

*Faculty of Informatics*

*Faculty of Informatics - Papers*

---

*University of Wollongong*

*Year 2006*

---

# New Constructing of regular Hadamard matrices

T. Xia\*      J. Seberry†

M. Xia‡

\*University of Wollongong, txia@uow.edu.au

†University of Wollongong, jennie@uow.edu.au

‡Central China Normal University, China

This article was originally published as Xia, T, Seberry, J and Xia, M, New Constructing of regular Hadamard matrices, WSEAS Transactions on Mathematics, 5(2006), 1068-1073.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/597>

# New Constructing of regular Hadamard matrices \*

Tianbing Xia, Jennifer Seberry  
 University of Wollongong  
 CCSR, SITACS  
 Northfields Avernue  
 NSW 2522, Australia  
 [txia, j.seberry]@uow.edu.au

Mingyuan Xia  
 Central China Normal University  
 School of Mathematics & Statistics  
 Wuhan, Hubei 430079  
 China  
 xiamy@mail.ccnu.edu.cn

*Abstract:* For every prime power  $q \equiv 7 \pmod{16}$ , we obtain the  $(q; a, b, c, d)$ -partitions of  $GF(q)$ , with odd integers  $a, b, c, d$ ,  $a \equiv \pm 1 \pmod{8}$  such that  $q = a^2 + 2(b^2 + c^2 + d^2)$  and  $d^2 = b^2 + 2ac + 2bd$ . Hence for each value of  $q$  the construction of SDS becomes equivalent to building a  $(q; a, b, c, d)$ -partition. The latter is much easier than the former. We give a new construction for an infinite family of regular Hadamard matrices of order  $4q^2$  by 16th power cyclotomic classes.

*Key-Words:* Regular Hadamard matrix, cyclotomic class, Supplement difference sets (SDS)

## 1 Introduction

An Hadamard matrix  $H$  of order  $v$  is a  $v \times v$  matrix with entries  $\pm 1$ , such that  $HH^T = vI$  where  $I$  is the identity matrix. An Hadamard matrix is called regular if all its rows contain the same number of entries 1. It is well known that if a regular Hadamard matrix of order  $v$  exists,  $v$  must be a complete square.

Williamson type Hadamard matrices of order  $4q^2$  with  $q \equiv 1 \pmod{4}$  prime power were firstly constructed in [6], then a family of regular Hadamard matrices of order  $4q^2$  for  $q \equiv 3 \pmod{8}$  prime power was obtained in [7]. In 1998, Q. Xiang [12] gave a nice simple construction for these cases. Then the authors in [8] and [9] obtained more general constructions by using special partitions of  $GF(q)$ . The only open case for the construction of regular Hadamard matrices of order  $4q^2$  with  $q$  prime power is that for  $q \equiv 7 \pmod{8}$ . [3] and [11] separately obtained many new results for regular Hadamard matrices of order  $4q^2$  for  $q \equiv 7 \pmod{16}$ . The mathematical idea of [3] is profound and has greatly inspired us to do this research.

Let  $G$  be an Abelian group of order  $v$ . We denote the group operation by multiplication. Subsets  $D_1, \dots, D_r$  of  $G$  are called  $r - \{v; |D_1|, \dots, |D_r|; \lambda\}$  supplementary difference sets (SDS) if

for every nonidentity element  $g$  in  $G$ , there are exactly  $\lambda$  elements  $(d, d')$  in  $D_1 \times D_1$ , or  $D_2 \times D_2, \dots$ , 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.  $a_1g_1 + \dots + a_vg_v$ ,  $a_i \in Z$ ,  $g_i \in G$ ,  $i = 1, \dots, v$ .  $(\sum_g a(g)g) + (\sum_g b(g)g) = \sum_g (a(g) + b(g))g$ .  $(\sum_g a(g)g)(\sum_h b(h)h) = \sum_k (\sum_{gh=k} a(g)b(h))k$ .

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  $A, B \subset G$ . We define  $AB^{(-1)} = \sum_{a \in A, b \in B} ab^{-1} \in Z[G]$  and denote  $\Delta A = AA^{(-1)}$ ,  $\Delta(A, B) = AB^{(-1)} + BA^{(-1)}$ .

With this convention  $D_1, D_2, \dots, D_r$  being  $r - \{v; |D_1|, \dots, |D_r|; \lambda\}$  SDS are equivalent to  $\sum_{i=1}^r \Delta D_i = (\sum_{i=1}^r |D_i| - \lambda) + \lambda G$ .

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

In this paper we assume  $p$  is an odd prime,  $r > 0$ , and

$$q = p^r = 16m + 7 = a^2 + 2(b^2 + c^2 + d^2) \quad (1)$$

with  $a, b, c$  and  $d$  odd integers and  $a \equiv \pm 1 \pmod{8}$ .

The paper is organized as follows. In Section 2 we represent  $q$  as the sum of  $|f_i(\zeta)|^2$ , where  $f_i(\zeta) = a_{i_0} + a_{i_1}\zeta + a_{i_2}\zeta^2 + \dots + a_{i_{2m}}\zeta^{2m}$ ,  $i = 0, \dots, 7$ , are polynomials of  $(2m + 1)$ -th root of unity  $\zeta$  including  $\zeta = 1$ , such that  $Ref_0(\zeta) = 0$ ,

\*The research supported by the ARC (No. LX0560185) was done during a visit of the third author at the University of Wollongong.

$f_1(\zeta)$  real,  $|f_i(\zeta)|^2 = |f_{9-i}(\zeta)|^2$ ,  $i = 2, 3, 4$ . In Section 3 we partition the group  $GF(q)$  into 16 subsets with certain desirable properties, i.e., we get a  $(q; a, b, c, d)$ -partition of  $GF(q)$  which is a powerful instrument for constructing SDS. Finally, for  $q < 1000$ , we list the values of  $a, b, c$  and  $d$  obtained in the  $(q; a, b, c, d)$ -partitions as an appendix.

Before we process 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 nonsquares of  $GF(q)$ ;
- $\delta$ : a primitive element of  $GF(q)^*$ ;
- $E_i$ :  $2(q+1)$ th power cyclotomic class;
- $C_j$ :  $16$ th power cyclotomic class;

Recall that the absolute trace  $Tr_{q^n}$  of an element  $g \in GF(q^n)$  is defined as  $Tr_{q^n}(g) = \sum_{j=0}^{n-1} g^{p^j} \in GF(p)$ .

For the detailed discussion of absolute and relative trace maps of finite fields we refer the reader to the textbooks such as [1], [2] and [4]. The characters of the group  $GF(q^n)$  are given by the following (see [5]). Let  $\xi$  be a fixed primitive  $p$ th root of unity,  $\alpha, \beta \in GF(q^n)$ , define a group homomorphism  $\chi_\alpha : GF(q^n) \rightarrow C^*$ ,  $\chi_\alpha(\beta) = \xi^{Tr_{q^n}(\alpha\beta)}$ , 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 A representation of $q$ by special polynomials

Let  $r$  be a non-square element of  $GF(q)$ . Then the polynomial  $P(\omega) = \omega^2 - r$  is irreducible in  $GF(q)$ , and the polynomials  $a\omega + b \pmod{P(\omega)}$ ,  $a, b \in GF(q)$ , form a finite field  $GF(q^2)$ . In what follows we will employ this concrete representation of  $GF(q^2)$ . If  $g$  is a generator of the cyclic group of nonzero elements of  $GF(q^2)$ , then  $g^{q+1} = \delta$  is a generator of the cyclic group of nonzero elements of  $GF(q)$ . For arbitrary  $h \in GF(q^2)$  define

$$tr(h) = h + h^q \quad (2)$$

(indeed,  $tr(h) = Tr_{q^2/q}(h)$ ), so that  $tr(h) \in GF(q)$ . It follows from this definition that

$$tr(g^k) = g^{(q+1)k} tr(g^{-k}) \quad (3)$$

for an arbitrary integer  $k$ .

Suppose  $q \equiv 7 \pmod{8}$ . For  $h \in GF(q^2)$ ,  $h \neq 0$ , let  $ind(h)$  be the least non-negative integer  $t$  such that  $g^t = h$ . Let  $\beta$  denote a primitive 16th root of unity. Then

$$\rho(h) = \begin{cases} \beta^{ind(h)}, & h \neq 0, \\ 0, & h = 0, \end{cases} \quad (4)$$

defines an 16th power character  $\rho$  of  $GF(q^2)$ . For  $a \in GF(q)$ ,  $a \neq 0$ , put  $\delta^j = a$ . By (4) we have  $\rho(a) = \beta^{(q+1)j}$ . Consequently  $\rho(a) = (-1)^j$  if  $q \equiv 7 \pmod{16}$  and  $\rho(a) = 1$  if  $q \equiv 15 \pmod{16}$ . In the case  $q \equiv 7 \pmod{16}$ ,  $\rho(a)$  reduces to the Legendre symbol in  $GF(q)$  defined by  $\rho(a) = 1, -1$  or  $0$  according to  $a$  is a nonzero square, a non-square or  $0$  in  $GF(q)$ . In the following we will assume that  $q \equiv 7 \pmod{16}$  and take  $r = -1$  (since  $-1$  is a non-square element in  $GF(q)$ ). Accordingly we obtain from (3) that

$$\rho(tr(g^k))\rho(tr(g^{-1})) = (-1)^k, \quad tr(g^k) \neq 0. \quad (5)$$

For a fixed  $\eta \in GF(q^2)$  put  $\eta = c\omega + d$ ,  $c, d \in GF(q)$ . Then  $\eta \in GF(q)$  if  $c = 0$  and  $\eta \notin GF(q)$  if  $c \neq 0$ . We require the formula

$$\sum_{\xi} \rho(tr(\xi))\rho(tr(\eta\xi)) = \begin{cases} \rho(d)q(q-1), & c = 0, \\ 0, & c \neq 0, \end{cases} \quad (6)$$

where the summation is over all  $\xi \in GF(q^2)$ . Put  $\xi = a\omega + b$ ,  $a, b \in GF(q)$ . By (2) we have  $tr(\xi) = 2b$  and  $tr(\eta\xi) = 2(bd - ac)$ . Therefore  $\sum_{\xi} \rho(tr(\xi))\rho(tr(\eta\xi)) = \sum_b \rho(2b) \sum_a \rho(2(bd - ac))$ , and (6) follows at once.

For  $\eta \neq 0$  we may put  $\eta = g^t$  ( $0 \leq t \leq q^2 - 2$ ), so that  $c = 0$  if  $q+1|t$  and  $c \neq 0$  if  $q+1 \nmid t$ . If  $c = 0$ , put  $t = j(q+1)$  and then  $\rho(d) = (-1)^j$ . The sum in (6) now becomes  $\sum_{k=0}^{q^2-2} \rho(tr(g^k))\rho(tr(g^{k+t})) = \sum_{h=0}^{q-2} \sum_{k=h(q+q)}^{h(q+1)+q} \rho(tr(g^k))\rho(tr(g^{k+t}))$ . The double sum on the right has the value  $0$  if  $q+1 \nmid t$ . Since  $\rho(tr(g^{k+q+1})) = -\rho(tr(g^k))$ , the value of the inner sum is the same for each  $h$ . For  $h = 0$  we get, in particular,

$$\sum_{k=0}^q \rho(tr(g^k))\rho(tr(g^{k+t})) = \begin{cases} (-1)^j q, & q+1|t, \\ 0, & q+1 \nmid t, \end{cases} \quad (7)$$

where, in the first case,  $t = j(q+1)$ .

**Theorem 1** Suppose  $q$  is a prime power  $\equiv 7 \pmod{16}$  and  $n = (q + 1)/8$ . Let  $g$  be a primitive element of  $GF(q^2)$ . Put

$$g^k = \alpha_k \omega + \beta_k, \quad \alpha_k, \beta_k \in GF(q), \quad (8)$$

and define

$$a_k = \rho(\alpha_k), \quad b_k = \rho(\beta_k). \quad (9)$$

Then the sums

$$\begin{aligned} f_{2i}(\zeta) &= \sum_{j=0}^{n-1} a_{i+16j} \zeta^j, \\ f_{2i+1}(\zeta) &= \sum_{j=0}^{n-1} b_{i+16j} \zeta^j, \end{aligned} \quad i = 0, 1, 2, 3 \quad (10)$$

satisfy the identity

$$\sum_{i=0}^7 |f_i(\zeta)|^2 = q \quad (11)$$

for each  $n$ th root of unity  $\zeta$  including  $\zeta = 1$ . Moreover, the following relations hold:

$$\begin{aligned} a_0 &= 0, \quad a_{16i} = -a_{16(n-i)}, \\ b_0 &= 1, \quad b_{16i} = b_{16(n-i)}, \end{aligned} \quad 1 \leq i < n. \quad (12)$$

**Proof.** Since  $g$  is a primitive element of  $GF(q^2)$  the integer  $k = (q + 1)/2 = 4n$  is the only value of  $k$  in the interval  $0 \leq k \leq q$  for which  $\text{tr}(g^k) = 0$ . Put  $g^{4n} = \lambda \omega$ ,  $\lambda \in GF(q)$ . The numbers  $a_k, b_k$  in (9) satisfy the relations

$$b_{k+4n} = -\rho(\lambda) a_k, \quad (13)$$

$$b_{k+8n} = -b_k, \quad (14)$$

$$b_{k+16n} = b_k. \quad (15)$$

Moreover, from (8) it follows that  $-\alpha_{16i} \omega + \beta_{16i} = (g^{16i})^q = g^{16n(8i-1)+16(n-i)} = \delta^{2(8i-1)} (\alpha_{16(n-i)} \omega + \beta_{16(n-i)})$ ,  $0 \leq i \leq n$ .

Hence  $\alpha_{16i} = -\delta^{2(8i-1)} \alpha_{16(n-i)}$ ,  $\beta_{16i} = \delta^{2(8i-1)} \beta_{16(n-i)}$ ,  $0 \leq i \leq n$ .

Consequently, (12) is valid.

Note that the periodicity property (15) implies

$$\sum_{i=0}^{n-1} b_{16i+t} = \sum_{i=0}^{n-1} b_{16i+s}, \quad t \equiv s \pmod{16}. \quad (16)$$

If we replace  $b$ 's by  $a$ 's, then (15) and (16) would also be true.

Denote the sum in (7) by  $F(t)$ . The assumption  $q \equiv 7 \pmod{16}$  implies that  $t = 0$  is the only

value of  $t$  in the interval  $0 \leq t < n$  for which  $16t$  is divisible by  $q + 1$ . Thus it follows from (7) that

$$F(16t) = \sum_{k=0}^q b_k b_{k+16t} = \begin{cases} q, & t = 0, \\ 0, & 1 \leq t < n. \end{cases} \quad (17)$$

On the other hand from (13), (14) and (17) we have  $F(16t) = \sum_{k=0}^3 \sum_{i=0}^{n-1} (a_{16i+k} a_{16i+k+16t} + b_{16i+k} b_{16i+k+16t})$ . Applying the finite Parseval relation:  $\sum_{i=0}^{n-1} c_i \bar{c}_{i+t} = \frac{1}{n} \sum_{j=0}^{n-1} |\varphi(\zeta^j)|^2 \zeta^{jt}$ ,  $0 \leq t < n$ , where  $\bar{c}_{i+t}$  is the conjugate of  $c_{i+t}$  and  $\varphi(\zeta) = \sum_{i=0}^{n-1} c_i \zeta^i$ , we now obtain

$$\begin{aligned} & \sum_{k=0}^3 \sum_{i=0}^{n-1} (a_{16i+k} a_{16i+k+16t} + b_{16i+k} b_{16i+k+16t}) \\ &= \frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^7 |f_k(\zeta^j)|^2 \zeta^{jt}. \end{aligned} \quad (18)$$

Combining (17) and (18) we get

$$F(16t) = \frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^7 |f_k(\zeta^j)|^2 \zeta^{jt}. \quad (19)$$

The inverted form of (19) is given by  $\sum_{k=0}^7 |f_k(\zeta^j)|^2 = \sum_{t=0}^{n-1} F(16t) \zeta^{-jt}$ ,  $j = 0, 1, \dots, n-1$ . By (17) we have  $F(0) = q$  and  $F(16t) = 0$  for  $1 \leq t < n$ , hence the last sum reduces to  $q$ . This completes the proof of the theorem.  $\square$

From (12) we know that  $R_e f_0(\zeta) = 0$  and  $f_1(\zeta)$  is real.

**Lemma 1** Under the assumption as in Theorem 1

$$|f_i(\zeta)|^2 = |f_{9-i}(\zeta)|^2, \quad i = 2, 3, 4, \quad (20)$$

for each  $n$ th root of unity  $\zeta$  including  $\zeta = 1$ .

**Proof.** Since  $|f_2(\zeta)|^2 = \sum_{t=0}^{n-1} (\sum_{i=0}^{n-1} a_{16i+1} a_{16i+1+16t}) \zeta^{-t}$ ,  $|f_7(\zeta)|^2 = \sum_{t=0}^{n-1} (\sum_{i=0}^{n-1} b_{16i+3} b_{16i+3+16t}) \zeta^{-t}$ . For the proof of  $|f_2(\zeta)|^2 = |f_7(\zeta)|^2$ , it is sufficient to show that

$$\sum_{i=0}^{n-1} a_{16i+1} a_{16(i+t)+1} = \sum_{i=0}^{n-1} b_{16i+3} b_{16(i+t)+3}, \quad (21)$$

$0 \leq t < n$ . Let  $g^{16i+k} = \alpha_{16i+k} \omega + \beta_{16i+k}$ , where  $g$  is a generator of  $GF(q^2)$ . Then

$$-\alpha_{16i+k} \omega + \beta_{16i+k} = \alpha_{16qi+qk} \omega + \beta_{16qi+qk}. \quad (22)$$

By (22) it follows that

$$\sum_{i=0}^{n-1} a_{16i+1} a_{16(i+t)+1} = \sum_{i=0}^{n-1} a_{16i+8n-1} a_{16(i+t)+8n-1}. \quad (23)$$

If  $n \equiv 1 \pmod{4}$ , the last sum of (23) becomes  $\sum_{i=0}^{n-1} a_{16i-1} a_{16(i+t)-1} = \sum_{i=0}^{n-1} b_{16i+3} b_{16(i+t)+3}$  as required. If  $n \equiv 3 \pmod{4}$ , the last sum of (23) is equal to  $\sum_{i=0}^{n-1} a_{16i+7} a_{16(i+t)+7} = \sum_{i=0}^{n-1} b_{16i+3} b_{16(i+t)+3}$ , again as required. Similarly, we can prove that  $\sum_{i=0}^{n-1} b_{16i+1} b_{16(i+t)+1} = \sum_{i=0}^{n-1} a_{16i+3} a_{16(i+t)+3}$ ,  $\sum_{i=0}^{n-1} a_{16i+2} a_{16(i+t)+2} = \sum_{i=0}^{n-1} b_{16i+2} b_{16(i+t)+2}$ ,  $0 \leq t < n$ . The lemma is proved.  $\square$

**Corollary 1** *Suppose  $q$  is a prime power  $\equiv 7 \pmod{16}$ . Then*

(i) *there are 5 polynomials  $f_0(\zeta)$ ,  $f_1(\zeta)$ ,  $f_2(\zeta)$ ,  $f_3(\zeta)$ ,  $f_4(\zeta)$  of  $\zeta$ , defined as in (8)-(10), satisfying the identity*

$$\begin{aligned} & |f_0(\zeta)|^2 + |f_1(\zeta)|^2 + 2(|f_2(\zeta)|^2 + \\ & |f_3(\zeta)|^2 + |f_4(\zeta)|^2) = q \end{aligned} \quad (24)$$

*for each  $n$ th root of unity  $\zeta$  including  $\zeta = 1$ . Moreover,  $\operatorname{Re} f_0(\zeta) = 0$  and  $f_1(\zeta)$  is real.*

(ii) *there are 4 odd integers  $a, b, c$  and  $d$  with  $a \equiv \pm 1 \pmod{8}$  such that*

$$a^2 + 2(b^2 + c^2 + d^2) = q. \quad (25)$$

**Proof.** By Theorem 1 and Lemma 1 (i) is trivial. Since  $f_0(1) = 0$  and  $n$  is odd, we know that  $a = f_1(1)$ ,  $b = f_2(1)$ ,  $c = f_3(1)$ ,  $d = f_4(1)$  are all odd and (25) holds. Because  $q \equiv 7 \pmod{16}$ , so that  $a \equiv \pm 1 \pmod{8}$ . This completes the proof of (ii).  $\square$

### 3 A partition of $GF(q)$

Let  $g$  be a generator of  $GF(q^2)$ . Put  $E_i = \{g^{2(q+1)j+i} : j = 0, \dots, \frac{(q-3)}{2}\}$ ,  $i = 0, \dots, 2q+1$ . It is easy to see that  $E_0 = \{\delta^{2k} : k = 0, \dots, \frac{(q-3)}{2}\} = S$ ,  $E_{q+1} = \{\delta^{2k+1} : k = 0, \dots, \frac{(q-3)}{2}\} = N$ .

For any  $i$ ,  $1 \leq i < 2(q+1)$ ,  $i \neq q+1$ , write  $g^i = \alpha\omega + \beta$ ,  $\alpha, \beta \in GF(q)$ , then  $\alpha \neq 0$  and  $E_i =$

$g^i E_0 \hat{=} \{(\alpha\delta^{2k}, \alpha^{-1}\beta(\alpha\delta^{2k})) : k = 0, \dots, \frac{(q-3)}{2}\}$ . So we can represent  $E_i$  by  $\{(\eta, r\eta) : \eta \in S\}$  or  $\{(\eta, r\eta) : \eta \in N\}$  according to  $\alpha \in S$  or  $\alpha \in N$ . For convenience, we denote  $E_0 = (0, S)$ ,  $E_{q+1} = (0, N)$  and  $\{(\eta, r\eta) : \eta \in S\} = (S, rS)$ ,  $\{(\eta, r\eta) : \eta \in N\} = (N, rN)$ . The partition given in the following theorem is useful for constructing SDS.

**Theorem 2** *Suppose  $q \equiv 7 \pmod{16}$  is a prime power. There are 16 subsets  $X_1, \dots, X_{16}$  of  $GF(q)$  such that*

$$|X_1| = |X_2| = \frac{(q-7)}{16}, \quad (26)$$

$$\begin{aligned} & \{|X_3| = |X_{16}|, |X_4| = |X_{15}|\} \\ & = \left\{ \frac{(q-7)}{16} + \frac{(1+b)}{2}, \frac{(q-7)}{16} + \frac{(1-b)}{2} \right\}, \end{aligned} \quad (27)$$

$$\begin{aligned} & \{|X_5| = |X_{13}|, |X_6| = |X_{14}|\} \\ & = \left\{ \frac{(q-7)}{16} + \frac{(1+c)}{2}, \frac{(q-7)}{16} + \frac{(1-c)}{2} \right\}, \end{aligned} \quad (28)$$

$$\begin{aligned} & \{|X_7| = |X_{12}|, |X_8| = |X_{11}|\} \\ & = \left\{ \frac{(q-7)}{16} + \frac{(1+d)}{2}, \frac{(q-7)}{16} + \frac{(1-d)}{2} \right\}, \end{aligned} \quad (29)$$

$$\{|X_9|, |X_{10}|\} = \left\{ \frac{(q-7)}{16} + \frac{(1+a)}{2}, \frac{(q-7)}{16} + \frac{(1-a)}{2} \right\}, \quad (30)$$

$$X_1 + \dots + X_{16} = GF(q), \quad (31)$$

$$V = MU \quad (32)$$

*for some odd integers  $a, b, c$  and  $d$  with  $a \equiv \pm 1 \pmod{8}$  satisfying (1), where  $V = (X_1N + X_2S, X_1S + X_2N, \dots, X_{15}N + X_{16}S, X_{15}S + X_{16}N)^T$ ,  $U = (X_1, \dots, X_{16})^T$  and  $M =$*

$$\begin{pmatrix} e_1^* & e_2^* & e_3^* & e_4^* & e_5^* & \dots & e_{12}^* & e_{13}^* & e_{14}^* & e_{15}^* & e_{16}^* \\ e_2 & e_1 & e_4 & e_3 & e_6 & \dots & e_{11} & e_{14} & e_{13} & e_{16} & e_{15} \\ e_{15} & e_{16} & e_2 & e_1 & e_4 & \dots & e_{10} & e_{12} & e_{11} & e_{14} & e_{13} \\ e_{16} & e_{15} & e_1 & e_2 & e_3 & \dots & e_{10} & e_{11} & e_{12} & e_{13} & e_{14} \\ e_{14} & e_{13} & e_{16} & e_{15} & e_1 & \dots & e_8 & e_9 & e_{10} & e_{11} & e_{12} \\ e_{13} & e_{14} & e_{15} & e_{16} & e_2 & \dots & e_7 & e_{10} & e_9 & e_{12} & e_{11} \\ e_{11} & e_{12} & e_{13} & e_{14} & e_{15} & \dots & e_5 & e_8 & e_7 & e_{10} & e_9 \\ e_{12} & e_{11} & e_{14} & e_{13} & e_{16} & \dots & e_6 & e_7 & e_8 & e_9 & e_{10} \\ e_{10} & e_9 & e_{12} & e_{11} & e_{14} & \dots & e_4 & e_5 & e_6 & e_7 & e_8 \\ e_9 & e_{10} & e_{11} & e_{12} & e_{13} & \dots & e_3 & e_6 & e_5 & e_8 & e_7 \\ e_7 & e_8 & e_9 & e_{10} & e_{11} & \dots & e_1 & e_4 & e_3 & e_6 & e_5 \\ e_8 & e_7 & e_{10} & e_9 & e_{12} & \dots & e_2 & e_3 & e_4 & e_5 & e_6 \\ e_6 & e_5 & e_8 & e_7 & e_{10} & \dots & e_{15} & e_1 & e_2 & e_3 & e_4 \\ e_5 & e_6 & e_7 & e_8 & e_9 & \dots & e_{16} & e_2 & e_1 & e_4 & e_3 \\ e_3 & e_4 & e_5 & e_6 & e_7 & \dots & e_{14} & e_{15} & e_{16} & e_2 & e_1 \\ e_4 & e_3 & e_6 & e_5 & e_8 & \dots & e_{13} & e_{16} & e_{15} & e_1 & e_2 \end{pmatrix}$$

*where  $e_i$  denotes  $|X_i|$  and  $e_i^*$  denotes  $|X_i| - 1$ ,  $i = 1, \dots, 16$ .*

**Proof.** Put  $C_i = \{g^{16j+i} : j = 0, \dots, \frac{(q^2-1)}{16} - 1\}$ ,  $i = 0, \dots, 15$ , where  $g$  is a generator of  $GF(q^2)$ . It is clear that  $C_i = \bigcup_{j=0}^{2m} E_{16j+i}$ ,  $i = 0, \dots, 15$ . Particularly,  $C_0$  and  $C_8 = g^{q+1}C_0$  can be written in the forms

$$\begin{aligned} C_0 &= (0, S) \cup \{(S, rS), r \in X_1\} \cup \{(N, rN), r \in X_2\}, \\ C_8 &= (0, N) \cup \{(N, rN), r \in X_1\} \cup \{(S, rS), r \in X_2\} \end{aligned} \quad (33)$$

for some  $X_1, X_2 \subset GF(q)$ . Obviously,

$$|X_1| + |X_2| = 2m = \frac{(q-7)}{8}. \quad (34)$$

For any  $i$ ,  $1 \leq i \leq 2m$ , write  $g^{16i} = \alpha\omega + \beta \in E_{16i}$ ,  $\alpha, \beta \in GF(q)$ . Then  $\alpha \neq 0$ . For  $k = 0$ , from (22) we know that  $-\alpha\omega + \beta = g^{16iq} \in E_{16(2m+1-i)}$ . Hence  $\alpha(-\alpha) \in N$  and  $\alpha^{-1}\beta + (-\alpha)^{-1}\beta = 0$ . Therefore  $r = \alpha^{-1}\beta \in X_i$  if and only if  $-r \in X_{3-i}$ ,  $i = 1, 2$ . These facts, together with (34), show that  $|X_1| = |X_2| = \frac{(q-7)}{16}$  and  $0 \in X_1 \cup X_2$ . Now set  $E = \{-r^{-1} : r \in (X_1 \cap N) \cup (X_2 \cap S)\}$ ,  $F = \{0\} \cup \{-r^{-1} : r \in (X_1 \cap S) \cup (X_2 \cap N)\}$  and take  $\{X_9, X_{10}\} = \{E, F\}$ . Since  $\{C_4, C_{12}\} = \{g^{\frac{(q+1)}{2}}C_0, g^{\frac{3(q+1)}{2}}C_0\}$  and  $\{E_{\frac{(q+1)}{2}}, E_{\frac{3(q+1)}{2}}\} = \{(S, 0), (N, 0)\}$ , so  $\{C_4, C_{12}\} = \{\bigcup_{r \in X_9} (S, rS) \cup \bigcup_{r \in X_{10}} (N, rN), \bigcup_{r \in X_9} (N, rN) \cup \bigcup_{r \in X_{10}} (S, rS)\}$ . Without loss of generality, we can write

$$\begin{aligned} C_4 &= \{(S, rS), r \in X_9\} \cup \{(N, rN), r \in X_{10}\}, \\ C_{12} &= \{(N, rN), r \in X_9\} \cup \{(S, rS), r \in X_{10}\}, \end{aligned} \quad (35)$$

Clearly,  $|X_9| + |X_{10}| = 2m + 1 = \frac{(q+1)}{8}$ . Similarly to (35) we can write

$$\begin{aligned} C_i &= \{(S, rS), r \in X_{2i+1}\} \cup \{(N, rN), r \in X_{2i+2}\}, \\ C_{i+8} &= \{(N, rN), r \in X_{2i+1}\} \cup \{(S, rS), r \in X_{2i+2}\}, \end{aligned} \quad (36)$$

$i = 1, \dots, 7$ , for some  $X_3, \dots, X_{16} \subset GF(q)$ . Obviously,

$$|X_{2i+1}| + |X_{2i+2}| = \frac{(q+1)}{8}, \quad i = 1, \dots, 7. \quad (37)$$

Let  $h = g^{16j+i} = \alpha\omega + \beta$ ,  $\alpha, \beta \in GF(q)$ ,  $0 \leq j < \frac{(q^2-1)}{16}$ ,  $1 \leq i \leq 3$ . Then  $\alpha \neq 0$  and  $h \in C_i$ . Now  $h^q = -\alpha\omega + \beta$ . If  $i = 1$ , by (22) we know that  $h^q \in C_7$ . Since the transformation:  $h \rightarrow h^q$  is one to one on  $GF(q^2)$ , it follows that  $|X_3| = |X_{16}|$  and  $|X_4| = |X_{15}|$ . If  $i = 2$ , by (22) we have  $h^q \in C_{14}$ , hence  $|X_5| = |X_{13}|$  and  $|X_6| = |X_{14}|$ . If  $i = 3$ , then  $h^q \in C_5$ , therefore  $|X_7| = |X_{12}|$  and  $|X_8| = |X_{11}|$ .

From Theorem 1, Lemma 1 and Corollary 1 it follows that  $\sum_{i=1}^8 (|X_{2i-1}| - |X_{2i}|)^2 = 2 \sum_{i=2}^4 (|X_{2i-1}| - |X_{2i}|)^2 + (|X_9| - |X_{10}|)^2 = q$ . Write

$$\begin{aligned} |X_9| - |X_{10}| &= a, & |X_3| - |X_4| &= b, \\ |X_5| - |X_6| &= c, & |X_7| - |X_8| &= d. \end{aligned} \quad (38)$$

Then  $a, b, c$  and  $d$  are odd and  $a \equiv \pm 1 \pmod{8}$ . Thus (27)–(30) will follow from (37) and (38).

Since  $\{(S, rS), r \in \bigcup_{i=1}^8 X_{2i-1}\} \cup \{(N, rN), r \in \bigcup_{i=1}^8 X_{2i}\} = \bigcup_{i=1}^{2m} E_{16i} \cup (\bigcup_{i=1}^7 \bigcup_{j=0}^{2m} E_{16j+i})$ , it follows that  $|\bigcup_{i=1}^{16} X_i| = q$ , i.e.,  $X_1 + \dots + X_{16} = GF(q)$ .

Now we are going to prove (32).

For any  $h = \alpha\omega + \beta \neq 0$ ,  $\alpha, \beta \in GF(q)$ , it is clear that  $\{hC_0, \dots, hC_{15}\} = \{C_0, \dots, C_{15}\}$ .

Note that  $(\alpha, \beta)(\alpha', \beta') = (\alpha\omega + \beta)(\alpha'\omega + \beta') = (\alpha\beta' + \beta\alpha', \beta\beta' - \alpha\alpha')$ , we have

$$\begin{aligned} hC_0 &= (\alpha S, \beta S) \cup \{((\alpha r + \beta)S, (\beta r - \alpha)S), r \in X_1\} \\ &\quad \cup \{((\alpha r + \beta)N, (\beta r - \alpha)N), r \in X_2\}, \\ hC_8 &= (\alpha N, \beta N) \cup \{((\alpha r + \beta)N, (\beta r - \alpha)N), r \in X_1\} \\ &\quad \cup \{((\alpha r + \beta)S, (\beta r - \alpha)S), r \in X_2\}, \end{aligned} \quad (39)$$

For any  $r_0 \in X_1$ , we can choose  $\alpha, \beta \in GF(q)$  such that  $\alpha \in S$  and  $\alpha^{-1}\beta = -r_0 \in X_2$ . In (39) the term  $(\alpha S, \beta S) = (S, -r_0 S) \in C_8$ . It follows that  $hC_0 = C_8$  and  $hC_8 = C_0$ . Then in (39) the term  $((\alpha r_0 + \beta)S, (\beta r_0 - \alpha)S) = (0, -(1 + r_0^2)S)$  should be equal to  $(0, N)$ , i.e.,  $1 + r_0^2 \in S$  for any  $r_0 \in X_1 \cup X_2$ . Now

$$\begin{aligned} hC_0 &= (0, N) \cup (S, -r_0 S) \cup \{(S, -r^{-1}(1 + r_0^2 + r r_0)S), r \in R_1\} \\ &\quad \cup \{(N, -r^{-1}(1 + r_0^2 + r r_0)N), r \in R_2\} \end{aligned} \quad (40)$$

where  $R_1 = ((X_1 - r_0) \cap S) \cup ((X_2 - r_0) \cap N)$ ,  $R_2 = ((X_1 - r_0) \cap N) \cup ((X_2 - r_0) \cap S)$ .

Comparing expression (40) with the second expression of (33), it follows that

$$|R_1| = |X_2| - 1 = |X_1| - 1, \quad (41)$$

$$|R_2| = |X_1| = |X_2|. \quad (42)$$

(41) and (42) mean that the coefficients of  $r_0$  in  $X_1N + X_2S$  and  $X_1S + X_2N$  are  $|X_1| - 1$  and  $|X_2|$  respectively.

Similarly, for  $r_0 \in X_1$ , we can choose a suitable  $h_i$  such that  $h_i C_i = C_{i+8}$  and  $h_i C_{i+8} = C_i$ ,  $i = 1, \dots, 7$ .

Comparing the expression of  $h_i C_i$  with that of  $C_{i+8}$ ,  $i = 1, \dots, 7$ , it follows that the coefficients of  $r_0$  in  $X_3N + X_4S, X_3S + X_4N, \dots, X_{15}N + X_{16}S$  and  $X_{15}S + X_{16}N$  are  $|X_{15}|, |X_{16}|, \dots, |X_3|, |X_4|$  respectively.

Repeating the procedure for  $X_2, \dots, X_{16}$  analogously, one can get (32). The theorem is proved.  $\square$

We call the partition satisfying (26)–(32) a  $(q; a, b, c, d)$ -partition of  $GF(q)$ .

For any subset  $A \subset GF(q)$ ,  $\beta, r \in GF(q)$ , we write  $\beta A^p + r = \{\beta\alpha^p + r : \alpha \in A\}$  and as well as in  $Z[GF(q)]$ .

**Theorem 3** Suppose  $W = \{X_1, \dots, X_{16}\}$  is a  $(q; a, b, c, d)$ -partition of  $GF(q)$ ,  $\beta, r \in GF(q)$  and  $\beta \neq 0$ . If  $\bar{W} = \{\bar{X}_1, \dots, \bar{X}_{16}\}$  is obtained from  $W$  under the following transformations:

- (i)  $\bar{X}_i = X_i + r, i = 1, \dots, 16,$
- (ii)  $\bar{X}_i = X_i^p, i = 1, \dots, 16,$
- (iii)  $\bar{X}_i = \beta X_i, i = 1, \dots, 16$  for  $\beta \in S,$
- (iv)  $\bar{X}_i = \beta X_2, \bar{X}_2 = \beta X_1,$  and  $\bar{X}_i = \beta X_i,$   
 $i = 3, \dots, 16$  for  $\beta \in N,$

then  $\bar{W}$  is also a  $(q; a, b, c, d)$ -partition of  $GF(q)$ .

The proof of the Theorem 3 is trivial.

### Corollary 2

Let  $\{X_1, \dots, X_{16}\}$  be a  $(q; a, b, c, d)$ -partition of  $GF(q)$  and  $a_k, b_k$  be given in (8), (9) for a fixed generator  $g$  of  $GF(q^2)$ . Then

- (i)  $|X_{2i+1}| - |X_{2i+2}| = \sum_{j=0}^{n-1} a_{16j+i}, i = 1, 2, 3, 4;$
  - (ii)  $|X_9| - |X_{10}| = \varepsilon \sum_{j=0}^{n-1} b_{16j}$
- where  $\varepsilon = 1$  or  $-1$  according to  $0 \in X_9$  or  $0 \in X_{10}$ .

## Appendix A.

Table of parameters  $a, b, c, d$  in the  $(q; a, b, c, d)$ -partition of  $GF(q)$  for  $q < 1000$ .

q	g	a	b	c	d
7	2	-1	1	1	1
23	2	1	3	-1	-1
71	8	-7	1	-1	-3
103	2	-7	5	1	-1
151	9	-1	5	7	-1
167	2	-1	3	7	5
199	13	-1	3	9	3
263	2	9	-9	-1	3
311	4	7	-1	7	9
343	$\delta + 1$	7	11	1	-5
359	11	-9	3	-7	-9
439	9	7	-5	1	-13
487	3	-1	-5	-7	-13
503	6	-17	-9	-1	5
599	11	-23	3	-1	-5
631	5	1	5	-17	1
647	2	-9	-15	7	3
727	2	-25	-5	1	-5
743	2	17	-13	-7	-3
823	3	-7	-9	9	-15
839	4	17	-7	-1	-15
887	2	7	9	-7	17
919	6	17	15	-9	3
967	2	-17	-13	-7	11
983	2	-7	-3	-17	13

\*  $\delta$  is a generator of  $GF(343)$  and satisfies  $\delta^3 = \delta + 5$ . Regular Hadamard matrices of order  $4 \cdot 7^{2r}$  have been constructed by [10] for all  $r \geq 1$ .

## References

- [1] D. Jungnickel, *Finite Fields: Structure and Arithmetic*, BI-Wissenschaftsverlag, Mannheim, 1993.
- [2] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, Berlin, 1986.
- [3] Ka Hin Leung, Siu Lun Ma and Bernhard Schmidt, New Hadamard matrices of order  $4p^2$  obtained from Jacobi sums of order 16, *J. Combin. Theory, Ser. A*, (to appear).
- [4] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Uni. Press, Cambridge, 1994.
- [5] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, 1601 (1995), Springer-Verlag, New York, Berlin.
- [6] M. Xia and G. Liu, An infinite class of supplementary difference sets and Williamson matrices, *J. Comb. Theory, Ser. A*, 58 (1991), pp. 310-317.
- [7] M. Xia and G. Liu, A new family of supplementary difference sets and Hadamard matrices, *J. Statist, Planning and Inference*, 51 (1996), pp. 283-291.
- [8] M. Xia, T. Xia and J. Seberry, A new method for constructing Williamson Matrices, *Journal of Designs, Codes and Cryptography*, 35 (2005), pp. 191-209.
- [9] M. Xia, T. Xia, J. Seberry and G. Zuo, A new method for constructing T-matrices, *Australasian Journal of Combinatorics*, Vol. 32 (2005), pp. 61-78.
- [10] T. Xia, M. Xia and J. Seberry, Regular Hadamard Matrix, Maximum Excess and SBIBD, *Australasian Journal of Combinatorics*, 27 (2003), pp. 263-275.
- [11] T. Xia, M. Xia and J. Seberry, Some new results of regular Hadamard matrices and SBIBD, *Australasian Journal of Combinatorics* (to appear).
- [12] Q. Xiang, Difference families from line and half line, *Europ. J. Combin.*, 19 (1998), pp. 395-400.