1-1-2006

New Constructing of regular Hadamard matrices

Tianbing Xia
University of Wollongong, txia@uow.edu.au

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

M. Xia
Central China Normal University, China

Follow this and additional works at: https://ro.uow.edu.au/infopapers

Part of the Physical Sciences and Mathematics Commons

Recommended Citation

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au
New Constructing of regular Hadamard matrices

Abstract
For every prime power $q \equiv 7 \mod 16$, we obtain the $(q, a, b, c, d)$-partitions of $GF(q)$, with odd integers $a, b, c, d, a \equiv \pm 1 \mod 8$ 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.

Keywords
Regular Hadamard matrix, cyclotomic class, Supplement difference sets (SDS)

Disciplines
Physical Sciences and Mathematics

Publication Details
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 journal article is available at Research Online: https://ro.uow.edu.au/infopapers/597
New Constructing of regular Hadamard matrices

Tianbing Xia, Jennifer Seberry
University of Wollongong
CCSR, SITACS
Northfields Avenue
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 \( q \equiv 7 \mod 16 \), we obtain the \((q; a, b, c, d)\)-partitions of \( GF(q) \), with odd integers \( a, b, c, d \), \( a \equiv \pm 1 \mod 8 \) 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 \( q \equiv 1 \mod 4 \) prime power were firstly constructed in [6], then a family of regular Hadamard matrices of order \( 4q^2 \) for \( q \equiv 3 \mod 8 \) 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 \( q \equiv 7 \mod 8 \). [3] and [11] separately obtained many new results for regular Hadamard matrices of order \( 4q^2 \) for \( q \equiv 7 \mod 16 \). 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 \( D_1, \ldots, D_r \) of \( G \) are called \( r - \{ \{v_1 \mid \{D_1 \mid \ldots, D_r \mid \lambda\}\} \) supplementary difference sets (SDS) if for every nonidentity element \( g \) in \( G \), there are exactly \( \lambda \) elements \( \{d_i d \} \) in \( D_1 \times D_1 \), or \( D_2 \times D_2 \), \ldots, 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. \( a_1 g_1 + \cdots + a_v g_v, \ a_i \in Z, \ g_i \in G, \ i = 1, \ldots, v \).

\( (\sum a(g) g) + (\sum b(g) g) = \sum (a(g) + b(g)) g \).

\( (\sum a(g) g)(\sum b(h) h) = \sum K a(g) b(h) k \).

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 \( D_1, D_2, \ldots, D_r \) being \( r - \{ \{v_1 \mid \{D_1 \mid \ldots, D_r \mid \lambda\}\} \) SDS are equivalent to \( \sum_i -1 \Delta D_i = (\sum_i -1 | D_i | - \lambda) + \lambda G \).

If \( r = 1 \), the single SDS becomes a difference set (DS) in the usual sense. When \( | D_1 | = \cdots = | D_r | = k \), we denote \( r - \{ \{v_1 \mid \{D_1 \mid \ldots, D_r \mid \lambda\}\} \) by \( r - \{v_1 \mid k \lambda \} \).

In this paper we assume \( p \) is an odd prime, \( r > 0 \), and

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

with \( a, b, c \) and \( d \) odd integers and \( a \equiv \pm 1 \mod 8 \).

The paper is organized as follows. In Section 2 we represent \( q \) as the sum of \( | f_i(\xi) | ^2 \), where \( f_i(\xi) = a_i + b_i \xi + c_i \xi^2 + \cdots + a_i 2m \xi^2m \), \( i = 0, \ldots, 7 \), are polynomials of \( (2m + 1) \)-th root of unity \( \xi \) including \( \xi^2 = 1 \), such that \( Ref_0(\xi) = 0 \),
\( f_i(s) \) real, \( |f_i(s)|^2 = |f_{i+3}(s)|^2, i = 2, 3, 4. \) 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 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 nonsquares of \( GF(q) \);

\( \delta \): a primitive element of \( GF(q)^* \);

\( E_2 \): \( 2(q+1) \)th power cyclotomic class;

\( C_j \): \( j \)th power cyclotomic class;

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

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 \( q \)th root of unity, \( \alpha, \beta \in GF(q^n) \), define a group homomorphism \( \chi_\alpha : GF(q^n) \to C^* \), \( \chi_\alpha(\beta) = \xi^{Tr_{q^n}(\alpha \beta)} \), 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 \( a\omega + b \) mod \( P(\omega) \), \( a, b \in GF(q) \), 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

\[
tr(h) = h + h^\delta \tag{2}
\]

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

\[
tr(g^k) = g^{(q^2+1)k} tr(g^{-k}) \tag{3}
\]

for an arbitrary integer \( k \).

Suppose \( q \equiv 7 \mod 8 \). 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

\[
\rho(h) = \begin{cases} 
\beta^{ind(h)}, & h \neq 0, \\
0, & h = 0,
\end{cases} \tag{4}
\]

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 \( q \equiv 7 \mod 16 \) and \( \rho(a) = 1 \) if \( q \equiv 15 \mod 16 \). In the case \( q \equiv 7 \mod 16 \), \( \rho(a) \) 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 \( q \equiv 7 \mod 16 \) and take \( r = 1 \) (since \( -1 \) is a non-square element in \( GF(q) \)). Accordingly we obtain from (3) that

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

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

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

where the summation is over all \( \xi \in GF(q^2) \). Put \( \xi = \omega + b, a, b \in GF(q) \). 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 \( \eta = q^i (0 \leq i \leq q^2 - 2) \), so that \( c = 0 \) if \( q+1 \mid t \) 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 \( \sum_{k=0}^{q^2-2} \rho(tr(g^k))\rho(tr(g^{k+1})) = \sum_{h=0}^{q-2} \sum_{k=h+q}^{h+q+1} \rho(tr(g^k))\rho(tr(g^{k+1})) \). 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,

\[
\sum_{k=0}^{q} \rho(tr(g^k))\rho(tr(g^{k+1})) = \begin{cases} 
(-1)^j q, & q+1 \mid t, \\
0, & q+1 \nmid t,
\end{cases} \tag{7}
\]

where, in the first case, \( t = j(q+1) \).
Theorem 1 Suppose \( q \) is a prime power \( q \equiv 7 \mod 16 \) and \( n = (q + 1)/8 \). Let \( g \) be a primitive element of \( GF(q^2) \). Put
\[
g^k = \alpha_k \omega + \beta_k, \quad \alpha_k, \beta_k \in GF(q),
\]
and define
\[
a_k = \rho(\alpha_k), \quad b_k = \rho(\beta_k).
\]
Then the sums
\[
f_{2i}(\zeta) = \sum_{j=0}^{n-1} a_{i+j} \zeta^j, \quad f_{2i+1}(\zeta) = \sum_{j=0}^{n-1} b_{i+j} \zeta^j, \quad i = 0, 1, 2, 3
\]
satisfy the identity
\[
\sum_{i=0}^{7} |f_i(\zeta)|^2 = q
\]
for each \( n \)th root of unity \( \zeta \) including \( \zeta = 1 \). Moreover, the following relations hold:
\[
a_0 = 0, \quad a_{16i} = \overline{a_{16(n-i)}}, \quad 1 \leq i < n.
\]

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 \( tr(g^k) = 0 \). Put \( g^{4n} = \omega \lambda, \; \lambda \in GF(q) \). The numbers \( a_k, b_k \) in (9) satisfy the relations
\[
b_{k+4n} = -\rho(\lambda) a_k, \quad b_{k+8n} = -b_k, \quad b_{k+16n} = b_k.
\]
Moreover, from (8) it follows that \(-\alpha_{16i} \omega + \beta_{16i} = (g^{16i})^q = g^{16i(n+i)} = \delta^2(8i-1)(\alpha_{16(n-i)} \omega + \beta_{16(n-i)}), \; 0 \leq i \leq n\).

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

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 \( q \equiv 7 \mod 16 \) 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
\[
F(16t) = \sum_{k=0}^{q} b_k b_{k+16t} = \begin{cases} q, & t = 0, \\ 0, & 1 \leq t < n. \end{cases}
\]

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: \( \sum_{t=0}^{n-1} c_t \bar{c}_{t+i} = \frac{1}{n} \sum_{j=0}^{n-1} |\varphi(\zeta^j)|^2 \zeta^j, \; 0 \leq t < n \), where \( c_{t+i} \) is the conjugate of \( c_{t+i} \) and \( \varphi(\zeta) = \sum_{t=0}^{n-1} c_t \zeta^t \), we now obtain
\[
\sum_{k=0}^{3} \sum_{i=0}^{n-1} (a_{16i+k} a_{16i+k+16t} + b_{16i+k} b_{16i+k+16t})
= \frac{1}{n} \sum_{j=0}^{n-1} \sum_{k=0}^{7} |f_k(\zeta)^j|^2 \zeta^{jt}.
\]

Combining (17) and (18) we get
\[
F(16t) = \frac{1}{n} \sum_{j=0}^{7} \sum_{k=0}^{n-1} |f_k(\zeta)^j|^2 \zeta^{jt}.
\]

The inverted form of (19) is given by \( \sum_{k=0}^{n-1} |f_k(\zeta)^j|^2 = \sum_{j=0}^{n-1} F(16t) \zeta^{-jt}, \; j = 0, 1, \ldots, n-1 \).

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.

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

Lemma 1 Under the assumption as in Theorem 1
\[
|f_i(\zeta)|^2 = |f_{9-i}(\zeta)|^2, \quad i = 2, 3, 4
\]
for each \( n \)th root of unity \( \zeta \) including \( \zeta = 1 \).

Proof. Since \( |f_2(\zeta)|^2 = \sum_{i=0}^{n-1} (\sum_{i=0}^{n-1} a_{16i+1} a_{16i+1+16t}) \zeta^{-it}, \quad |f_4(\zeta)|^2 = \sum_{i=0}^{n-1} (\sum_{i=0}^{n-1} b_{16i+3} b_{16i+3+16t}) \zeta^{-it} \). For the proof of \( |f_2(\zeta)|^2 = |f_4(\zeta)|^2 \), it is sufficient to show that
\[
\sum_{i=0}^{n-1} a_{16i+1} a_{16(i+t)+1} = \sum_{i=0}^{n-1} b_{16i+3} b_{16(i+t)+3},
\]
\( 0 \leq t < n \). Let \( g^{16i+k} = \alpha_{16i+k} \omega + \beta_{16i+k}, \) where \( g \) is a generator of \( GF(q^2) \). Then
\[
-\alpha_{16i+k} \omega + \beta_{16i+k} = \alpha_{16q+k} \omega + \beta_{16q+k}.
\]
By (22) it follows that
\[ \sum_{i=0}^{n-1} a_{16i+1} a_{16(i+t)+1} = \sum_{i=0}^{n-1} a_{16i+8n-1} a_{16(i+t)+8n-1}. \] (23)

If \( n \equiv 1 \mod 4 \), 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 \( n \equiv 3 \mod 4 \), the last sum of (23) is equal to \( \sum_{i=0}^{n-1} b_{16i+7} a_{16(i+t)+7} = \sum_{i=0}^{n-1} b_{16i+3} b_{16(i+t)+3} \), 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 \( \equiv 7 \mod 16 \). 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
\[ |f_0(\zeta)|^2 + |f_1(\zeta)|^2 + 2(1 - a_2(\zeta)^2) = |f_2(\zeta)|^2 + |f_3(\zeta)|^2 + |f_4(\zeta)|^2 = q \] (24)
for each \( n \)th root of unity \( \zeta \) including \( \zeta = 1 \). Moreover, \( R_c f_0(\zeta) = 0 \) and \( f_1(\zeta) \) is real.

(ii) there are 4 odd integers \( a, b, c, d \) with \( a \equiv 0 \mod 8 \) such that
\[ a^2 + 2(b^2 + c^2 + d^2) = q. \] (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 \( q \equiv 7 \mod 16 \), so that \( a \equiv 1 \mod 8 \). This completes the proof of (ii). \( \square \)

3 A partition of \( GF(q) \)

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

For any \( i, 1 \leq i < 2q + 1, i \neq q + 1 \), write
\[ g^i = \alpha \omega + \beta, \alpha, \beta \in GF(q), \text{then } \alpha \neq 0 \text{ and } E_i = g^i E_0 = \{\alpha \delta^{2k}, \alpha^{-1} \beta (\alpha \delta^{2k}) : k = 0, \ldots, (q - 3)\}. \]
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 \( \{\eta, r \eta : \eta \in S = (S, r S), \{\eta, r \eta : \eta \in N \} = (N, r N) \). The partition given in the following theorem is useful for constructing SDS.

**Theorem 2** Suppose \( q \equiv 7 \mod 16 \) is a prime power. There are 16 subsets \( X_1, \ldots, X_{16} \) of \( GF(q) \) such that
\[ |X_1| = \frac{(q - 7)}{16}; |X_2| = \frac{(q^2 - 7)}{2}; |X_3| = \frac{(q^2 - 16)}{2}; \]
\[ |X_4| = \frac{(q - 7)}{2} + \frac{(q - 1)}{2}; |X_5| = \frac{(q - 16)}{2}; \]
\[ |X_6| = \frac{(q^2 - 7)}{2}; |X_7| = \frac{(q^2 - 16)}{2}; \]
\[ |X_8| = \frac{(q - 7)}{2} + \frac{(q - 1)}{2}; |X_9| = \frac{(q - 16)}{2}; \]
\[ |X_{10}| = \frac{(q^2 - 7)}{2}; |X_{11}| = \frac{(q^2 - 16)}{2}; \]
\[ |X_{12}| = \frac{(q - 7)}{2} + \frac{(q - 1)}{2}; |X_{13}| = \frac{(q - 16)}{2}; \]
\[ |X_{14}| = \frac{(q^2 - 7)}{2}; |X_{15}| = \frac{(q^2 - 16)}{2}; \]
\[ |X_{16}| = \frac{(q - 7)}{2} + \frac{(q - 1)}{2}; |X_{17}| = \frac{(q - 16)}{2}; \]
\[ V = MU \]
for some odd integers \( a, b, c, d \) with \( a \equiv 1 \mod 8 \) satisfying (1), where \( V = (X_{11} N + X_{2} S, X_{1} S + X_{2} N, \ldots, X_{15} N + X_{16} S, X_{15} S + X_{16} N)^T, U = (X_{1}, \ldots, X_{16})^T \) and \( M = (\begin{array}{ccccccccc}
\mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 & \mathbf{e}_4 & \mathbf{e}_5 & \mathbf{e}_6 & \mathbf{e}_7 & \mathbf{e}_8 & \mathbf{e}_9 & \mathbf{e}_{10} & \mathbf{e}_{11} & \mathbf{e}_{12} & \mathbf{e}_{13} & \mathbf{e}_{14} & \mathbf{e}_{15} & \mathbf{e}_{16}
\end{array})
\]
where \( \mathbf{e}_i \) denotes \( |X_i| \) and \( \mathbf{e}_i^* \) denotes \( |X_i| - 1, i = 1, \ldots, 16 \).

**Proof.** Put \( C_i = \{g^j : j = 0, \ldots, (q^2 - 1)/2 - 1 \}, i = 0, \ldots, 15 \), where \( g \) is a generator of \( GF(q^2) \). It is clear that \( C_i = \bigcup_{j=0}^{q-1} E_{j+i}, i = 0, \ldots, 15 \). Particularly, \( C_0 \) and \( C_8 \) can be written in the forms
\[ C_0 = (0, S) \cup \{(S, r S), r \in X_1 \} \cup \{(N, r N), r \in X_2 \}, \]
\[ C_8 = (0, N) \cup \{(N, r N), r \in X_1 \} \cup \{(S, r S), r \in X_2 \}, \]
for some \( X_1, X_2 \subset GF(q) \). Obviously,
\[ |X_1| + |X_2| = 2m = \frac{(q - 7)}{8}. \] (34)
For any $i$, $1 \leq i \leq 2m$, write $g^{16i} = \alpha + \beta \in E_{16i}$, $\alpha, \beta \in GF(q)$. Then $\alpha \neq 0$. For $k = 0$, from (22) we know that $\alpha - \beta = g^{16i} \in E_{16}$. Hence $\alpha(\alpha - \beta) = E_1$. $\alpha^2 - \beta^2 = 0$. Therefore $\alpha^2 = \beta^2$ in $X_i$ if and only if $r$ in $X_i$ only if $i = 1$.  

These facts, together with (34), show that $|X_1| = |X_2| = |X_3| = \frac{q^2 - 1}{8}$ and $0 \in X_1 \cup X_2$. Now set $E = \{ -r^{-1} : r \in (X_1 \cap N) \cup (X_2 \cap N) \}$, $F = \{ 0 \} \cup \{ -r^{-1} : r \in (X_1 \cap S) \cup (X_2 \cap N) \}$ and take $X_0 = (E,F)$. Since $C_4 = \{ g_{\frac{1}{2}(4i+1)}, g_{\frac{1}{2}(4i+1)} \}$ and $\{ E_{16i}, E_{16i} \} = \{ (S,0), (N,0) \}$, so $C_4 = \{ g_{\frac{1}{2}(4i+1)}, g_{\frac{1}{2}(4i+1)} \}$, Clearly, $|X_9| + |X_{10}| = 2m + 1 = \frac{q^2 - 1}{8}$. Similarly $\frac{1}{2}$ (35) we can write

\begin{equation}
C_9 = \{(S,r,S), r \in X_9 \} \cup \{(N,r,N), r \in X_10 \}, \quad C_{12} = \{(N,r,N), r \in X_9 \} \cup \{(S,r,S), r \in X_{10} \}.
\end{equation}

(35)

Now we are going to prove (32).

For any $h$, $\alpha + \beta \neq 0$, $\alpha, \beta \in GF(q)$, it is clear that \{ $h_{C_0} = \{ C_0 \}$ \} = \{ $C_0 \}$. \}

Note that $(\alpha, \beta')(\alpha', \beta') = (\alpha + \beta, (\alpha' + \beta') = (\alpha + \beta, 0) = (\alpha + \beta, 0)$, we have

\begin{align}
\alpha = (\alpha + \beta, \beta, \beta - \alpha) & = h_{C_0} \cup \{(\alpha + \beta, \beta, \beta - \alpha) \}, r \in X_1 \}
\end{align}

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

\begin{align}
\alpha = (0, N) \cup (S, -r_0 \in S) \cup \{(S, -r_1 + (1 + r_0 \in S), r \in R_1 \}
\end{align}

where $R_1 = ((X_1 - r_0) \cap N) \cup ((X_2 - r_0) \cap N)$, $R_2 = ((X_1 - r_0) \cap N) \cup ((X_2 - r_0) \cap N)$. Comparing expression (40) with the second expression of (33), it follows that

\begin{align}
| R_1 | = | X_2 | = 1 = | X_1 | = 1 - 1, \\
| R_2 | = | X_1 | = | X_2 |.
\end{align}

(41) and (42) mean that the coefficients of $r_0$ in $X_1^N + X_2^S$ and $X_1^S + X_2^N$ are $| X_1 | = 1$ and $| X_2 |$ respectively.

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

Comparing the expression of $h_{C_i}$ with that of $C_{i+8}$, $i = 1, \ldots, 7$, it follows that the coefficients of $r_0$ in $X_3^S + X_5^N + X_6^S + X_7 N$ and $X_7^S + X_8^N$ are $| X_4 | = 1$, $| X_5 | = \cdots$, $| X_3 |$ respectively.

Repeating the procedure for $X_2, \ldots, X_{10}$ analogously, one can get (32). The theorem is proved.

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 $\beta^P + r = \{ \beta^P + r : \alpha \in A \}$ and as well as in $Z[GF(q)]$.

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

\begin{itemize}
    \item\textbf{Step 1.} \textit{If} $r \neq 0, \text{then}$ $\overline{X}_i = X_{i+1}$, \textit{and} $\overline{X}_{i+1} = X_{i-1}$ for $i = 1, \ldots, 15$
    \item\textbf{Step 2.} \textit{If} $r = 0, \text{then}$ $\overline{X}_i = X_{i+1}$, \textit{and} $\overline{X}_{i+1} = X_{i-1}$ for $i = 1, \ldots, 15$
\end{itemize}
(i) \( X_i = X_i + r, \ i = 1, \cdots, 16, \)
(ii) \( X_i = X_i^p, \ i = 1, \cdots, 16, \)
(iii) \( X_i = \beta X_i, \ i = 1, \cdots, 16 \text{ for } \beta \in S, \)
(iv) \( X_i = \beta X_2, \ X_2 = \beta X_1, \text{ and } \beta X_i, \ i = 3, \cdots, 16 \text{ for } \beta \in N, \)
then \( \widetilde{W} \) is also a \( (q; a, b, c, d) \)-partition of \( GF(q). \)

The proof of the Theorem 3 is trivial.

**Corollary 2**

Let \( \{X_1, \cdots, X_{16}\} \) 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 \( y \) of \( GF(q^2). \) Then

(i) \( |X_{2i+1}| - |X_{2i+2}| = \sum_{j=0}^{q-1} a_{16j+i}, \ i = 1, 2, 3, 4; \)
(ii) \( |X_9| - |X_{10}| = \varepsilon \sum_{j=0}^{q-1} b_{16j} \)
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 \( q < 1000. \)

<table>
<thead>
<tr>
<th>q</th>
<th>g</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>2</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>71</td>
<td>8</td>
<td>-7</td>
<td>1</td>
<td>-1</td>
<td>-3</td>
</tr>
<tr>
<td>103</td>
<td>2</td>
<td>-7</td>
<td>5</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>151</td>
<td>9</td>
<td>-1</td>
<td>5</td>
<td>7</td>
<td>-1</td>
</tr>
<tr>
<td>167</td>
<td>2</td>
<td>-1</td>
<td>3</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>199</td>
<td>13</td>
<td>-1</td>
<td>3</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>263</td>
<td>2</td>
<td>9</td>
<td>-9</td>
<td>-1</td>
<td>3</td>
</tr>
<tr>
<td>311</td>
<td>4</td>
<td>7</td>
<td>-1</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>343</td>
<td>1</td>
<td>7</td>
<td>11</td>
<td>1</td>
<td>-5</td>
</tr>
<tr>
<td>359</td>
<td>11</td>
<td>-9</td>
<td>3</td>
<td>-7</td>
<td>-9</td>
</tr>
<tr>
<td>439</td>
<td>9</td>
<td>7</td>
<td>-5</td>
<td>1</td>
<td>-13</td>
</tr>
<tr>
<td>487</td>
<td>3</td>
<td>-1</td>
<td>-5</td>
<td>-7</td>
<td>-13</td>
</tr>
<tr>
<td>503</td>
<td>6</td>
<td>-17</td>
<td>-9</td>
<td>-1</td>
<td>5</td>
</tr>
<tr>
<td>599</td>
<td>11</td>
<td>-23</td>
<td>3</td>
<td>-1</td>
<td>-5</td>
</tr>
<tr>
<td>631</td>
<td>5</td>
<td>1</td>
<td>5</td>
<td>-17</td>
<td>1</td>
</tr>
<tr>
<td>647</td>
<td>2</td>
<td>-9</td>
<td>-15</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>727</td>
<td>2</td>
<td>-25</td>
<td>-5</td>
<td>1</td>
<td>-5</td>
</tr>
<tr>
<td>743</td>
<td>2</td>
<td>17</td>
<td>-13</td>
<td>-7</td>
<td>-3</td>
</tr>
<tr>
<td>823</td>
<td>3</td>
<td>-7</td>
<td>-9</td>
<td>9</td>
<td>-15</td>
</tr>
<tr>
<td>839</td>
<td>4</td>
<td>17</td>
<td>-7</td>
<td>-1</td>
<td>-15</td>
</tr>
<tr>
<td>887</td>
<td>2</td>
<td>7</td>
<td>9</td>
<td>-7</td>
<td>17</td>
</tr>
<tr>
<td>919</td>
<td>6</td>
<td>17</td>
<td>15</td>
<td>-9</td>
<td>3</td>
</tr>
<tr>
<td>967</td>
<td>2</td>
<td>-17</td>
<td>-13</td>
<td>-7</td>
<td>11</td>
</tr>
<tr>
<td>983</td>
<td>2</td>
<td>-7</td>
<td>-3</td>
<td>-17</td>
<td>13</td>
</tr>
</tbody>
</table>

* \( \delta \) 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**


