2013

Some new constructions of orthogonal designs

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

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

Mingyuan Xia
*Central China Normal University, xiamy@mail.ccnu.edu.cn*

Shangli Zhang
*Beijing Jiaotong University, shlzhang@center.njtu.edu.cn*

Publication Details

Some new constructions of orthogonal designs

Abstract
In this paper we construct OD(4pq^{r}(q+1); pq^{r}, pq^{r}, pq^{r+1}, pq^{r+1}, pq^{r+1}, pq^{r+1}) for each core order q \equiv 3(\text{mod} 4), r \geq 0 or q = 1, p odd, p \leq 21 and p \in \{25, 49\}, and COD(2q^{r}(q + 1); q^{r}, q^{r}, q^{r+1}, q^{r+1}) for any prime power q \equiv 1 (\text{mod} 4) (including q = 1), r \geq 0.

Keywords
era2015, constructions, designs, orthogonal

Disciplines
Engineering | Science and Technology Studies

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/eispapers/2258
Some new constructions of orthogonal designs

Tianbing Xia  Jennifer Seberry
School of CS and SE, Informatics
University of Wollongong
NSW 2522
Australia
txia@uow.edu.au  j.seberry@uow.edu.au

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

Shangli Zhang
School of Science
Beijing Jiaotong University
Beijing
China
shlzhang@center.njtu.edu.cn

Abstract

In this paper we construct OD(4pq^r(q+1); pq^r, pq^r, pq^r, pq^r+1, pq^r+1, pq^r+1, pq^r+1) for each core order \( q \equiv 3 \pmod{4}, r \geq 0 \) or \( q = 1, p \) odd, \( p \leq 21 \) and \( p \in \{25, 49\} \), and COD(2q^r(q+1); q^r, q^r, q^r+1, q^r+1) for any prime power \( q \equiv 1 \pmod{4} \) (including \( q = 1 \), \( r \geq 0 \).

1 Introduction

An orthogonal design (OD) \( X \) of order \( n \) and type \( (s_1, \ldots, s_m) \), \( s_i \) positive integers, is an \( n \times n \) matrix with entries \( \{0, \pm x_1, \ldots, \pm x_m\} \) (the \( x_i \) are commuting indeterminates) satisfying

\[
XX^T = \left( \sum_{i=1}^{m} s_ix_i^2 \right) I_n,
\]

where \( I_n \) is the identity matrix of order \( n \). This is denoted by OD(\( n; s_1, \ldots, s_m \)).
Such generically orthogonal matrices have played a significant role in the construction of Hadamard matrices (see, e.g., [3], [6]) and they have been extensively used in the study of weighing matrices (e.g. [3] and [8]).

Since Baumert and Hall [9] gave the first example of Baumert-Hall arrays, or $OD(4^t; t, t, t, t)$, and Plotkin [7] defined Plotkin arrays, or $OD(8^t; t, t, t, t, t, t, t, t)$, to construct Hadamard matrices, many research results have been published for $T$-matrices that are used in the construction of Plotkin arrays (see [3], [5], [9], [10]).

Turyn [11] introduced the notion of a complex Hadamard matrix, i.e., an $n \times n$ matrix $C$ whose entries are chosen from $\{\pm 1, \pm i\}$ and satisfy $CC^* = nI_n$ ($^*$ is conjugate transpose). He further showed how such matrices could be used to construct Hadamard matrices, and gave several examples. Further examples of such matrices are given in [3] and [4].

For a complex analogue of orthogonal designs there are several possible generalizations; we choose the one which gives real orthogonal designs as a special case.

A complex orthogonal design (COD) [4] of order $n$ and type $(s_1, \ldots, s_m)$ ($s_i$ positive integers) on the real commuting variables $x_1, \ldots, x_m$ is an $n \times n$ matrix $X$, with entries chosen from $\{\varepsilon_1 x_1, \ldots, \varepsilon_m x_m : \varepsilon_i \text{ a fourth root of } 1\}$ satisfying

$$XX^* = \left(\sum_{i=1}^m s_i x_i^2\right)I_n.$$

For further discussion we need the following definitions from [6].

**Definition 1 [Amicable Matrices; Amicable Set]** Two square real matrices of order $n$, $A$ and $B$, are said to be amicable if $AB^T - BA^T = 0$.

A set $\{A_1, \ldots, A_{2n}\}$ of square real matrices is said to be an amicable set if

$$\sum_{i=1}^{2n} (A_{2i-1}A_{2i}^T - A_{2i}A_{2i-1}^T) = 0.$$

It is easy to generalize an amicable set to the case of square complex matrices. For this, we just need to replace $A^T$ by $A^*$, the conjugate transpose of $A$.

**Definition 2 [T-matrices]** $(0, \pm 1)$ type 1 matrices $T_1, T_2, T_3$ and $T_4$ of order $n$ are called $T$-matrices if the following conditions are satisfied:

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

(b) $\sum_{i=1}^4 T_i T_i^T = nI_n$.

$T$-matrices can be used to construct orthogonal designs (see [1]).

The following definition was first used by Holzmann and Kharaghani in [5].

**Definition 3 [Weak amicable]** The $T$-matrices $T_1, T_2, T_3$ and $T_4$ are said to be weak amicable if

$$T_1(T_3 + T_4)^T + T_2(T_3 - T_4)^T = (T_3 + T_4)T_1^T + (T_3 - T_4)T_2^T.$$
**Definition 4 [Core]** Let $Q$ be a matrix of order $n$, with zero diagonal and all other elements $±1$ satisfying

$$QQ^T = nI_n - J_n, \ QJ_n = J_nQ = 0,$$

where $J_n$ is the matrix of order $n$, consisting entirely of 1’s. Further if $n \equiv 1 \pmod{4}$, $Q^T = Q$, and if $n \equiv 3 \pmod{4}$, then $Q^T = -Q$. Here $Q$ is called the **core** and $n$ is the **core order**.

If $H = I_n + K$ is an Hadamard matrix of order $n$ with $K^T = -K$, we call it skew type Hadamard matrix.

Here we rewrite the following theorem as

**Theorem 1** ([12]) *If there exists a skew type Hadamard matrix of order $q + 1$, then there exists a core of order $q$.***

It is well-known that if $q + 1 = 2^t n_1 \ldots n_s$, each $n_i$ of the form $p^r + 1 \equiv 0 \pmod{4}$, and $p$ is prime, then $q$ is a core order. Moreover, if $q \equiv 3 \pmod{4}$ is a core order, then $q^r$ is a core order for any odd $r \geq 1$ (see [9], p. 497).

In Section 2 we give an infinite class of OD with 8 variables. In Section 3 we construct several families of COD with 4 variables. In Section 4 we construct weak amicable $T$-matrices.

## 2 The construction of OD

The Goethals-Seidel (or Wallis-Whiteman) array has been proven to be a very useful tool for construction of orthogonal designs. Such arrays are essential for construction of orthogonal designs with more than four variables.

For convenience we need following definition:

**Definition 5 [Additive property]** A set of matrices $\{B_1, \ldots, B_m\}$ of order $n$ with entries in $\{0, \pm x_1, \ldots, \pm x_k\}$ is said to satisfy the **additive property**, with weight $\sum_{i=1}^k s_i x_i^2$, if

$$\sum_{i=1}^m B_i B_i^T = (\sum_{i=1}^k s_i x_i^2) I_n. \quad (1)$$

Kharaghani [6] gave an infinite number of arrays which are suitable for any amicable set of 8 type 1 matrices. Here **suitable** means a set of matrices satisfying the **additive property**. If one substitutes the matrices in an orthogonal design, or the Goethals-Seidel array, one can get an orthogonal design. We rewrite the following theorems without proof.

**Theorem 2** ([6]) *There is an 8 $\times$ 8 array which is suitable to make an $8n \times 8n$ orthogonal matrix for any amicable set of 8 type 1 matrices of order $n$ satisfying an additive property.*
Theorem 3 ([6]) For each prime power \( q \equiv 3 \pmod{4} \) there is an array suitable for any amicable set of eight matrices \( A_i \) satisfying

\[
\sum_{i=1}^{4} (A_{2i-1}A_{2i}^T + A_{2i}A_{2i-1}^T) = cI_{q+1},
\]

where \( c \) is a constant expression.

More general results are given in [2]. As an application we give an example of such an OD.

If \( A \) is a circulant matrix of order \( n \) with the first row \((a_1, \ldots, a_n)\), we denote it by

\[ A = \text{circ}(a_1, \ldots, a_n). \]

Example 1 Let \( x_1, x_2, x_3, x_4 \) and \( x_5 \) be real commuting variables and

\[
\begin{align*}
A_1 &= \text{circ}(x_1, x_2, x_3, x_4, -x_4, -x_3, x_2), & A_2 &= \text{circ}(-x_1, x_2, x_3, -x_4, x_4, x_3, x_2), \\
A_3 &= \text{circ}(x_1, -x_2, x_3, -x_4, x_4, x_3, -x_2), & A_4 &= \text{circ}(-x_1, -x_2, -x_3, -x_4, x_4, x_3, x_2), \\
A_5 &= \text{circ}(x_5, x_2, x_3, x_4, x_3, x_2, -x_2), & A_6 &= \text{circ}(-x_5, x_2, x_3, x_4, x_3, -x_2), \\
A_7 &= \text{circ}(x_5, -x_2, x_3, -x_4, x_4, x_3, x_2), & A_8 &= \text{circ}(-x_5, -x_2, x_3, -x_4, x_3, x_2).
\end{align*}
\]

It is easy to verify that

\[
\sum_{i=1}^{4} (A_{2i-1}A_{2i}^T - A_{2i}A_{2i-1}^T) = 0 \quad \text{and} \quad \sum_{i=1}^{8} A_iA_i^T = (4(x_1^2 + x_5^2) + 16(x_2^2 + x_3^2 + x_4^2))I_7.
\]

From the proof of Theorem 2, using the method in [6], one can construct an OD(56; 4, 4, 16, 16, 16).

Theorem 4 Let \( q \equiv 3 \pmod{4} \) be a core order. Then there is an OD(4q^r(q + 1); q^r, q^r, q^r, q^r, q^{r+1}, q^{r+1}, q^{r+1}, q^{r+1}) for any integer \( r \geq 0 \).

Proof. Let \( Q \) be a core of order \( q \), and let \( a_1, \ldots, a_8 \) be real commuting variables. Set

\[ A_{2i-1}(0) = a_{2i}, \quad A_{2i}(0) = a_{2i-1}, \quad i = 1, 2, 3, 4. \]

It is clear that, as \( A_i(0) \) are commuting variables,

\[
\begin{align*}
A_1(0), \ldots, A_8(0) & \text{ are type 1,} \\
A_{2i-1}(0)A_{2i}^T(0) &= A_{2i}(0)A_{2i-1}^T(0), \quad i = 1, 2, 3, 4,
\end{align*}
\]

and (with \( q^0 = 1 \),

\[
A_{2i-1}(0)A_{2i}^T(0) + qA_{2i}(0)A_{2i}^T(0) = q^0(qa_{2i-1}^2 + a_{2i}^2)I_{q^0}, \quad i = 1, 2, 3, 4.
\]
Suppose that for \( r \geq 1 \) we have
\[
A_1(r-1), \ldots, A_8(r-1) \text{ are all type 1}
\]
\[
A_{2i-1}(r-1)A^T_{2i}(r-1) = A_{2i}(r-1)A^T_{2i-1}(r-1), \quad \text{and}
\]
\[
A_{2i-1}(r-1)A^T_{2i}(r-1) + qA_{2i}(r-1)A^T_{2i}(r-1) = q^{r-1}(qa^2_{2i-1} + a^2_{2i})I_{q^r-1},
\]
\( i = 1, 2, 3, 4. \)

Write
\[
A_{2i-1}(r) = J_q \times A_{2i}(r-1), \quad A_{2i}(r) = I_q \times A_{2i-1}(r-1) + Q \times A_{2i}(r-1),
\]
where \( \times \) is the Kronecker product. Then \( A_1(r), \ldots, A_8(r) \) are type 1 of size \( q^r \).

It is easy to verify that
\[
A_{2i-1}(r)A^T_{2i}(r) = A_{2i}(r)A^T_{2i-1}(r),
\]
\[
A_{2i-1}(r)A^T_{2i-1}(r) + qA_{2i}(r)A^T_{2i}(r) = q^{r}(qa^2_{2i-1} + a^2_{2i})I_{q^r}, \quad i = 1, 2, 3, 4.
\]

Now let \( B_i \) of size \((q + 1)q^r \) be given by
\[
B_i = I_{q+1} \times A_{2i-1}(r) + K \times A_{2i}(r), \quad i = 1, 2, 3, 4, \quad K = \begin{bmatrix} 0 & e^T \\ -e & Q \end{bmatrix},
\]
where \( e^T = (1, \ldots, 1) \) is a row vector with \( q \) components.

Then \( B_1, B_2, B_3 \) and \( B_4 \) are of type 1 and
\[
\sum_{i=1}^{4} B_iB_i^T = \sum_{i=1}^{4} q^{r}(qa^2_{2i-1} + a^2_{2i})I_{q^r(q+1)}.
\]

From Theorem 3 it follows that there is an \( \text{OD}(4q^r(q+1); q^r, q^r, q^r, q^r, q^{r+1}, q^{r+1}, q^{r+1}) \).

Note that Corollary 5 of [6] is a special case of Theorem 4 with \( r = 0 \).

If there are type 1 \( T \)-matrices of order \( n \), then there exist an \( \text{OD}(4n; n, n, n, n) \) (see [9]). Further, from [5], weak amicable sets can be used to get the following.

**Lemma 1** For \( p \) odd, \( 1 \leq p \leq 21, \ p \in \{25, 49\} \), there exists an \( \text{OD}(8p; p, p, p, p, p, p, p, p, p, p) \).

**Proof.** For each \( p \in \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 49\} \), there exist \( T \)-matrices \( T_1, T_2, T_3 \) and \( T_4 \) of order \( p \) satisfying weak amicability.

The explicit construction of such \( T \)-matrices of these orders can be found in Table 1 of [5] and the Appendix of this paper. From Theorem 5 and Corollary 6 of [5], there exist \( \text{OD}(8p; p, p, p, p, p, p, p, p, p, p) \). \( \square \)

**Theorem 5** Let \( T_1, T_2, T_3 \) and \( T_4 \) be \( T \)-matrices of order \( p \) with weak amicability. Then there is an \( \text{OD}(4pq^r(q+1); pq^r, pq^r, pq^r, pq^r, q^{r+1}, q^{r+1}, q^{r+1}) \) for each core order \( q \equiv 3 \pmod{4} \) and \( r \geq 0 \).
Proof. Write
\[ f(a, b, c, d) = T_1a + T_2b + T_3c + T_4d. \]
Here \( a, b, c \) and \( d \) are real commuting variables. Let \( A_1, \ldots, A_8 \) be defined as follows:
\[
A_1 = f(x_1, x_2, x_3, x_4), \quad A_2 = f(-x_8, -x_7, x_6, x_5), \\
A_3 = f(x_2, -x_1, x_4, -x_3), \quad A_4 = f(x_7, -x_8, -x_5, x_6), \\
A_5 = f(x_3, -x_4, -x_1, x_2), \quad A_6 = f(x_5, x_6, x_7, x_8), \\
A_7 = f(x_4, x_3, -x_2, -x_1), \quad A_8 = f(x_6, -x_5, x_8, -x_7),
\]
where \( x_1, \ldots, x_8 \) are real commuting variables. Set
\[
A_{2i}(0) = A_{2i-1}, \quad A_{2i-1}(0) = A_{2i}, \quad i = 1, 2, 3, 4.
\]
For \( r \geq 1 \) let
\[
A_{2i-1}(r) = J_q \times A_{2i}(r - 1), \\
A_{2i}(r) = I_q \times A_{2i-1}(r - 1) + Q \times A_{2i}(r - 1), \quad i = 1, 2, 3, 4,
\]
where \( Q \) is a square matrix of order \( q \) defined as in Theorem 4. Replacing
\[
A_{2i-1}(r)A_{2i}^T(r) = A_{2i}(r)A_{2i-1}^T(r), \\
A_{2i-1}(r)A_{2i}^T(r) + qA_{2i}(r)A_{2i}^T(r) = q^r(qa_{2i-1}^2 + a_{2i}^2)I_{q^r}, \quad i = 1, 2, 3, 4, \quad r \geq 0,
\]
by
\[
\sum_{i=1}^{4} (A_{2i-1}(r)A_{2i}^T(r) - A_{2i}(r)A_{2i-1}^T(r)) = 0,
\]
\[
\sum_{i=1}^{4} (A_{2i-1}(r)A_{2i}^T(r) + qA_{2i}(r)A_{2i}^T(r)) = pq^r \sum_{i=1}^{4} (qx_i^2 + x_{i+4}^2)I_{pq^r},
\]
respectively, and repeating the procedure of the proof of Theorem 4, one can obtain the theorem.

Corollary 1 For \( p \) odd, \( 1 \leq p \leq 21 \) and \( p \in \{25, 49\} \), there exists an OD\( (8pq^r(q + 1); pq^r, pq^r, pq^r, pq^r, pq^r, pq^r, pq^r, pq^r) \) with each core order \( q \equiv 3 \) (mod 4) and integer \( r \geq 0 \).

3 The construction of COD

In this section we give several infinite classes of COD.

Theorem 6 There exists a COD\( (2q^r(q + 1); q^r, q^r, q^r, q^r) \) for each prime power \( q \equiv 1 \) (mod 4) and \( r \geq 0 \).
Proof. Let \( Q \) be the symmetric core of order \( q \equiv 1 \pmod{4} \).

Now let

\[
A_{2i-1}(0) = a_{2i-1}, \quad A_{2i}(0) = a_{2i}, \quad i = 1, 2,
\]

where \( a_1, a_2, a_3 \) and \( a_4 \) are real commuting variables. Note that \( q^0 = 1 \). It is clear that

\[
A_{2i-1}(0)A_{2i}(0) = A_{2i}(0)A_{2i-1}(0),
\]

\[
A_{2i-1}(0)A_{2i-1}(0) + qA_{2i}(0)A_{2i}(0) = q^0(a_{2i-1}^2 + qa_{2i}^2)I_{q^0}, \quad i = 1, 2,
\]

\[
A_i(0)A_j(0) = A_j(0)A_i(0), \quad 1 \leq i, j \leq 4.
\]

Suppose that for \( r \geq 1 \) we have

\[
A_{2i-1}(r - 1)A_{2i}(r - 1) = A_{2i}(r - 1)A_{2i-1}(r - 1),
\]

\[
A_{2i-1}(r - 1)A_{2i-1}(r - 1) + qA_{2i}(r - 1)A_{2i}(r - 1) = q^{r-1}(a_{2i-1}^2 + qa_{2i}^2)I_{q^{r-1}}, \quad i = 1, 2,
\]

\[
A_i(r - 1)A_j(r - 1) = A_j(r - 1)A_i(r - 1), \quad 1 \leq i, j \leq 4.
\]

Write

\[
A_{2j-1}(r) = J_q \times A_{2j}(r - 1), \quad A_{2j}(r) = I_q \times A_{2j-1}(r - 1) + iQ \times A_{2j}(r - 1),
\]

\( i = \sqrt{-1}, \quad j = 1, 2 \). It follows that

\[
A_{2i-1}(r)A_{2i}(r) = A_{2i}(r)A_{2i-1}(r),
\]

\[
A_{2i-1}(r)A_{2i-1}(r) + qA_{2i}(r)A_{2i}(r) = q^r(a_{2i-1}^2 + qa_{2i}^2)I_{q^r}, \quad i = 1, 2,
\]

\[
A_i(r)A_j(r) = A_j(r)A_i(r), \quad 1 \leq i, j \leq 4.
\]

Let

\[
K = \begin{bmatrix} 0 & e^T \\ e & Q \end{bmatrix}.
\]

Put

\[
F_j = I_{q+1} \times A_{2j-1}(r) + iK \times A_{2j}(r), \quad i = \sqrt{-1}, \quad j = 1, 2.
\]

We have

\[
F_jF_j^* = q^r(a_{2j-1}^2 + qa_{2j}^2)I_{q^r(q+1)}, \quad j = 1, 2,
\]

\[
F_1F_2 = F_2F_1.
\]

Finally, let

\[
X = \begin{pmatrix} F_1 & F_2 \\ -F_2^* & F_1^* \end{pmatrix}.
\]

Then \( X \) is a COD(\( 2q^r(q + 1); q^r, q^r, q^{r+1}, q^{r+1} \)), as required. \( \square \)

From the proof of Theorem 6 we can obtain the following theorem.

**Theorem 7** There is a COD(\( q^r(q + 1); q^r, q^r, q^{r+1}, q^{r+1} \)) for each prime power \( q \equiv 1 \pmod{4} \) and \( r \geq 0 \).
4 The construction of weak amicable $T$-matrices

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

$$a_1g_1 + a_2g_2 + \cdots + a_pg_p, \ a_i \in Z, \ g_i \in G, \ 1 \leq i \leq p.$$ 

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

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

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

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

For any subset $A$ of $G$, we define

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

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

Let a set $\{X_1, \ldots, X_8\}$ be a $C$-partition of an abelian additive group $G$ of order $p$, i.e.,

$$X_i \subset G, \ X_i \cap X_j = \emptyset, \ i \neq j,$$

and

$$ \sum_{i=1}^8 X_i = G, \ \sum_{i=1}^8 X_iX_i^{(-1)} = p + \sum_{i=1}^4 \left(X_iX_{i+4}^{(-1)} + X_{i+1}X_i^{(-1)}\right),$$

where the equations above hold in the group ring $Z[G]$; (see [13]).

For any $A \subset G$, set

$$I(A) = (a_{ij})_{1 \leq i,j \leq n}, \ a_{ij} = \begin{cases} 1, & \text{if } g_j - g_i \in A, \\ 0, & \text{otherwise}, \end{cases}$$

where $g_1, \ldots, g_p$ are elements of $G$ in any order. That is, $I(A)$ is the $(0,1)$ incidence matrix of $A$ of type 1. Now let

$$T_i = I(X_i) - I(X_{i+4}), \ i = 1, 2, 3, 4,$$

then $T_1, T_2, T_3$ and $T_4$ are $T$-matrices of order $p$.

Let $\sum_g a(g)g \in Z[G]$ where $a(g) \in Z$ and $g \in G$. If, for any $g \in G$, we have $a(g) = a(-g)$, then we call $\sum_g a(g)g$ symmetric in the group ring $Z[G]$.

It is clear that $T$-matrices $T_1, T_2, T_3$ and $T_4$ of order $p$ satisfy weak amicability, if and only if $T_1(T_3 + T_4)^T + T_2(T_3 - T_4)^T$ is symmetric, and if and only if $(X_1 - X_5)(X_3^{(-1)} - X_7^{(-1)} + X_4^{(-1)} - X_8^{(-1)}) + (X_2 - X_6)(X_3^{(-1)} - X_7^{(-1)} - X_4^{(-1)} + X_8^{(-1)})$ is symmetric in the group ring $Z[G]$.

The following theorem and corollary will simplify the verification of weak amicability in some cases.
Theorem 8 Let $G$ be an abelian group of order $n$ and let $\{X_1, \ldots, X_8\}$ be a $C$-partition of $G$. If both $X_1 - X_5 + X_2 - X_6$ and $X_3 - X_7 + X_4 - X_8$ are symmetric in the group ring $\mathbb{Z}[G]$, then there exist $T$-matrices of order $n$ satisfying weak amicability if and only if $(X_2 - X_6)(X_4^{(-1)} - X_8^{(-1)})$ is also symmetric in the group ring $\mathbb{Z}[G]$.

Using the same assumptions as in Theorem 8, we have the following corollary.

Corollary 2 If $X_4 = X_8 = \emptyset$, then there exist $T$-matrices of order $n$ satisfying weak amicability.

Appendix

Now we give decomposition of the sum of four squares and the new sets of $T$-matrices which have weak amicability for $p = 9, 25, 49$. The values $1 \leq p \leq 21$ are given in Holtzmann and Kharaghani [5].

\[ p = 9 = 3^2 + 0^2 + 0^2 + 0^2, \quad Q_1 = \{0, 1, x + 1\}, \quad Q_2 = \{2\} - \{x + 2\}, \]
\[ Q_3 = \{2x\} - \{2x + 2\}, \quad Q_4 = \{2x + 1\} - \{x\}. \]

\[ p = 25 = 5^2 + 2^2 + 0^2 + 0^2, \quad Q_1 = \{0\} - E_0 \cup E_1, \quad Q_2 = E_2 - E_6, \quad Q_3 = E_3 - E_7, \]
\[ Q_4 = E_4 - E_5, \quad \text{where} \quad E_i = \{g^{8j+i} : j = 0, 1, 2\}, \quad i = 0, \ldots, 7, \]
\[ \text{and} \quad g = x + 1(\text{mod} \ x^2 - 3, \text{mod} \ 5) \text{ is a generator of } \mathbb{GF}(25). \]

\[ p = 49 = 7^2 + 0^2 + 0^2 + 0^2, \quad Q_1 = \{0\} \cup E_0 \cup E_1 \cup E_6 \cup E_{12} - E_3 \cup E_7, \]
\[ Q_2 = E_4 \cup E_{10} \cup E_{15} - E_8 \cup E_{11} \cup E_{13}, \quad Q_3 = E_9 - E_2, \]
\[ Q_4 = E_5 - E_{14}, \quad \text{where} \quad E_i = \{g^{16j+i} : j = 0, 1, 2\}, \quad i = 0, \ldots, 15, \quad \text{and} \]
\[ g = x + 2 \ (\text{mod} \ x^2 + 1, \text{mod} \ 7) \text{ is a generator of } \mathbb{GF}(49). \]

Remark. Holzmann and Kharaghani [5] have given constructions of weak amicable $T$-matrices of order 9 in $\mathbb{Z}_9$ and for $9 = 2^2 + 2^2 + 1^2 + 0^2$, however, our construction is given in $\mathbb{GF}(9)$ and for $9 = 3^2$. These constructions are different in essence.

Conjecture ([5]). There exist infinite orders of $T$-matrices satisfying weak amicability for all odd integers.

Acknowledgements

We are grateful to the referees for their helpful comments.

References


(Received 7 July 2011; revised 10 May 2012, 5 June 2012)