Construction of $T-$matrices of order $6m+1$

Mingyuan Xia[†] and Tianbing Xia[‡], Jennifer Seberry[‡] and Hong Qin[†]

[†] School of Mathematics and Statistics,
Central China Normal University, Wuhan, Hubei 430079, P. R. China
EMail: [xiamy, qinhong]@mail.ccnu.edu.cn

[‡] School of Computing and Information Technology,
University of Wollongong, NSW 2522, Australia
Email: [txia, j.seberry]@uow.edu.au

Abstract

In this paper we prove the necessary and sufficient condition for an integer n to equal a^2+3b^2. Consequently, every prime power $6m+1$ has a representation of the form a^2+3b^2. Then we show how to construct $T-$matrices of order $6m+1$ by using 4 sequences of lengths r, r, $2m-r$, $2m-r$ with $r=m-2$ or $r=m$ in which the first is a subset of the integers $\{0,1,\cdots,2m-1\}$ with size r, the second and third sequences are of $(1,-1)$, and every component of the last sequence belongs to the set $\{0,1,2\}$. For $m\leq 13$ and $m\neq 9$, we give concrete constructions.

Keywords T-matrices; Hadamard matrices; Representability.

1 Introduction

$T-$matrices play important roles in the construction of Hadamard matrices. In 1965 L. Baumert and M. Hall, Jr [1] found a construction of Hadamard matrices of order $12n$ from known Williamson matrices of order n. In 1972, Joan Cooper and Jennifer Seberry Wallis [3] gave the first definition of $T-$matrices. J. Seberry and M. Yamada [6] gave further insight into their constructions and applications. In 1984 M. Y. Xia [9] proposed the idea of $C-$partitions on an Abelian group, and then an infinite family of $C-$partitions on $GF(q^2)$ with q prime power$\equiv 3 \pmod 8$ was found [10]. In 2010 G. Zuo and M. Xia [11] and in 2013 G. Zuo, M. Xia and T. Xia [12] gave some new methods to construct composite T-matrices by using strongly disjoint $T-$matrices and suitable $T-$matrices, and found infinite new orders of $T-$matrices. This paper is devoted to a new method of construction of $T-$matrices.

For a given positive integer n if there are integers a and b such that

$$n = a^2 + 3b^2, \tag{1}$$

we call n representable.

There are 2 problems which will be discussed in this paper: the representability of a given number and construction of $T-$matrices for this order. Concretely, we will prove that a given number n is representable if and only if its every square free factor $\not\equiv 2 \pmod 3$ has even exponents. Then, corresponding to (1), we will construct $T-$matrices of this order.

We believe that the method of construction of $T-$matrices given in this paper is new.

In the following sections, if b is divisible by a, we denote it as $a|b$; otherwise, we denote it as $a \not| b$.

2 Representability

In this section we will prove the necessary and sufficient condition for which (1) holds.

Theorem 1 *A given number n is representable if and only if its every square free factor $\not\equiv 2 \pmod 3$ has even exponents in the prime factorization of n.*

We will prove the theorem by the following lemmas. The proof use the similar methods alone the lines of the proofs in Chapter 1 of [5] by William J Levesque, and also in Chapter 4 of [2] by Duncan Buell. Readers can find the alternate route in the books.

Lemma 1 *If n is representable, then its every square free factor $\not\equiv 2 \pmod 3$ has even exponents in the prime factorization of n.*

Proof. Since n is representable, there are 2 integers a and b satisfying (1).

First, we will prove the case: if a prime $p \equiv 2 \pmod 3$ is odd and p^r is a factor of n, then r is even. Otherwise, write $p^r = q$ and the greatest common divisor $(a, q) = d$. Then $(b, q) = d$ too. From (1) it follows

$$a^2 + 3b^2 \equiv 0 \pmod q,$$

i.e.,

$$a^2 \equiv -3b^2 \pmod q. \tag{2}$$

If $d = 1$. Consider Jacobi's symbol:

$$\begin{aligned} (\frac{-3b^2}{q}) &= (\frac{-1}{q})(\frac{3}{q}) \\ &= (-1)^{q-1}(\frac{q}{3}) \\ &= (\frac{2}{3}) = -1. \end{aligned}$$

But $(\frac{a^2}{q}) = 1$ (For Jacobi's symbol see [8] for the details). Consequently, (2) can't hold. Hence $d > 1$. Then $d = p^t$ for some integers $t > 0$. Since $p^{2t}|n$, so $r \geq 2t$. If $r = 2t$, the conclusion holds. Assume $r > 2t$. Let $a_1 = a/d$, $b_1 = b/d$, $q_1 = q/d^2$ and $n_1 = n/d^2$. Now $(a_1, q_1) = (b_1, q_1) = 1$ and

$$a_1^2 \equiv -3b_1^2 \pmod{q_1}. \tag{3}$$

Using Jacobi's symbol again, repeating the discussion above for a_1, b_1 and q_1, we can get the contradiction. So, $r = 2t$.

Now suppose 2^r, r odd, is a square free factor of n. Write $q = 2^r$ and $n_1 = n/q$. Then n_1 is odd and $n_1 \equiv 1$ or $3 \pmod 4$. Denote the greatest common divisor $(a, q) = d$. So, $(b, q) = d$ too. If d=1, then both a and b are odd. So, $a^2 + 3b^2 \equiv 4 \pmod 8$. But $n \equiv 0, 2, 6 \pmod 8$ according as $r \geq 3$, $r = 1$ and $n_1 \equiv 1 \pmod 4$, $r = 1$ and $n_1 \equiv 3 \pmod 4$, respectively. This is a contradiction.

If $d > 1$. Then $d = 2^t$ for some integer $t > 0$. Since $d^2|n$, we have $r > 2t$. Write $a_1 = a/d$, $b_1 = b/d$, $m_1 = n/d^2$, repeat the discussion above for a_1, b_1, m_1, we can get a contradiction too. The proof is completed. □

Lemma 1 proved the necessary condition for the representability of a number.

Corollary 1 *Let prime $p \equiv 2 \pmod 3$. Then p^{2t+1} isn't representable for any $t \geq 0$.*

Lemma 2 *If both m and n are representable, then mn is representable.*

Proof. Let

$$m = a^2 + 3b^2,\ n = c^2 + 3d^2.$$

Then

$$mn = (ac + 3bd)^2 + 3(ad - bc)^2,$$

or

$$mn = (ac - 3bd)^2 + 3(ad + bc)^2.$$

□

Lemma 3 *Every square is representable.*

The proof of Lemma 3 is trivial.

We quote the following theorem of Fermat without proof.

Theorem 2 *(Theorem of Fermat) A prime is representable if and only if it is 3 or congruent to 1 (mod 3).*

Lemma 2 *and* Theorem 2 together are sufficient conditions for Theorem 1.

Lemma 4 *For any prime $p \equiv 1 \pmod 3$, its representation is unique in the sense: If $p = a^2 + 3b^2$ and $p = c^2 + 3d^2$, then $a^2 = c^2$ and $b^2 = d^2$.*

Proof. Let $p = a^2 + 3b^2 = c^2 + 3d^2$. It is clear that

$$0 < |a|,\ |b|,\ |c|,\ |d| \leq (p-1)/2,$$

and

$$(a, p) = (b, p) = 1.$$

The set of all residues $(ia)^2 \pmod p$, $0 < i \leq (p-1)/2$, is just the set of all non-zero quadratic residues (mod p). So, there is an i $(0 < i \leq (p-1)/2)$ such that $c^2 \equiv (ia)^2 \pmod p$. For any i there is a unique r such that $|ia - rp| \leq (p-1)/2$. Clearly, $(ia)^2 \equiv (ia - rp)^2 \pmod p$. Therefore, $c^2 \equiv (ia - rp)^2 \pmod p$. Now both $|c|$ and $|ia - rp| \leq (p-1)/2$, hence we have

$$c^2 = (ia - rp)^2.$$

Similarly, we can get j $(0 < j \leq \frac{p-1}{2})$ and s such that

$$d^2 = (jb - sp)^2.$$

Then

$$\begin{aligned} p &= (ia - rp)^2 + 3(jb - sp)^2 \\ &= [i^2 - 2iar - 6jbs + (r^2 + 3s^2)p]p + 3(j^2 - i^2)b^2. \end{aligned}$$

It follows that

$$3(j^2 - i^2)b^2 \equiv 0 \pmod p.$$

Since $(3, p) = (b, p) = 1$ and $0 < i,\ j < \frac{p-1}{2}$, we have

$$\begin{aligned} &j = i, \\ &1 = (i - ar - 3bs)^2 + 3(as - br)^2. \text{ (use } a^2 + 3b^2 = p.) \end{aligned}$$

Therefore

$$\begin{aligned} &as = br, \\ &1 = (i - ar - 3bs)^2. \end{aligned}$$

From the first equation above we obtain $s = \frac{br}{a}$. Substitute it for s in the second equation above, we obtain

$$\begin{aligned} 1 &= [\frac{ia - (a^2 + 3b^2)r}{a}]^2 \\ &= (\frac{ia - pr}{a})^2 \\ &= (\frac{c}{a})^2, \end{aligned}$$

as required. Thus $b^2 = d^2$. The proof is completed. □

Remark. For representable prime powers the uniqueness of their representation isn't true. For example, let $q = 91 = a^2 + 3b^2 = c^2 + 3d^2$, where $(a, b) = (4, 5)$ and $(c, d) = (8, 3)$. Now $i = 2,\ r = 0,\ j = 37,\ s = 2$ and we have

$$c^2 + 3d^2 = (ia - rq)^2 + 3(jb - sq)^2.$$

Though $(a, q) = (b, q) = 1$, $0 < i,\ j \leq \frac{q-1}{2}$ and $j^2 - i^2 \equiv 0 \pmod{q}$, but $j \neq i$.

Corollary 2 *If n=6m+1 is a prime power, then it is also representable.*

Proof. Let $n = p^r$, p prime, $r > 0$ integer. If $p \equiv 1 \pmod 3$, then p^r is representable and has the form $6m + 1$ with some m for any $r > 0$. If $p \equiv 2 \pmod 3$, since $p^r = 6m + 1$, r must be even, hence n is representable. The proof is completed. □

Corollary 3 *Let m be a prime power, $n = 6m+1 = a^2+3b^2$. Then $a \equiv m+1 \pmod 2$ and $b \equiv m \pmod 2$. Moreover, if $a \equiv 1 \pmod 3$, then $(a-1)/3 \equiv m \pmod 2$; if $a \equiv 2 \pmod 3$, then $\frac{a+1}{3} \equiv m \pmod 2$.*

Proof. It is obvious that both a and b can't be even at the same time since $6m + 1$ is odd. Similarly, both a and b can't be odd at the same time. Otherwise, $a^2 + 3b^2$ would be $\equiv 0 \pmod 4$. Therefore, $a + b \equiv 1 \pmod 2$. If m is even. b should be even and a is odd, since at this time $6m + 1 \equiv 1 \pmod 4$. If m is odd. b must be odd and a is even, since at this time $6m + 1 \equiv 3 \pmod 4$. If $a \equiv 1 \pmod 3$, then $a = 3t + 1$ for some integer t. Substitute $3t + 1$ for a, we have

$$6m + 1 = 9t^2 + 6t + 1 + 3b^2,$$

i.e.,

$$2m = 3t^2 + 2t + b^2.$$

From the last equation above it follows that

$$t^2 + b^2 \equiv 0 \pmod 2.$$

Hence

$$t \equiv b \equiv m \pmod 2,$$

i.e.,

$$\frac{a-1}{3} \equiv m \pmod 2.$$

Similarly, one can prove that if $a \equiv 2 \pmod 3$, then $\frac{a+1}{3} \equiv m \pmod 2$. The proof is completed. □

3 Construction $T-$matrices of order $6m+1$

Definition 1 *(T-matrices) Four ciculant or type* 1 $(0,1,-1)$ *matrices* T_1, T_2, T_3 *and* T_4 *of order* t *are called* $T-$*matrices if the following 2 conditions are satisfied:*

- $T_i * T_j = 0,\ i \neq j$;
- $\sum_{i=1}^{4} T_i T_i' = tI_t$,

where $*$ *denotes Hadamard product,* T_i' *is the transpose of* T_i, I_t *is the identity matrix of order* t.

Let G be an Abelian group of order t. It is convenient to use the group ring $Z[G]$ of the group G over the ring Z of rational integers. From [10] we know that if subsets $A_1, \cdots, A_8$ of G form a $C-$partition of G, i.e.,

$$A_i \cap A_j = \phi \text{ for } i \neq j,\ \cup_{i=1}^{8} A_i = G,$$

and

$$\sum_{i=1}^{8} A_i A_i^{-1} - \sum_{i=1}^{4} (A_i A_{i+4}^{-1} + A_{i+4} A_i^{-1}) = t,$$

then there are $T-$matrices T_1, T_2, T_3 and T_4 of order t with

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

where

$$I(A) = (a_{ij})_{1 \leq i,j \leq t},$$

and $a_{ij} = 1$ or 0 according as $g_j g_i^{-1}$ belongs to A or not, provided the elements g_1, $\ldots$, g_t are of G arranged in any order. Instead of $A_1, \cdots, A_8$, we consider

$$Q_i = A_i - A_{i+4},\ i = 1,2,3,4,$$

and define

$$T_i = I(Q_i) = I(A_i) - I(A_{i+4}),\ i = 1,2,3,4.$$

Thus T_1, T_2, T_3 and T_4 are $T-$matrices of order t if and only if $\sum_{i=1}^{4} Q_i Q_i^{-1} = t$.

In the following we assume $t = 6m+1$ $(m > 0)$ is a prime power and

$$t = a^2 + 3b^2.$$

Without loss of generality we may assume $a,\ b \geq 0$.

Let g be a generator of the multiplicative group of $GF(t)$. Set

$$c_i(j) = g^{2mj+i}, j = 0,1,2,\ i = 0, \cdots, 2m-1,$$
$$c_i = \{g^{2mj+i} : j = 0,1,2\},\ i = 0, \cdots, 2m-1.$$

Our constructions for Q_1, Q_2, Q_3 and Q_4 are roughly as follows.

Let X be a subset of $S = \{0, 1, \cdots, 2m-1\}$, $Y = S \backslash X$ and $|X| = r \equiv m \pmod 2$. We denote 0 by z. Set

$$\begin{array}{l} Q_1 = z + \sum_{i \in X} \alpha_i c_i, \\ Q_2 = \sum_{j \in Y} \beta_j c_j(\delta_j), \\ Q_3 = g^{2m} Q_2, \\ Q_4 = g^{4m} Q_2, \end{array} \tag{4}$$

where α_i, β_j are 1 or -1, $\delta_i \in \{0, 1, 2\}$, such that,

$$|1 + 3 \sum_{i \in X} \alpha_i| = a, \quad |\sum_{j \in Y} \beta_i| = b. \tag{5}$$

The equations can be written as follows. Let λ and μ be the numbers of ones in a set $\{\alpha_i : i \in X\}$ and a set $\{\beta_j : j \in Y\}$, respectively. If we take $\mu = m + \frac{b-r}{2}$, the second equation of (5) will be satisfied. If we take $\lambda = \frac{r + \frac{a-1}{3}}{2}$ for $a \equiv 1 \pmod 3$ or $\frac{r - \frac{a+1}{3}}{2}$ for $a \equiv 2 \pmod 3$, the first equation of (5) will be satisfied too.

Now the problem is to define X, α_i, β_j and δ_k satisfying

$$\sum_{i=1}^{4} Q_i Q_i^{-1} = t. \tag{6}$$

Clearly, such $Q_i, i = 1, 2, 3, 4$, are completely determined by these X, Y, α_i, β_j and δ_j, where $i \in X$ and $j \in Y$. Thus our aim is to define 4 sequences of lengths r, r, $2m - r$, $2m - r$, respectively, satisfying equation (6). We say that such quadruple (Q_1, Q_2, Q_3, Q_4) has $T-$property.

Theorem 3 *Suppose the quadruple (Q_1, Q_2, Q_3, Q_4) given in (4) has $T-$property and k is a positive integer. Let U, V be 2 ordinal sets such that*

$$\begin{array}{l} U = \{x + k (\mathrm{mod}\ 2m) : x \in X\}, \\ V = \{y + k (\mathrm{mod}\ 2m) : y \in Y\}. \end{array}$$

Then, using U and V in (4) instead of X and Y respectively, the obtained quadruple $(Q_1^*, Q_2^*, Q_3^*, Q_4^*)$ has the $T-$property too.

The proof is trivial.

The main advantage of the theorem above is that it greatly reduces the search space.

In this paper we choose the ordinal set X with one of the following 2 patterns:

$(w1)$ $i \in X$, if and only if $2m - i \in X$;

$(w2)$ $X = \{0, \cdots, r-1\}$.

Here $2m$ is the same as 0 in X and $X = \phi$ if $r = 0$. Since $|X| = r \equiv m \pmod 2$, there is only one of 0, and m belongs to X for m odd in the case $(w1)$.

Consider the automorphic transformation on $GF(t)$:

(a) $y \to yd$ for any fixed element d of $GF(t)$ provided $d \neq 0$;

(b) $y \to y^{-1}$.

Indeed, every trasformation of (a) is a translation. It is clear that if (Q_1, Q_2, Q_3, Q_4) has the $T-$property, then under every transformation of (a) T-property will be preserved. But for the transformation of (b) $T-$property can not be preserved. However, we have the following theorem.

Theorem 4 *Suppose the quadruple* (Q_1, Q_2, Q_3, Q_4) *given in (4) has the* $T-$*property. If the following conditions hold:*

(i) $i \in X$ *if and only if* $2m - i \in X$ *(*$2m$ *is treated the same as* 0*);*

(ii) $\alpha_i = \alpha_{2m-i}$ *for every* $i \in X$*;*

(iii) $\beta_j = \beta_{2m-j}$ *for every* $j \in Y$*;*

(iv) $0 \notin Y$, $\delta_j + \delta_{2m-j} = s$ *for every* $j \in Y$, *where* $s = 0$ *or* 1 *or* 2*;*

(v) $0 \in Y$, $\delta_0 = 0$, $\delta_j + \delta_{2m-j} = 2$ *for every* $j(\neq 0) \in Y$*;*

then the transformation $y \to y^{-1}$ *preserves the* $T-$*property for this quadruple.*

Proof. It is easy to see that, using g^{-1} instead of g, $c_0(j)$ becomes $c_0(-j)$ (where $-j \equiv 3 - j \pmod 3$), $c_i(j)$ becomes $c_{2m-i}(2 - j)$ for $0 < i < 2m$. Consequently, substituting g^{-1} for g, Q_1, Q_2 become

$$Q_1(g^{-1}) = Q_1(g).$$

If $0 \notin Y$,

$$\begin{aligned} Q_2(g^{-1}) &= \textstyle\sum_{j\in Y} \beta_j c_{2m-j}(2 - \delta_j) \\ &= \textstyle\sum_{j\in Y} \beta_{2m-j} c_{2m-j}(2 - s + \delta_{2m-j}) \\ &= \textstyle\sum_{j\in Y} \beta_j c_j(2 - s + \delta_j), \\ Q_3(g^{-1}) &= g^{-2m} Q_2(g^{-1}) \\ &= \textstyle\sum_{j\in Y} \beta_j c_j(1 - s + \delta_j), \\ Q_4(g^{-1}) &= \textstyle\sum_{j\in Y} \beta_j c_j(-s + \delta_j). \end{aligned}$$

We know that the triple $\{2 - s + \delta_j,\ 1 - s + \delta_j,\ -s + \delta_j\} \pmod 3$ is equivalent to the triple $\{\delta_j,\ 1 + \delta_j,\ 2 + \delta_j\} \pmod 3$. So the transformation keeps the $T-$property.

If $0 \in Y$, it follows that $Q_1(g^{-1}) = Q_1(g)$ and $Q_2(g^{-1}) = Q_2(g)$. The Theorem has been proved. □

We call (ii)-(iii) symmetric conditions. Theorem 4 greatly speed up the search process for (Q_1, Q_2, Q_3, Q_4) with the $T-$property, if such a sequence exists.

We denote 1 and -1 by $+$ and $-$ respectively for $\alpha's$ and $\beta's$. We give several examples of Theorem 4:

(I) $7 = 2^2 + 3 \times 1^2$, $g = 3$, $r = m = 1$, $X = \{0\}$, $z-$, $+$, 0;

(II) $13 = 1^2 + 3 \times 2^2$, $g = 2$, $m = 2$, $r = 0$, $X = \phi$, z, $+--$, 0012;

(III) $19 = 4^2 + 3 \times 1^2$, $g = 2$, $r = m = 3$, $X = \{0,\ 1,\ 5\}$, $z-{+}{+}$, $+-+$, 000;

(IV) $37 = 5^2 + 3 \times 2^2$, $g = 2$, $r = 2 = m/3$, $X = \{0,\ 6\}$, $z--$, $+--+--+--+$, 0110011001.

In the following examples we give 4 sequences (X, $\alpha's$, $\beta's$, $\delta's$)of lengths m, m, m, m with the $T-$property and X which satisfy the condition $(w1)$.

$m = 1,\ t = 7 = 2^2 + 3 \times 1^2,\ g = 3,\ \{0\},\ -,\ +,\ 0;$
$m = 3,\ t = 19 = 4^2 + 3 \times 1^2,\ g = 2,\ \{0, 1, 5\},\ -++,\ +-+,\ 000;$
$m = 4,\ t = 25 = 5^2 + 3 \times 0^2,\ g = x + 1 \pmod{x^2 - 3,\ \text{mod } 5}$,[1]
$\{0, 1, 4, 7\},\ +--,\ ++-,\ 0110;$
$m = 5,\ t = 31 = 2^2 + 3 \times 3^2,\ g = 3,\ \{0, 3, 4, 6, 7\},\ -++-,\ ++-++,\ 00112;$
$m = 6,\ t = 37 = 5^2 + 3 \times 2^2,\ g = 2,\ \{0, 1, 5, 6, 7, 11\},\ -+---+,\ +----+,\ 010120;$
$m = 7,\ t = 43 = 4^2 + 3 \times 3^2,\ g = 3,\ \{0, 3, 5, 6, 8, 9, 11\},\ +-+-+-+,\ +-----+,$
0011002;
$m = 10,\ t = 61 = 7^2 + 3 \times 2^2,\ g = 2,\ \{0, 1, 4, 5, 6, 10, 14, 15, 16, 19\},$
$++--+++-+,\ ++-------++,\ 0110111012;$
$m = 11,\ t = 67 = 8^2 + 3 \times 1^2,\ g = 2,\ \{0, 3, 6, 8, 9, 10, 12, 13, 14, 16, 19\},$
$-++---------++,\ +--+-++--++,\ 00220011120;$
$m = 12,\ t = 73 = 5^2 + 3 \times 4^2,\ g = 5,\ \{0, 2, 3, 5, 7, 9, 12, 15, 17, 19, 21, 22\},$
$-+--+-+-+--+,\ -++++++++--++-,\ 010202011020;$
$m = 13,\ t = 79 = 2^2 + 3 \times 5^2,\ g = 3,\ \{0, 1, 2, 3, 4, 7, 8, 18, 19, 22, 23, 24, 25\},$
$--++++----++++-,\ +-+++-++--++++,\ 0002001221010.$

When $m = 9$, $t = 55$, there is not a representation in the form $a^2 + 3b^2$. When $m = 2$ and 8, there are not $4-$sequences of lengths m, m, m, m with X satisfying $(w1)$.

In the following list the sequences have the $T-$property with X satisfying $(w2)$, i.e., $X = \{0, \cdots, r-1\}$. In this case we can omit X and write 3 sequences ($\alpha's$, $\beta's$,

[1] $g = x+1 \pmod{x^2-3,\ \text{mod } 5}$ represents a generator exists when module x^2-3 and 5. So does the same with the others.

$\delta's$) of lengths r, $2m-r$, $2m-r$

$$
\begin{aligned}
&25 = 5^2 + 3\times 0^2,\ g = x+1 \ (\mathrm{mod}\ x^2-3,\ \mathrm{mod}\ 5),\\
&\quad r = 2,\ --,\ +++---,\ 021020;\\
&31 = 2^2 + 3\times 3^2,\ g = 3,\\
&\quad r = 1,\ -,\ +++---+++,\ 012001012;\\
&37 = 5^2 + 3\times 2^2,\ g = 2,\\
&\quad r = 2,\ --,\ +++----++,\ 0010011001;\\
&43 = 4^2 + 3\times 3^2,\ g = 3,\\
&\quad r = 1,\ +,\ +++++-----++++,\ 0022220012021;\\
&43 = 4^2 + 3\times 3^2,\ g = 3,\\
&\quad r = 3,\ +-+,\ +++--+--+++,\ 01010012012;\\
&49 = 7^2 + 3\times 0^2,\ g = x+2 \ (\mathrm{mod}\ x^2+1,\ \mathrm{mod}\ 7),\\
&\quad r = 2,\ ++,\ +++----++++--,\ 02010111210202;\\
&49 = 1^2 + 3\times 4^2,\ g = x+2 \ (\mathrm{mod}\ x^2+1,\ \mathrm{mod}\ 7),\\
&\quad r = 0,\ \phi,\ -++--++++++--++-,\ 0102102122212011.
\end{aligned}
$$

To search for $T-$matrices of order $6m+1$ using base sequences, one must search for 4 sequences of lengths $3m+1$, $3m+1$, $3m$, $3m$, respectively [4, 6]. It is obvious that our method makes the searching process simpler and greatly reduces the computation time.

From our searching algorithm, we have the following conclusion:

There are (α,β,δ) sequences of lengths m, m, m, satisfying equation (6) at least for $m = 1, 2, 3, 6$, and (α,β,δ) sequences of lengths $m-2$, $m+2$ and $m+2$ satisfying equation (6) at least for $m = 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13$.

For more details see Table 1 below.

We have the following conjecture.

Conjecture. If $6m+1$ is a prime power, then there are (α,β,δ) sequences of lengths r, $2m-r$, $2m-r$, satisfying equation (6), where $r \equiv m \pmod 2$, $0 \le r < m$ for $m > 1$.

Example 1. Let $t = 19$. When $m = 3$, $a = 4$, $b = 1$. Set

$$c_i = \{2^{6j+i} : j = 0, 1, 2\},\ i = 0, 1, 2, 3, 4, 5.$$

- $r = 1$ and $X = \{0\}$. We have (α,β,δ) sequences of lengths 1, 5, 5 as follows:

$$
\begin{array}{ccccccc}
+, & & & & & & \\
+ & + & + & + & - & -, & \\
0 & 0 & 0 & 1 & 0. & &
\end{array}
$$

Q_1, Q_2, Q_3, Q_4 determined by the sequences above are

$$
\begin{aligned}
&Q_1 = \{0\} + c_0 = \{0, 1, 7, 11\},\\
&Q_2 = c_1(0) + c_2(0) + c_3(0) - c_4(1) - c_5(0) = \{2, 4, 8\} - \{17, 13\},\\
&Q_3 = c_1(1) + c_2(1) + c_3(1) - c_4(2) - c_5(1) = \{14, 9, 18\} - \{5, 15\},\\
&Q_4 = c_1(2) + c_2(2) + c_3(2) - c_3(0) - c_5(2) = \{3, 6, 12\} - \{16, 10\}.
\end{aligned}
$$

- $r = 3$ and $X = \{0, 1, 2\}$. We have (α, β, δ) sequences of lengths 3, 3, 3, as follows:

$$\begin{array}{ccc} + & - & +, \\ + & - & +, \\ 0 & 0 & 0. \end{array}$$

The corresponding sequences Q_1, Q_2, Q_3, Q_4 are:

$$\begin{aligned} Q_1 &= \{0\} + c_0 - c_1 + c_2 = \{0, 1, 4, 6, 7, 9, 11\} - \{2, 3, 14\}, \\ Q_2 &= c_3(0) - c_4(0) + c_5(0) = \{8, 13\} - \{16\}, \\ Q_3 &= c_3(1) - c_4(1) + c_5(1) = \{18, 15\} - \{17\}, \\ Q_4 &= c_3(2) - c_4(2) + c_5(2) = \{12, 10\} - \{5\}. \end{aligned}$$

- $r = 5$. There is no solution of this form.

In the Table 1 let $X = \{0, \cdots, r-1\}$.

m	t	a	b	g	r	αs	βs	δs	note
2	13	1	2	2	2	$+-$	$++$	01	
3	19	4	1	2	1	$+$	$+++--$	00010	
4	25	5	0	$x+1$	2	$--$	$+++---$	021020	(mod x^2-3, mod 5)
5	31	2	3	3	3	$-+-$	$++-----$	0000102	
6	37	5	2	2	6	$+--+--$	$++--++$	100110	
6	37	5	2	2	4	$+---$	$++-+--++$	00222021	
7	43	4	3	3	5	$-+++-$	$+++++---+$	02020000	
							$+$	2	
8	49	1	4	$x+2$	6	$---+++$	$+----+---$	01101111	(mod x^2+1, mod 7)
							$-+$	20	
8	49	7	0	$x+2$	6	$++--++$	$+++++----$	02010022	(mod x^2+1, mod 7)
							$-+$	22	
10	61	7	2	2	8	$+++++-$	$+++---++$	022201100	
						$--$	$--++$	101	
11	67	8	1	2	9	$---+++$	$+--+-+-+$	012100200	
						$---$	$-+++--$	0221	
12	73	5	4	5	10	$--+-++$	$++-+-++-$	020211000	
						$-+--$	$-+-+++$	21211	
13	79	2	5	3	11	$+-+++-$	$+-+++-++$	000101220	
						$--+--$	$--++++-$	002211	

Table 1: α, β, δ sequences

T-matrices of orders 73 and 79 are first found in [12] by another method.

References

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

[2] Duncan A. Buell, *Binary Quadratic Forms - Classical Theory and Modern Computations*, Springer, 1989.

[3] J. Cooper and J. S. Wallis, A construction for Hadamard arrays, *Bull. Austral. Math. Soc.*, 7(1972), 269-278.

[4] C. Koukouvinos, Base sequences $BS(n+1,\ n)$, *http://www.math.ntua.gr/people/ckoukouv/baseeq.htm*, (2006)

[5] William J. LeVeque, *Topics in Number Theory*, Dover, 1956.

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

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

[8] Ivan Matevievich Vinogradoff, *The Foundation of Number Theory*, National publishing house of technology-theory literatures, Moscow 1952.

[9] M. Xia, On supplementary difference sets and Hadamard matrices, *Acta Math. Sci. (Chinese)*, 4(1984), 81-92.

[10] M. Xia and T. Xia, A family of C-partions and T-matrices, *J. Combin. Designs*, 7(1999), 269-281.

[11] G. Zuo and M. Xia, A special class of $T-$matrices, *Designs, Codes and Cryptography*, 54(2010), 21-28.

[12] G. Zuo, M. Xia and T. Xia, Constructions of composite $T-$matrices, *Linear Algebra and its Applications*, 438(2013), 1223-1228.