

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 $(q;x,y)-$Partitions

Let ω be a symbol. Then the set of all elements $\alpha\omega+\beta$, α, $\beta \in GF(q)$, is $GF(q^2)$. The polynomial $\omega^2-\delta$ is irreducible on $GF(q)$. It is well known that there is an element $g=\alpha\omega+\beta$, α, $\beta\in GF(q)$, such that

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

Choose a generator element g of $GF(q^2)$ and put

$$S_i = \{g^{(8m+4)j+i} : j=0,1,\cdots,2m-1\}, \quad i=0,1,\cdots,8m+3.$$

It is easy to show that

$$S_0 = \{\delta^{2k} : k=0,1,\cdots,2m-1\} = S$$

and

$$S_{4m+2} = \{\delta^{2k+1} : k=0,1,\cdots,2m-1\} = N.$$

For any i, $1\le i<8m+4$, $i\neq 4m+2$, write $g^i=\alpha\omega+\beta$. Then $\alpha\neq 0$ and

$$\begin{aligned} S_i = g^i S_0 &= \{\alpha\delta^{2k}\omega+\beta\delta^{2k} : k=0,1,\cdots,2m-1\} \\ &= \{(\alpha\delta^{2k}, \alpha^{-1}\beta(\alpha\delta^{2k})) : k=0,1,\cdots,2m-1\}. \end{aligned}$$

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

$$S_0=(0,S), \quad S_{4m+2}=(0,N)$$

and

$$\begin{aligned} \{(\beta,r\beta):\beta\in S\} &= (S,rS), \\ \{(\beta,r\beta):\beta\in N\} &= (N,rN). \end{aligned}$$

The partition given in the following theorem is basic for this paper. It provide a new method for constructing SDS, DS and Hadamard matrices.

Theorem 1 *There exist four subsets X_1, X_2, X_3 and X_4 of $GF(q)$, such that*

$$\begin{aligned} \{|X_1|,|X_2|\} &= \{m+y, m-y\}, \\ \{|X_3|,|X_4|\} &= \{m+\tfrac{1}{2}(1+x), m+\tfrac{1}{2}(1-x)\}, \end{aligned} \tag{2}$$

$$X_1+X_2+X_3+X_4 = GF(q), \tag{3}$$

$$X_1S+X_2N = \sum_{i=1}^{4}(|X_i|-1)X_i, \tag{4}$$

$$X_1N+X_2S = |X_2|X_1+|X_1|X_2+|X_4|X_3+|X_3|X_4, \tag{5}$$

$$X_3S+X_4N = |X_3|X_1+|X_4|X_2+|X_2|X_3+|X_1|X_4, \tag{6}$$

$$X_3N+X_4S = |X_4|X_1+|X_3|X_2+|X_1|X_3+|X_2|X_4, \tag{7}$$

for some x, y satisfying (1).

We call the partition satisfying (2)–(7) the $(q;x,y)-$partition.

Proof. Put

$$C_i = \{g^k : k = i(mod\ 4)\},\quad i = 0, 1, 2, 3,$$

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

$$C_i = \bigcup_{j=0}^{2m} S_{4j+i},\quad i = 0, 1, 2, 3.$$

Particularly, C_0 and $C_2 = g^{4m+2}C_0$ can be written in the forms

$$C_0 = (0, S) \cup \{(S, rS), r \in X_1\} \cup \{(N, rN), r \in X_2\}, \tag{8}$$
$$C_2 = (0, N) \cup \{(N, rN), r \in X_1\} \cup \{(S, rS), r \in X_2\} \tag{9}$$

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

$$|X_1| + |X_2| = 2m. \tag{10}$$

For any $1 \leq i \leq 2m$, write $g^{4i} = \alpha\omega + \beta (\in S_{4i})$, and $\alpha \neq 0$ for sure. Now

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

and

$$(\alpha\omega + \beta)^{4m+1} = \alpha\omega^{4m+1} + \beta = -\alpha\omega + \beta.$$

So $\alpha(-\alpha) \in S$ and $\alpha^{-1}\beta + (-\alpha)^{-1}\beta = 0$. Therefore, $r = \alpha^{-1}\beta \in X_i$ if and only if $-r \in X_i$, $i = 1, 2$. These facts, together with (10), show that

$$|X_1| \equiv 0 \equiv |X_2|(mod\ 2) \tag{11}$$

and

$$0 \notin X_1 \cup X_2. \tag{12}$$

Now take

$$X_3 = \{r^{-1}\delta : r \in (X_1 \cap N) \cup (X_2 \cap S)\}, \tag{13}$$
$$X_4 = \{0\} \cup \{r^{-1}\delta : r \in (X_1 \cap S) \cup (X_2 \cap N)\}. \tag{14}$$

Since $\{C_1, C_3\} = \{g^{2m+1}C_0, g^{6m+3}C_0\}$ and $\{S_{2m+1}, S_{6m+3}\} = \{(S, 0), (N, 0)\}$. So

$$\{g^{2m+1}C_0, g^{6m+3}C_0\} = \{\bigcup_{r\in X_3}(S, rS)\cup(\bigcup_{r\in X_4}(N, rN)), \bigcup_{r\in X_3}(N, rN)\cup(\bigcup_{r\in X_4}(S, rS))\}.$$

Without loss of generality, we can write

$$C_1 = \{(S, rS), r \in X_3\} \cup \{(N, rN), r \in X_4\}, \tag{15}$$
$$C_3 = \{(N, rN), r \in X_3\} \cup \{(S, rS), r \in X_4\}. \tag{16}$$

Clearly,

$$|X_3| + |X_4| = 2m + 1. \tag{17}$$

From Whiteman [11] we know that

$$(|X_1| - |X_2|)^2 + (|X_3| - |X_4|)^2 = q. \tag{18}$$

From (10), (11), (17) and (18) it follows that

$$(|X_1| - |X_2|)^2 \ \cong 4y^2 \text{ and } (|X_3| - |X_4|)^2 \ \cong x^2$$

for some x, y. Conseqently,

$$\begin{aligned} \{|X_1|, |X_2|\} &= \{m + y, m - y\}, \\ \{|X_3|, |X_4|\} &= \{m + \frac{1}{2}(1 + x), m + \frac{1}{2}(1 - x)\}, \end{aligned}$$

and (2) is proved.

Since

$$\{(S, rS), r \in X_1 \cup X_3\} \cup \{(N, rN), r \in X_2, X_4\} = \bigcup_{i=1}^{2m} S_{4i} \cup (\bigcup_{j=0}^{2m} S_{4j+1}),$$

we have

$$|X_1 \cup X_2 \cup X_3 \cup X_4| = 4m + 1,$$

that is

$$X_1 + X_2 + X_3 + X_4 = GF(q),$$

and (3) holds.

Now we are going to prove (4)$-$(7).

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

$$\{hC_0, hC_1, hC_2, hC_3\} = \{C_0, C_1, C_2, C_3\}. \tag{19}$$

Note that

$$(\alpha\omega + \beta)(\alpha^{'}\omega + \beta^{'}) = (\alpha\beta^{'} + \beta\alpha^{'}, \alpha\alpha^{'}\delta + \beta\beta^{'}), \tag{20}$$

we have

$$\begin{aligned} hC_0 = \ & (\alpha S, \beta S) \cup \{((\alpha r + \beta)S, (\alpha\delta + \beta r)S), r \in X_1\} \cup \\ & \{((\alpha r + \beta)N, (\alpha\delta + \beta r)N), r \in X_2\}, \end{aligned} \tag{21}$$

$$\begin{aligned} hC_2 = \ & (\alpha N, \beta N) \cup \{((\alpha r + \beta)N, (\alpha\delta + \beta r)N), r \in X_1\} \cup \\ & \{((\alpha r + \beta)S, (\alpha\delta + \beta r)S), r \in X_2\}, \end{aligned} \tag{22}$$

$$\begin{aligned} hC_1 = \ & \{((\alpha r + \beta)S, (\alpha\delta + \beta r)S), r \in X_3\} \cup \\ & \{((\alpha r + \beta)N, (\alpha\delta + \beta r)N), r \in X_4\}, \end{aligned} \tag{23}$$

$$\begin{aligned} hC_3 = \ & \{((\alpha r + \beta)N, (\alpha\delta + \beta r)N), r \in X_3\} \cup \\ & \{((\alpha r + \beta)S, (\alpha\delta + \beta r)S), r \in X_4\}. \end{aligned} \tag{24}$$

For any $r_0 \in X_1$ we can choose α, $\beta \in GF(q)$ such that $\alpha \in S$ and $\alpha^{-1}\beta = -r_0$. Since $-r_0 \in X_1$ and in (21) the term

$$(\alpha S, \beta S) = (S, -r_0 S) \in C_0,$$

it follows that

$$hC_0 = C_0 \text{ and } hC_2 = C_2.$$

Consequently, in (21) the term

$$((\alpha r_0 + \beta)S, (\alpha\delta + \beta r_0)S) = (0, (\delta - r_0^2)S)$$

should be equal to $(0, S)$. *i.e.*, $\delta - r_0^2 \in S$. Now

$$\begin{aligned} hC_0 &= (S, -r_0 S) \cup (0, S) \cup \{((r - r_0)S, (\delta - r_0 r)S), r \in X_1, r \neq r_0\} \\ &\quad \cup\{((r - r_0)N, (\delta - r_0 r)N), r \in X_2\} \\ &= (0, S) \cup (S, -r_0 S) \cup \{(S, r^{-1}(\delta - r_0^2 - r_0 r)S), r \in E_1\} \\ &\quad \cup\{(N, r^{-1}(\delta - r_0^2 - r_0 r)N), r \in E_2\} \end{aligned}$$

where

$$\begin{aligned} &X + r = \{\alpha + r : \alpha \in X\}, \\ &E_1 = ((X_1 - r_0) \cap S) \cup ((X_2 - r_0) \cap N), \quad (25) \\ &E_2 = ((X_1 - r_0) \cap N) \cup ((X_2 - r_0) \cap S). \quad (26) \end{aligned}$$

Comparing expression (21) with (8), we have

$$\begin{aligned} |E_1| &= |(X_1 - r_0) \cap S)| + |(X_2 - r_0) \cap N| = |X_1| - 1, \quad (27) \\ |E_2| &= |(X_1 - r_0) \cap N| + |(X_2 - r_0) \cap S| = |X_2|. \quad (28) \end{aligned}$$

(27) and (28) mean that the coefficients of r_0 in $X_1S + X_2N$ and $X_1N + X_2S$ are $|X_1| - 1$ and $|X_2|$ respectively.

Similarly, for $r_0 \in X_1$ we can prove $hC_1 = C_1$ and $hC_3 = C_3$. Comparing the expression (23) with (15), it follows that the cofficients of r_0 in $X_3S + X_4N$ and $X_3N + X_4S$ are $|X_3|$ and $|X_4|$ respectively.

Similarly, repeating the procedure above for X_2, X_3 and X_4, one can get (4)$-$(7). Theorem 1 is proved. □

Theorem 2 *Let $W = \{X_1, X_2, X_3, X_4\}$ be a $(q; x, y)-$partition of $GF(q)$, β, $r \in GF(q)$ and $\beta \neq 0$, and $\bar{W} = \{\bar{X}_1, \bar{X}_2, \bar{X}_3, \bar{X}_4\}$ obtained from W under the following transformations:*

(a) $\bar{X}_i = X_i + r$, $i = 1, 2, 3, 4$,

(b) $\bar{X}_i = \{\alpha^p :\ \alpha \in X_i\}$, $i = 1, 2, 3, 4$,

(c) $\bar{X}_i = \beta X_i$, *$i = 1,2,3,4$ for $\beta \in S$,*

(d) $\bar{X}_1 = \beta X_2$, $\bar{X}_2 = \beta X_1$, $\bar{X}_i = \beta X_i$, *$i = 3,4$ for $\beta \in N$.*

Then $\bar{W}$ is also a $(q;x,y)-$partition of $GF(q)$.

The proof of Theorem 2 is trivial.

Remark 1 *If q is a prime, the representation $q = x^2 + 4y^2$ is known to be unique. If $q = p^r$, $p \equiv 3(mod\ 4)$, then r is even, $r = 2t$, and the unique solution is $x = \pm p^t$, $y = 0$. If $q = p^r$, $r > 1$, $p \equiv 1(mod\ 4)$, the representation is not unique, and so the values of x and y in (1) and (2) are not completely determined by Theorem 1. In the last case there is a problem: Does a $(q;x,y)-$partition exist for every given pair (x,y) satisfying (1)?*

Example 1 $q = 125 = 4 \cdot 31 + 1 = 5^2 + 4 \cdot 5^2 = (-11)^2 + 4 \cdot 1^2$.
Let δ be a root of the equation $\delta^3 = \delta + 2$. Then

$$GF(5^3)^* = \{\delta^i : i = 0, 1, \cdots, 123\}.$$

Denote

$$\begin{aligned}
I_1 &= \{9,12,24,27,30,32,34,37,40,43,44,45,47,56,58,59,\\
&\quad 71,74,86,89,92,94,96,99,102,105,106,107,109,118,120,121\},\\
I_2 &= \{1,2,3,8,11,13,15,22,35,38,42,46,49,53,57,63,64,\\
&\quad 65,70,73,75,77,84,97,100,104,108,111,115,119\},\\
I_3 &= \{4,16,17,18,20,21,25,26,36,41,54,55,61,66,78,79,80,\\
&\quad 82,83,87,88,98,103,116,117,123\},\\
I_4 &= \{0,5,6,7,10,14,19,23,28,29,31,33,39,48,50,51,52,60,62,\\
&\quad 67,68,69,72,76,81,85,90,91,93,95,101,110,112,113,114,122\}.
\end{aligned}$$

Take

$$X_i = \{\delta^j : j \in I_i\}, \quad i = 1,2,3, \quad X_4 = \{0\} \cup \{\delta^j : j \in I_4\}.$$

It is easy to verify that $\{X_1, X_2, X_3, X_4\}$ is a $(125; -11, 1)-$partition.

Does a $(125; 5, 5)-$partition exist?

Remark 2 *Indeed, the following numbers*

$$\begin{aligned}
&|(X_1+\alpha) \cap S| + |(X_2+\alpha) \cap N|,\\
&|(X_1+\alpha) \cap N| + |(X_2+\alpha) \cap S|,\\
&|(X_3+\alpha) \cap S| + |(X_4+\alpha) \cap N|,\\
&|(X_3+\alpha) \cap N| + |(X_4+\alpha) \cap S|
\end{aligned}$$

are equal to the coefficients of $-\alpha \in GF(q)$ *in*

$$\begin{aligned} &X_1S + X_2N, \\ &X_1N + X_2S, \\ &X_3S + X_4N, \\ &X_3N + X_4S \end{aligned}$$

respectively.

3 Generalized cyclotomic classes and SDS

In this section, by using $(q;x,y)-$partitions, we will construct generalized cyclotomic classes and SDS.

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 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 $\chi_\beta(Q)$ by $\chi_N(Q)$ 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] and [8] or uniform cyclotomy [1]. They are

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

Theorem 3 *Suppose* $\{X_1, X_2, X_3, X_4\}$ *is a* $(q;x,y)-$*partition of* $GF(q)$. C_0, C_2, C_1 *and* C_3 *are subsets of* $GF(q^2)$, *given as in (8), (9), (15) and (16) respectively. Then*

$$C_iC_j = \delta_{ij}2m(2m+1) + \sum_{k=0}^{3}\langle j-i, k\rangle C_{i+k}, \quad 0 \le i \le j \le 3, \tag{29}$$

where $\delta_{ij} = 0$ *or* 1 *according as* $i \neq j$ *or* $i = j$, *the table for* $\langle i,j\rangle$ *is, with* $\langle i,j\rangle$ *in the ith row and jth column,* $i, j = 0, 1, 2, 3$,

$$\begin{array}{cccc} \langle 0,0\rangle & \langle 0,1\rangle & \langle 0,2\rangle & \langle 0,3\rangle \\ \langle 0,1\rangle & \langle 0,3\rangle & \langle 1,2\rangle & \langle 1,2\rangle \\ \langle 0,2\rangle & \langle 1,2\rangle & \langle 0,2\rangle & \langle 1,2\rangle \\ \langle 0,3\rangle & \langle 1,2\rangle & \langle 1,2\rangle & \langle 0,1\rangle \end{array}$$

in which

$$\langle 0,0\rangle = m^2 - m - 1 + 3y^2,$$

$$\begin{aligned}
\langle 0,1\rangle &= m^2+m-y^2+ef,\\
\langle 0,2\rangle &= m^2+m-y^2,\\
\langle 0,3\rangle &= m^2+m-y^2-ef,\\
\langle 1,2\rangle &= m^2+y^2,\\
e &= \frac{1}{2}(|X_1|-|X_2|), \quad f=|X_3|-|X_4|,
\end{aligned}$$

and $C_j = C_i$ *as* $i \equiv j(mod\, 4)$.

Proof. We denote the right hand side of (29) by R_{ij} and discuss the case $i=j=0$ at first. Now we calculate the character values of C_i, $i=0,1,2,3$, as follows.

For any α_1, $\alpha_2 \in GF(q)$,

$$\begin{aligned}
\chi_{(\alpha_1,\alpha_2)}(C_0) &= \sum_{\beta\in S}\xi^{Tr_{q^2}(\alpha_1\beta\omega+\alpha_2\beta)} + \sum_{\beta\in S, r\in X_1}\xi^{Tr_{q^2}((\alpha_1 r+\alpha_2)\beta\omega+\alpha_1\delta\beta+\alpha_2 r\beta)}\\
&\quad + \sum_{\beta\in N, r\in X_2}\xi^{Tr_{q^2}((\alpha_1 r+\alpha_2)\beta\omega+\alpha_1\delta\beta+\alpha_2 r\beta)}\\
&= \sum_{\beta\in S}\xi^{Tr_q(Tr_{q^2/q}(\alpha_1\beta\omega+\alpha_2\beta))}\\
&\quad + \sum_{\beta\in S, r\in X_1}\xi^{Tr_q(Tr_{q^2/q}((\alpha_1 r+\alpha_2)\beta\omega+\alpha_1\delta\beta+\alpha_2 r\beta))}\\
&\quad + \sum_{\beta\in N, r\in X_2}\xi^{Tr_q(Tr_{q^2/q}((\alpha_1 r+\alpha_2)\beta\omega+\alpha_1\delta\beta+\alpha_2 r\beta))}\\
&= \sum_{\beta\in S}\xi^{Tr_q(2\alpha_2\beta)} + \sum_{\beta\in S, r\in X_1}\xi^{Tr_q(2(\alpha_1\delta+\alpha_2 r)\beta)} + \sum_{\beta\in N, r\in X_2}\xi^{Tr_q(2(\alpha_1\delta+\alpha_2 r)\beta)}\\
&= \chi_{2\alpha_2}(S) + \sum_{r\in X_1}\chi_{2(\alpha_1\delta+\alpha_2 r)}(S) + \sum_{r\in X_2}\chi_{2(\alpha_1\delta+\alpha_2 r)}(N).
\end{aligned}$$

If $\alpha_1=\alpha_2=0$,

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

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

$$\begin{aligned}
\chi_{(\alpha_1,0)}(C_0) &= |S| + \sum_{r\in X_1}\chi_{2\alpha_1\delta}(S) + \sum_{r\in X_2}\chi_{2\alpha_1\delta}(N)\\
&= 2m + |X_1|\chi_{2\alpha_1}(N) + |X_2|\chi_{2\alpha_1}(S).
\end{aligned}$$

If $2\alpha_2\in S$, we set $\alpha = \alpha_2^{-1}\alpha_1\delta$, then

$$\begin{aligned}
\chi_{(\alpha_1,\alpha_2)}(C_0) &= a + \sum_{r\in X_1}\chi_{2\alpha_2(\alpha_1\alpha_2^{-1}\delta+r)}(S) + \sum_{r\in X_2}\chi_{2\alpha_2(\alpha_1\alpha_2^{-1}\delta+r)}(N)\\
&= a + \sum_{r\in X_1}\chi_{\alpha+r}(S) + \sum_{r\in X_2}\chi_{\alpha+r}(N)
\end{aligned}$$

$$\begin{aligned}
&= a+\sum_{r\in(X_1+\alpha)\cap S}\chi_r(S)+\sum_{r\in(X_1+\alpha)\cap N}\chi_r(S)\\
&\quad+\sum_{r\in(X_1+\alpha)\cap\{0\}}\chi_r(S)+\sum_{r\in(X_2+\alpha)\cap\{0\}}\chi_r(N)\\
&\quad+\sum_{r\in(X_2+\alpha)\cap S}\chi_r(N)+\sum_{r\in(X_2+\alpha)\cap N}\chi_r(N)\\
&= (1+k_1)a+k_2b+2m|((X_1\cup X_2)+\alpha)\cap\{0\}|,
\end{aligned}$$

where

$$k_1=|(X_1+\alpha)\cap S|+|(X_2+\alpha)\cap N|, \tag{30}$$
$$k_2=|(X_1+\alpha)\cap N|+|(X_2+\alpha)\cap S|. \tag{31}$$

If $2\alpha_2\in N$, let $\alpha=\alpha_1\alpha_2^{-1}\delta$ again, we get

$$\chi_{(\alpha_1,\alpha_2)}(C_0)=(1+k_1)b+k_2a+2m|((X_1\cup X_2)+\alpha)\cap\{0\}|.$$

Similarly, we have

$$\begin{aligned}
&\chi_{(0,0)}(C_2)=2m(2m+1),\\
&\chi_{(\alpha_1,0)}(C_2)=2m+|X_1|\chi_{2\alpha_1}(S)+|X_2|\chi_{2\alpha_1}(N),\\
&\chi_{(\alpha_1,\alpha_2)}(C_2)=\begin{cases}(1+k_1)b+k_2a+2m|((X_1\cup X_2)+\alpha)\cap\{0\}|, & 2\alpha_2\in S,\\ (1+k_1)a+k_2b+2m|((X_1\cup X_2)+\alpha)\cap\{0\}|, & 2\alpha_2\in N,\end{cases}\\
&\chi_{(0,0)}(C_1)=2m(2m+1),\\
&\chi_{(\alpha_1,0)}(C_1)=|X_3|\chi_{2\alpha_1}(N)+|X_4|\chi_{2\alpha_1}(S),\\
&\chi_{(\alpha_1,\alpha_2)}(C_1)=\begin{cases}k_3a+k_4b+2m|((X_3\cup X_4)+\alpha)\cap\{0\}|, & 2\alpha_2\in S,\\ k_3b+k_4a+2m|((X_3\cup X_4)+\alpha)\cap\{0\}|, & 2\alpha_2\in N,\end{cases}
\end{aligned}$$

and

$$\begin{aligned}
&\chi_{(0,0)}(C_3)=2m(2m+1),\\
&\chi_{(\alpha_1,0)}(C_3)=|X_3|\chi_{2\alpha_1}(S)+|X_4|\chi_{2\alpha_1}(N),\\
&\chi_{(\alpha_1,\alpha_2)}(C_3)=\begin{cases}k_3b+k_4a+2m|((X_3\cup X_4)+\alpha)\cap\{0\}|, & 2\alpha_2\in S,\\ k_3a+k_4b+2m|((X_3\cup X_4)+\alpha)\cap\{0\}|, & 2\alpha_2\in N,\end{cases}
\end{aligned}$$

where

$$k_3=|(X_3+\alpha)\cap S|+|(X_4+\alpha)\cap N|, \tag{32}$$
$$k_4=|(X_3+\alpha)\cap N|+|(X_4+\alpha)\cap S|. \tag{33}$$

It is trivial that

$$|\ C_0C_0\ |=4m^2(2m+1)^2=|\ R_{00}\ |\ .$$

We know that for any $r \neq 0$,

$$\chi_r(S) + \chi_r(N) = -1, \quad \chi_r(S)\chi_r(N) = -m,$$
$$\chi_r^2(S) = m - \chi_r(S), \quad \chi_r^2(N) = m - \chi_r(N).$$

Hence, for $\alpha_1 \neq 0$,

$$\begin{aligned}
\chi_{(\alpha_1,0)}(C_0C_0) &= [2m + |X_1|\chi_{2\alpha_1}(N) + |X_2|\chi_{2\alpha_1}(S)]^2 \\
&= m^2 + (4m+1)y^2 + 2me[\chi_{2\alpha_1}(N) - \chi_{2\alpha_1}(S)]
\end{aligned}$$

and

$$\begin{aligned}
\chi_{(\alpha_1,0)}(R_{00}) &= 2m(2m+1) + \sum_{i=0}^{3}\langle 0,i\rangle\chi_{(\alpha_1,0)}(C_i) \\
&= 2m(2m+1) - \langle 0,2\rangle + (\langle 0,0\rangle - \langle 0,2\rangle)\chi_{(\alpha_1,0)}(C_0) \\
&\quad +(\langle 0,1\rangle - \langle 0,2\rangle)\chi_{(\alpha_1,0)}(C_1) + (\langle 0,3\rangle - \langle 0,2\rangle)\chi_{(\alpha_1,0)}(C_3) \\
&= m^2 + (4m+1)y^2 + 2me(\chi_{2\alpha_1}(N) - \chi_{2\alpha_1}(S)).
\end{aligned}$$

For $2\alpha_2 \in S$,

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

and

$$\begin{aligned}
\chi_{(\alpha_1,\alpha_2)}(R_{00}) &= 2m(2m+1) - \langle 0,2\rangle + (\langle 0,0\rangle - \langle 0,2\rangle)\chi_{(\alpha_1,\alpha_2)}(C_0) \\
&\quad +(\langle 0,1\rangle - \langle 0,2\rangle)\chi_{(\alpha_1,\alpha_2)}(C_1) + (\langle 0,3\rangle - \langle 0,2\rangle)\chi_{(\alpha_1,\alpha_2)}(C_3) \\
&= 3m^2 + m + y^2 + ef(k_3 - k_4)(a-b) \\
&\quad +(4y^2 - 2m - 1)((1+k_1)a + k_2b \\
&\quad +2m|((X_1 \cup X_2) + \alpha) \cap \{0\}|).
\end{aligned}$$

If $-\alpha \in X_1$, noting Remark 2, from (30) $-$ (33) and Theorem 1, we have

$$k_1 = |X_1| - 1, \quad k_2 = |X_2|, \quad k_3 = |X_3| \text{ and } k_4 = |X_4|.$$

Hence

$$\begin{aligned}
\chi_{(\alpha_1,\alpha_2)}(C_0C_0) &= m(|X_1| - |X_2|)^2 - |X_1|^2a - |X_2|^2b \\
&\quad +4m(m + |X_1|a + |X_2|b) \\
&= m^2 + (4m+1)y^2 + 2me(a-b)
\end{aligned}$$

and

$$\begin{aligned}\chi_{(\alpha_1,\alpha_2)}(R_{00}) &= 3m^2+m+y^2+ef(|X_3|-|X_4|)(a-b)\\ &\quad +(4y^2-2m-1)(2m+|X_1|a+|X_2|b)\\ &= m^2+(4m+1)y^2+2me(a-b).\end{aligned}$$

If $-\alpha \in X_2$, then

$$k_1=|X_2|-1,\quad k_2=|X_1|,\quad k_3=|X_4| \text{ and } k_4=|X_3|,$$

we can get

$$\chi_{(\alpha_1,\alpha_2)}(C_0C_0)=m^2+(4m+1)y^2+2me(b-a)=\chi_{(\alpha_1,\alpha_2)}(R_{00}).$$

If $-\alpha \in X_3$, now

$$k_1=|X_3|-1,\quad k_2=|X_4|,\quad k_3=|X_2| \text{ and } k_4=|X_1|,$$

we get

$$\chi_{(\alpha_1,\alpha_2)}(C_0C_0)=5m^2+3m+\frac{1}{2}-(4m+1)y^2+f(m+\frac{1}{2})(b-a)=\chi_{(\alpha_1,\alpha_2)}(R_{00}).$$

Finally, if $-\alpha \in X_4$, then

$$k_1=|X_4|-1,\quad k_2=|X_3|,\quad k_3=|X_1| \text{ and } k_4=|X_2|,$$

we have

$$\chi_{(\alpha_1,\alpha_2)}(C_0C_0)=5m^2+3m+\frac{1}{2}-(4m+1)y^2+f(m+\frac{1}{2})(a-b)=\chi_{(\alpha_1,\alpha_2)}(R_{00}).$$

For $2\alpha_2 \in N$, the equation

$$\chi_{(\alpha_1,\alpha_2)}(C_0C_0)=\chi_{(\alpha_1,\alpha_2)}(R_{00})$$

holds too. From the discussion above it follows that

$$C_0C_0=R_{00}=2m(2m+1)+\langle 0,0\rangle C_0+\langle 0,1\rangle C_1+\langle 0,2\rangle C_2+\langle 0,3\rangle C_3.$$

The proof of the rest of the theorem is similar. $\square$

Theorem 3 shows that the formulas (11.6.85) and (11.6.90) in [5] (pp. 187-188) are still valid for C_0, C_2, C_1 and C_3 defined by (8), (9), (15) and (16) respectively, which need not be cyclotomic sets. We call them generalized cyclotomic classes.

Theorem 4 *Under the assumptions of Theorem 3, C_0, C_1, C_2 and C_3 are $4-\{q^2; \frac{(q^2-1)}{4}; \frac{(q^2-5)}{4}\}$ SDS in $GF(q^2)$.*

Proof. Note that for every i, $0 \leq i \leq 3$,

$$\triangle C_i = C_i C_i^{(-1)} = C_i C_i,$$

from (29) we have

$$\sum_{i=0}^{3} \triangle C_i = \frac{1}{4}(3q^2+1) + \frac{1}{4}(q^2-5)GF(q^2).$$

The theorem is proved. □

Example 2 *Let $q = 5$. Now $m = x = y = 1$, $S = \{1, 4\}$, $N = \{2, 3\}$. Take*

$$X_1 = \{0, 1\}, \quad X_2 = \phi, \quad X_3 = \{2, 4\}, \quad \text{and } X_4 = \{3\}.$$

It is easy to verify that X_1, X_2, X_3 and X_4 satisfy (2)–(7). Define C_0, C_2, C_1 and C_3 by (8), (9), (15) and (16) respectively, then

$$\begin{array}{ll} C_0 = (0, S) \cup (S, 0) \cup (S, S), & C_2 = (0, N) \cup (N, 0) \cup (N, N), \\ C_1 = (S, 2S) \cup (S, 4S) \cup (N, 3N), & C_3 = (N, 2N) \cup (N, 4N) \cup (S, 3S). \end{array}$$

From Theorem 3 it follows that

$$\langle 0, 0 \rangle = \langle 0, 1 \rangle = 2, \quad \langle 0, 2 \rangle = \langle 1, 2 \rangle = 1, \quad \langle 0, 3 \rangle = 0.$$

It is easy to check that C_0, C_2, C_1 and C_3 satisfy (29). However they are generalized cyclotomic classes, not cyclotomic sets.

To construct $4 - \{q^2; \frac{1}{2}q(q-1); q(q-2)\}$ SDS in $GF(q^2)$ we need the following lemmas.

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

(i) $\triangle S_i = 2m + (m-1)S_i + mS_{i+4m+2}$,

(ii) $\triangle (S_i, S_{i+4m+2}) = 2m(S_i + S_{i+4m+2})$,

(iii) $\triangle (S_i + S_{i+4m+2}, S_j + S_{j+4m+2}) = 2GF(q^2)^* - 2(S_i + S_j + S_{i+4m+2} + S_{j+4m+2})$, $i \neq j$, $0 \leq i, j \leq 8m+3$.

For proof see [13].

Lemma 2 *Let $E = \bigcup_{i=1}^{m}(S_{a_i} \cup S_{a_i+4m+2})$, $\{a_1, \cdots, a_m\} \subset \{0, 1, \cdots, 8m+3\}$. Then*

(a) $\triangle E = 4m^2 + m(m+1)GF(q^2)^* + (2m+1)E$,

(b) for any α_1, $\alpha_2 \in GF(q)$, $(\alpha_1, \alpha_2) \neq (0,0)$,

$$\chi_{(\alpha_1,\alpha_2)}(E) = -m \text{ or } 3m+1. \tag{34}$$

Proof. (a) follows from Lemma 1 by direct calculation. Since $\triangle E = EE^{(-1)} = EE$, by (a) we get

$$\chi^2_{(\alpha_1,\alpha_2)}(E) = \chi_{(\alpha_1,\alpha_2)}(\triangle E) = 4m^2 - m(m-1) + (2m+1)\chi_{(\alpha_1,\alpha_2)}(E).$$

The last equation above of $\chi_{(\alpha_1,\alpha_2)}(E)$ has 2 roots: $-m$ and $3m+1$. This completes the proof. □

Let C_0, C_1, C_2 and C_3 be given in Theorem 3. Then they can be written in the following forms (see [13], [14] and [15] for details).

$$\begin{array}{ll} C_0 = \bigcup_{i=0}^{2m} S_{a_i}, & C_2 = \bigcup_{i=0}^{2m} S_{a_i+4m+2}, \\ C_1 = \bigcup_{j=0}^{2m} S_{b_j}, & C_3 = \bigcup_{j=0}^{2m} S_{b_j+4m+2}, \end{array}$$

where $\{a_0, \cdots, a_{2m}, b_0, \cdots, b_{2m}\} \equiv \{0, 1, \cdots, 4m+1\} (mod\ 4m+2)$. Take any subsets $F_1 \subset \{a_0, \cdots, a_{2m}\}$, $F_2 \subset \{b_0, \cdots, b_{2m}\}$, such that $|F_1| = |F_2| = m$, and put

$$A = \bigcup_{a_i \in F_1} (S_{a_i} \cup S_{a_i+4m+2}), \quad B = \bigcup_{b_j \in F_2} (S_{b_j} \cup S_{b_j+4m+2}), \tag{35}$$

$$D_0 = B \cup C_0, \quad D_2 = B \cup C_2, \quad D_1 = A \cup C_1, \quad D_3 = A \cup C_3. \tag{36}$$

Theorem 5 *D_0, D_1, D_2 and D_3 are $4 - \{q^2; \frac{1}{2}q(q-1); q(q-2)\}$ SDS in $GF(q^2)$.*

Proof. From Lemma 2 we can get

$$\begin{aligned} \triangle D_0 &= \triangle B + \triangle(B, C_0) + \triangle C_0 \\ &= 4m^2 + m(m-1)GF(q^2)^* + (2m+1)B + \triangle(B, C_0) + \triangle C_0 \end{aligned}$$

and

$$\triangle D_2 = 4m^2 + m(m-1)GF(q^2)^* + (2m+1)B + \triangle(B, C_2) + \triangle C_2.$$

Consequently from Lemma 1 we have

$$\begin{aligned} \triangle D_0 + \triangle D_2 &= 8m^2 + 2m(m-1)GF(q^2)^* + 2(2m+1)B \\ &\quad + \triangle(B, C_0 + C_2) + \triangle C_0 + \triangle C_2 \\ &= 8m^2 + 6m^2 GF(q^2)^* - 2m(C_0 + C_2) + \triangle C_0 + \triangle C_2. \end{aligned}$$

Similarly,

$$\triangle D_1 + \triangle D_3 = 8m^2 + 6m^2 GF(q^2)^* - 2m(C_1 + C_3) + \triangle C_1 + \triangle C_3.$$

Therefore, from Theorem 4

$$\begin{aligned}\sum_{i=0}^{3} \triangle D_i &= 16m^2 + (12m^2 - 2m)GF(q^2)^* + \sum_{i=0}^{3} \triangle C_i \\ &= q^2 + q(q-2)GF(q^2).\end{aligned}$$

The proof is completed. □

It is well known that the $(1, -1)$ incidence matrices (type 1) of D_0, D_1, D_2 and D_3 are Williamson type matrices of order q^2 (see [13]).

4 Square Case

Let q be a complete square. In this case [2] proved the following Theorem.

Theorem 6 *There exist four subsets X_1, X_2, X_3 and X_4 of $GF(q)$, such that*

$$|X_1| = |X_2| = m, \tag{37}$$

$$\{|X_3|, |X_4|\} = \{\frac{(\sqrt{q}-1)^2}{4}, \frac{(\sqrt{q}+1)^2}{4}\}, \tag{38}$$

and (3)–(7) hold.

In our terminology, this is a $(q; \pm\sqrt{q}, 0)-$partition.

Example 3 $q = 25 = 4 \cdot 6 + 1 = (-3)^2 + 4 \cdot 2^2 = 5^2$. *Now* $m = 6$. *Let* $\delta = z + 1$. *Then*

$$\begin{aligned}&GF(5^2)^* = \{\delta^k (mod\ z^2 - 3, mod\ 5) : \ k = 0, 1, \cdots, 23\}, \\ &S = \{\delta^{2k} : \ k = 0, \cdots, 11\}, \quad N = \{\delta^{2k+1} : \ k = 0, \cdots, 11\}.\end{aligned}$$

Case 1. $x = -3$, $y = 2$. *Take*

$$\begin{aligned}&X_1 = \{1, \delta^7, \delta^9, \delta^{10}, \delta^{12}, \delta^{19}, \delta^{21}, \delta^{22}\}, \quad X_2 = \{\delta^2, \delta^8, \delta^{14}, \delta^{20}\} \\ &X_3 = \{\delta^4, \delta^5, \delta^6, \delta^{11}, \delta^{16}, \delta^{17}, \delta^{18}, \delta^{23}\}, \quad X_4 = \{0, \delta, \delta^3, \delta^{13}, \delta^{15}\}.\end{aligned}$$

It is easy to verify that $\{X_1, X_2, X_3, X_4\}$ is a $(25; -3, 2)-$partition of $GF(25)$.

Case 2. $x = 5$, $y = 0$. *Take*

$$\begin{aligned}&Y_1 = \{\delta, \delta^2, \delta^{10}, \delta^{13}, \delta^{14}, \delta^{22}\}, \quad Y_2 = \{\delta^7, \delta^8, \delta^9, \delta^{19}, \delta^{20}, \delta^{21}\}, \\ &Y_3 = \{1, \delta^5, \delta^{12}, \delta^{17}\}, \quad Y_4 = \{0, \delta^3, \delta^4, \delta^6, \delta^{11}, \delta^{15}, \delta^{16}, \delta^{18}, \delta^{23}\}.\end{aligned}$$

It is easy to check that $\{Y_1, Y_2, Y_3, Y_4\}$ is a $(25; 5, 0)-$partition of $GF(25)$.

By the analogy with Theorem 2 we have

Theorem 7 *Let $W = \{X_1, X_2, X_3, X_4\}$ be a $(q; \pm\sqrt{q}, 0)-$partition of $GF(q)$, β, $r \in GF(q)$, $\beta \neq 0$, and $\bar{W} = \{\bar{X}_1,\ \bar{X}_2,\ \bar{X}_3,\ \bar{X}_4\}$ obtained from W under the following transformations:*

(a) $\bar{X}_i = X_i + r,\ i = 1, 2, 3, 4,$

(b) $\bar{X}_i = \{\alpha^p :\ \alpha \in X_i\},\ i = 1, 2, 3, 4,$

(c) $\bar{X}_i = \beta X_i,\ i = 1, 2, 3, 4,\ \beta \in S,$

(d) $\bar{X}_1 = \beta X_2,\ \bar{X}_2 = \beta X_1,\ \bar{X}_i = \beta X_i,\ i = 3, 4,\ \beta \in N.$

Then $\bar{W}$ is also a $(q; \pm\sqrt{q}, 0)-$partition of $GF(q)$.

There are some special properties of C_i, $i = 0,\ 1,\ 2,\ 3$, constructed from $(q; \pm\sqrt{q}, 0)-$partition by (8), (9), (15) and (16).

Theorem 8 *Suppose X_1, X_2, X_3 and X_4 form a $(q; \pm\sqrt{q}, 0)-$partition of $GF(q)$, C_0, C_1, C_2 and C_3 are given by (8), (15), (9) and (16) respectively. Then*

$$\triangle C_i = 2m(2m+1) - (2m+1)C_i + m(m+1)GF(q^2)^*,\ i = 0, 1, 2, 3, \tag{39}$$

and C_0, C_1, C_2 and C_3 are $4 - \{q^2; \frac{(q^2-1)}{4}; \frac{(q^2-5)}{4}\}$ SDS.

Proof. Since $y = 0$, in this case

$$\langle 0, 0 \rangle = m^2 - m - 1, \quad \langle 0, 1 \rangle = \langle 0, 2 \rangle = \langle 0, 3 \rangle = m^2 + m,$$

hence by Theorem 3 equation (39) holds. The second part of the theorem is trivial by Theorem 4. □

Lemma 3 *For any α_1, $\alpha_2 \in GF(q)$, $(\alpha_1, \alpha_2) \neq (0, 0)$, there exists only one C_i with $\chi_{(\alpha_1,\alpha_2)}(C_i) = -3m - 1$ and the others are $\chi_{(\alpha_1,\alpha_2)}(C_j) = m$, $j \neq i$.*

Proof. From (39) we have

$$\chi^2_{(\alpha_1,\alpha_2)}(C_i) = m(3m+1) - (2m+1)\chi_{(\alpha_1,\alpha_2)}(C_i).$$

Hence

$$\chi_{(\alpha_1,\alpha_2)}(C_i) = m \text{ or } -3m - 1. \tag{40}$$

$\sum_{i=0}^{3} \chi_{(\alpha_1,\alpha_2)}(C_i) = -1$. The conclusion of the lemma follows. □

Theorem 9 *Suppose X_1, X_2, X_3 and X_4 form a $(q;\pm\sqrt{q},0)-$partition of $GF(q)$, D_0, D_1, D_2 and D_3 are given as in (35) and (36). Then D_0, D_1, D_2 and D_3 are $4-\{q^2;\frac{1}{2}q(q-1);q(q-2)\}$ SDS, and for any $\alpha \in GF(q^2)^*$, there exists only one D_i with $\chi_\alpha(D_i)=\pm q$ and the others with $\chi_\alpha(D_j)=0$, $i\neq j$.*

Proof. The first part of Theorem 9 directly follows from Theorem 5. Since $\chi_\alpha(C_i)=m$ or $-3m-1$, and $\chi_\alpha(A)$ and $\chi_\alpha(B)=-m$ or $3m+1$, the possible values of $\chi_\alpha(D_i)$ would be 0, $\pm q$. Now

$$\sum_{i=0}^{3}\chi_\alpha^2(D_i)=q^2.$$

The second conclusion of the theorem follows immediately. □

Remark 3 *In $Z_2^2\times GF(q^2)$, let*

$$D=(0,0,D_0)\cup(0,1,D_1)\cup(1,0,D_2)\cup(1,1,GF(q^2)\backslash D_3).$$

It is well known that D would be a $(4q^2,2q^2-q,q^2-q)$ DS if X_1, X_2, X_3 and X_4 form a $(q;\pm\sqrt{q},0)-$partition, and the $(1,-1)$ incidence matrices (type 1) of D_0, D_1, D_2 and $GF(q^2)\backslash D_3$ are special Williamson matrices of order q^2 (see [4], [10], [14] and [15]).

References

[1] L. D. Baumert, W. H. Mills and R. L. Ward, Uniform cyclotomy, *J. Number Theory*, vol. 14, pp. 67-82, 1982.

[2] Y. Q. Chen, On the existence of Abelian Hadamard difference sets and a new family of difference sets, *Finite Fields and their Applications*, vol. 3, pp. 234-256, 1997.

[3] J. A. Davis and J. Jedwab, A unifying construction for difference sets, *J. Combin. Theory Ser. A*, vol. 80, pp.13-78, 1997.

[4] M. van. Eupen and V. D. Tonchev, Linear codes and the existence of a reversible Hadamard difference set in $Z_2\times Z_2\times Z_5^4$, *J. Comb. Theory Ser. A*, vol 79, pp. 161-167, 1997.

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

[6] D. Jungnickel, Finite Fields: Structure and Arithmetic, *BI-Wissenschaftsverlag*, Mannbeim, 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*, Lecture Notes in Mathematics, vol. 1601, Springer-Verlag, New York, Berlin, 1995.

[10] R. J. Turyn, A special class of Williamson matrices and difference sets, *J. Comb. Theory Ser. A*, 36, pp. 111-115, 1984.

[11] A. L. Whiteman, An infinite family of Hadamard matrices of Williamson type, *J. Combin. Theory Ser. A*, 14, pp. 334-340, 1973.

[12] R. M. Wilson and Q. Xiang, Constructions of Hadamard difference sets, *J. Combin. Theory Ser. A*, 77, pp. 148-160, 1997.

[13] M. Xia and G. Liu, An infinite class of supplementary difference sets and Williamson matrices, *J. Comb. Theory, Ser. A*, vol. 58, pp. 310-317, 1991.

[14] M. Xia, Some infinite classes of special Williamson matrices and difference sets, *Journal of Combinatorial Theory*, Ser. A, 61, pp. 230-242, 1992.

[15] M. Xia, Williamson matrices and difference sets, *Incl. Group, Difference sets and the Monster*, Walter de Gruyter, Berlin, New York, pp. 233-237, 1996.

[16] Q. Xiang and Y. Q. Chen, On Xia's construction of Hadamard difference sets, *Finite Fields and their Applications*, vol. 2, pp. 87-95, 1996.