Des. Codes Cryptogr. (2007) 45:139–155
DOI 10.1007/s10623-007-9103-4

Existence of Z-cyclic 3PDTWh(p) for Prime $p \equiv 1 \pmod 4$

Xiande Zhang · Gennian Ge

Received: 11 January 2007 / Revised: 6 June 2007 / Accepted: 21 June 2007 /
Published online: 17 July 2007

Abstract A directed triplewhist tournament on p players over Z_p is said to have the three-person property if no two games in the tournament have three common players. We briefly denote such a design as a 3PDTWh(p). In this paper, we investigate the existence of a Z-cyclic 3PDTWh(p) for any prime $p \equiv 1 \pmod 4$ and show that such a design exists whenever $p \equiv 5, 9, 13 \pmod{16}$ and $p \geq 29$. This result is obtained by applying Weil's theorem. In addition, we also prove that a Z-cyclic 3PDTWh(p) exists whenever $p \equiv 1 \pmod{16}$ and $p < 10{,}000$ except possibly for $p = 257{,}769$.

Keywords Weil theorem · Whist tournament · Z-cyclic · 3PDTWh

AMS Classification 05B05

1 Introduction

A *whist tournament* Wh(v) for $v = 4n$(or $4n + 1$) is a schedule of games (a, b, c, d) where the unordered pairs $\{a, c\}, \{b, d\}$ are called *partners*, the pairs $\{a, b\}, \{c, d\}, \{a, d\}, \{b, c\}$ are called *opponents*, such that

(1) the games are arranged into $4n - 1$(or $4n + 1$) rounds, each of n games;
(2) each player plays in exactly one game in each round(or all rounds but one);
(3) each player partners every other player exactly once;
(4) each player opposes every other player exactly twice.

Communicated by : C.J. Colbourn.

Gennian Ge's Research was supported by National Natural Science Foundation of China under Grant No. 10471127, Zhejiang Provincial Natural Science Foundation of China under Grant No. R604001, and the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry.

X. Zhang · G. Ge (✉)
Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, P.R. China
e-mail: gnge@zju.edu.cn

We may think of (a, b, c, d) as the cyclic order of the four players sitting round a table. We refer to the pairs $\{a, b\}$ and $\{c, d\}$ as pairs of *opponents of the first kind*, and the pairs $\{a, d\}$ and $\{b, c\}$ as pairs of *opponents of the second kind*. A *triplewhist tournament* TWh(v) is a Wh(v) in which each player is an opponent of the first (resp., second) kind exactly once with every other player. The triplewhist tournament problem was first introduced by Moore [35] in 1896. For a long time there was no progress until Baker [8] proved in 1975 that a TWh(v) exists for $v = 4$, 8, 16, 24 and for all large v, $v \equiv 1 \pmod 4$ and $v \equiv 0$, 4, 12 (mod 16). In 1997, much progress was made by Lu and Zhu in [34]. They proved that the necessary condition for the existence of a TWh(v), namely $v \equiv 0$ or 1 (mod 4), is also sufficient with 2 definite exceptions, namely $v = 5, 9$, as well as 15 possible exceptions in the range $12 \leq v \leq 133$. Subsequent improvements were made by Ge and Zhu in [28], Ge and Lam [24], and finally by Abel and Ge [3]. We summarize the known results as follows.

Theorem 1.1 ([3]) *Necessary conditions for existence of a TWh(v), are $v \equiv 0, 1$ (mod 4) and $v \geq 4$. These conditions are also sufficient except for $v = 5, 9, 12, 13$ and possibly for $v = 17$.*

In the games (a, b, c, d) of a Wh(v), we may also refer to b as the *left-hand opponent* of a and as the *right-hand opponent* of c, and similar definitions apply to each of a, b, c, d. A *directedwhist tournament* DWh(v) is a Wh(v) in which each player is a left (resp., right) hand opponent of every other player exactly once. A basic necessary condition for the existence of a DWh(v) is $v \equiv 0, 1 \pmod 4$. It is fairly well known [10] that a DWh(v) exists for all $v \geq 5$ whenever $v \equiv 1 \pmod 4$. On the other hand, the results for the existence of a DWh(v) whenever $v \equiv 0 \pmod 4$ are still not conclusive. It is known [36,37] that a DWh(v) exists for all $v \geq 4$ whenever $v \equiv 0 \pmod 4$, except for $v = 4, 8, 12$ and with at most 27 possible exceptions of which the largest is 188. More specifically, we have the following theorem.

Theorem 1.2 ([10,36,37]) *Necessary conditions for existence of a $DWh(v)$ are $v \equiv 0, 1$ (mod 4) and $v \geq 4$. These conditions are also sufficient except for $v = 4, 8, 12$ and possibly for $v \in \{16, 20, 24, 32, 36, 44, 48, 52, 56, 64, 68, 76, 84, 88, 92, 96, 104, 108, 116, 124, 132, 148, 152, 156, 172, 184, 188\}$.*

Whist tournaments which are simultaneously both triplewhist and directedwhist are called *directed triplewhist tournaments* and denoted briefly by DTWh(v). These were first investigated by Anderson and Finizio in [5,6].

A whist tournament is said to have *three person-property,* denoted by 3PWh(v) as in [19,26,33], if any two games do not have three common players. It was Hartman who first discussed this property in [30]. If we regard games in a 3PWh(v) as blocks, we obtain a super-simple $(v, 4, 3)$-BIBD (we call it a sub-design of the 3PWh(v)). This kind of design was introduced and studied by Gronau and Mullin [29] and also studied by Chen [15,16]. Such designs with resolvable property were investigated by Ge and Lam [25] and Zhang and Ge [38].

For the existence of a DWh(v) with the three person property, briefly denoted by 3PDWh(v), Finizio [19] was able to obtain several infinite classes and some examples where $v \equiv 1 \pmod 4$. Subsequently, for this case, a conclusive result was given by Bennett and Ge [9] and we now have the following theorem.

Theorem 1.3 ([9,19]) *There exists a $3PDWh(v)$ for all $v > 5$, where $v \equiv 1$ (mod 4).*

For the existence of a TWh(v) with the three person property, briefly denoted by 3PTWh(v), Ge [23] recently gave an almost complete solution. Concretely, we have the following theorem.

Theorem 1.4 ([23]) *The necessary conditions for existence of a* $3PTWh(v)$*, namely,* $v \equiv 0, 1 \pmod 4$ *and* $v \geq 8$*, are also sufficient except for* $v = 9, 12, 13$ *and possibly for* $v = 17$.

For the existence of a 3PWh(v) which is simultaneously both triplewhist and directedwhist, briefly denoted by 3PDTWh(v), Anderson and Finizio [5] gave an asymptotic solution for the case of $v \equiv 1 \pmod 4$. Recently, Abel et al. [1] gave a near solution as follows.

Theorem 1.5 ([1]) *There exists a* $3PDTWh(v)$ *for all* $v \geq 25$*, where* $v \equiv 1 \pmod 4$*, with the possible exceptions of* $v \in \{117, 129, 141, 145, 153, 165, 177, 185, 189, 209, 213\}$.

A whist tournament is said to be *Z-cyclic* if the players are elements in $Z_m \cup A$, where $m = v$, $A = \emptyset$ when $v \equiv 1 \pmod 4$ and $m = v - 1$, $A = \{\infty\}$ when $v \equiv 0 \pmod 4$. It is further required that the round $j + 1$ is obtained by adding $+1 \pmod m$ to every element in round j. When ∞ is present then $\infty + 1 = \infty$. For the existence of Z-cyclic whist tournaments, much less is known despite of the efforts of many authors, such as Abel et al. [1,2], Anderson et al. [5–7], Buratti [12], Feng and Chang [18], Finizio [20,21], Ge and Ling [27], Ge and Zhu [28], and Liaw [31]. The following results are known.

Theorem 1.6 ([1,5,6]) *A Z-cyclic* $DTWh(p)$ *exists for all primes* $p \equiv 5 \pmod 8$*,* $p \geq 29$*, or* $p \equiv 1 \pmod 8$*,* $41 \leq p < 10{,}000$*,* $p \neq 257, 449, 641, 769, 1153, 1409, 7681$.

Theorem 1.7 ([18]) *A Z-cyclic* $3PTWh(p)$ *exists for all primes* $p \equiv 1 \pmod 4$ *with the only exceptions of* $p = 5, 13, 17$.

Lemma 1.8 ([1]) *There exists a Z-cyclic* $3PDTWh(p)$ *for p prime,* $p \equiv 1 \pmod 4$ *and* $29 \leq p \leq 241$.

In this paper, we shall investigate the problem of existence of Z-cyclic 3PDTWh(v)s. The main focus of our attention will be the case where $v \equiv 1 \pmod 4$ is a prime p. We show that a Z-cyclic 3PDTWh(p) exists whenever $p \equiv 5, 9, 13 \pmod{16}$ and $p \geq 29$. This result is obtained by applying Weil's theorem. In addition, we also prove that a Z-cyclic 3PDTWh(p) exists whenever $p \equiv 1 \pmod{16}$ and $p < 10{,}000$ except possibly for $p = 257{,}769$. For general information on whist tournaments see the survey paper of Anderson [4]. We use [11] as our standard reference on design theory.

2 Basic constructions

In this section, we will establish the criteria for the existence of a Z-cyclic 3PDTWh(p). Given a prime $p \equiv 1 \pmod n$ and a primitive element $w \in Z_p$, we use C_0^n to denote the multiplicative subgroup $\{w^{in} : 0 \leq i < (p-1)/n\}$ of the n-th powers modulo p, and C_j^n to denote the coset of C_0^n in Z_p^*, i.e., $C_j^n = w^j \cdot C_0^n$. Our constructions are based on the following lemma.

Lemma 2.1 *Let* $p \equiv 1 \pmod 4$ *be a prime. Suppose that n is an integer such that* $4n|(p-1)$ *and* $-1 \in C_{2n}^{4n}$*. Suppose also that* $\{(a_i, b_i, c_i, d_i) : 0 \leq i \leq n-1\}$ *is a set of quadruples of elements of* Z_p^* *satisfying the following conditions:*

(1) *each of the sets* $\bigcup_{i=0}^{n-1}\{a_i, b_i, c_i, d_i\}$, $\bigcup_{i=0}^{n-1}\{b_i - a_i, c_i - b_i, d_i - c_i, a_i - d_i\}$ *is a representative system of the coset classes* $\{C_0^{4n}, C_1^{4n}, \ldots, C_{4n-1}^{4n}\}$;

(2) *each of the sets* $\bigcup_{i=0}^{n-1}\{a_i-b_i, c_i-d_i\}$, $\bigcup_{i=0}^{n-1}\{a_i-c_i, b_i-d_i\}$, $\bigcup_{i=0}^{n-1}\{a_i-d_i, b_i-c_i\}$ *is a representative system of the coset classes* $\{C_0^{2n}, C_1^{2n}, \ldots, C_{2n-1}^{2n}\}$.

Then $R=\{(a_iy, b_iy, c_iy, d_iy) : 0 \le i \le n-1, y \in C_0^{4n}\}$ *forms an initial round of a Z-cyclic DTWh*(p).

Proof It is easy to check that the following identities are satisfied:

$$\bigcup_{i=0}^{n-1}\{a_i, b_i, c_i, d_i\}\cdot C_0^{4n} = Z_p\setminus\{0\};$$
$$\bigcup_{i=0}^{n-1}\{\pm(a_i-b_i), \pm(c_i-d_i)\}\cdot C_0^{4n} = Z_p\setminus\{0\};$$
$$\bigcup_{i=0}^{n-1}\{\pm(a_i-c_i), \pm(b_i-d_i)\}\cdot C_0^{4n} = Z_p\setminus\{0\};$$
$$\bigcup_{i=0}^{n-1}\{\pm(a_i-d_i), \pm(b_i-c_i)\}\cdot C_0^{4n} = Z_p\setminus\{0\};$$
$$\bigcup_{i=0}^{n-1}\{b_i-a_i, c_i-b_i, d_i-c_i, a_i-d_i\}\cdot C_0^{4n} = Z_p\setminus\{0\}.$$

The assertion then follows. □

The basic idea is to add some additional conditions to make the above initial round in Lemma 2.1 satisfy the three-person property. The following notations are useful for checking this, which can be found in [18,22,33].

Let G be an abelian group, and a, b, c be pairwise distinct elements of G. Let $O(a,b,c) = \{\{a+g, b+g, c+g\} : g \in G\}$, which is called the *orbit* of $\{a,b,c\}$ under the action of G. The notation

$$G(a,b,c) = \{\{b-a, c-a\}, \{a-b, c-b\}, \{a-c, b-c\}\}$$

is called a *generating set* for $O(a,b,c)$, and clearly $G(a,b,c)$ is invariant under the action of G. That is, $G(a,b,c) = G(a+g, b+g, c+g)$, for any $g \in G$. If the order of G is a prime p, $p \neq 3$, then the length of the orbit $O(a,b,c)$ equals p. It is easy to see that two sets $G(a,b,c)$ and $G(a',b',c')$ are equal if and only if their intersection is not empty.

Lemma 2.2 ([18]) $O(a,b,c)\cap O(a',b',c') = \emptyset$ *if and only if* $G(a,b,c) \neq G(a',b',c')$.

By Lemma 2.2, we need to check that all the generating sets in the initial round are pairwise distinct.

Lemma 2.3 ([18]) *Let* $p \equiv 1 \pmod 4$ *be a prime. Suppose that* n *is an integer such that* $4n|(p-1)$ *and* $-1 \in C_{2n}^{4n}$. *Let* $a, b, c \in Z_p$ *be pairwise distinct. If* $a^2+b^2+c^2 \neq ab+bc+ac$, *then* $G(a,b,c) \neq G(ay, by, cy)$ *for any* $y \in C_0^{4n}\setminus\{1\}$.

Let $e(g) = i$ if $g \in C_i^{4n}$. Define $E(a,b,c) = \{\{e(b-a), e(c-a)\}, \{e(a-b), e(c-b)\}, \{e(a-c), e(b-c)\}\}$. We have the following lemma.

Lemma 2.4 ([18]) *Let* $p \equiv 1 \pmod 4$ *be a prime. Suppose that* n *is an integer such that* $4n|(p-1)$. *Suppose also that* $\{a,b,c\}$ *and* $\{e,f,g\}$ *are two distinct triples. If* $E(a,b,c) \neq E(e,f,g)$, *then* $G(ay, by, cy) \neq G(ey', fy', gy')$ *for any* $y, y' \in C_0^{4n}$.

Particularly, if $\{a, b, c\} \cup \{e, f, g\} = \{a, b, c, d\}$, the requirement $E(a, b, c) \neq E(e, f, g)$ in Lemma 2.4 can be relaxed. We say the element a in $\{a, b, c, d\}$ satisfies property $\mathcal{P}$ if

$$(b-a)^2 \not\equiv (c-a)(d-a) \pmod{p},$$
$$(c-a)^2 \not\equiv (b-a)(d-a) \pmod{p},$$
$$(d-a)^2 \not\equiv (b-a)(c-a) \pmod{p}.$$

If each element of the quadruple $\{a, b, c, d\}$ satisfies property $\mathcal{P}$, we say that the quadruple $\{a, b, c, d\}$ has property $\mathcal{P}$.

Lemma 2.5 *Let $p \equiv 1 \pmod 4$ be a prime. Suppose that n is an integer such that $4n|(p-1)$ and $-1 \in C_{2n}^{4n}$. Suppose also that (a, b, c, d) is a game from the initial round in Lemma 2.1. If $\{a, b, c, d\}$ has property $\mathcal{P}$, then the four generating sets $G(ay, by, cy)$, $G(ay', by', dy')$, $G(ay'', cy'', dy'')$ and $G(by''', cy''', dy''')$ are pairwise distinct for any $y, y', y'', y''' \in C_0^{4n}$.*

Proof We only prove the case for $G(ay, by, cy) \neq G(ay', by', dy')$ for any $y, y' \in C_0^{4n}$. For the other cases, the proof can be similarly done. Here, $G(ay, by, cy) = \{\{(b-a)y, (c-a)y\}, \{(a-b)y, (c-b)y\}, \{(a-c)y, (b-c)y\}\}$, and $G(ay', by', dy') = \{\{(b-a)y', (d-a)y'\}, \{(a-b)y', (d-b)y'\}, \{(a-d)y', (b-d)y'\}\}$. The proof is separated into the following three parts:

Suppose $\{(b-a)y, (c-a)y\} = \{(b-a)y', (d-a)y'\}$. If $y \neq y'$, then $(b-a)y \neq (b-a)y'$. Otherwise, $(c-a)y \neq (d-a)y'$ since $c-a \neq d-a$. Hence, we have $(b-a)y = (d-a)y'$ and $(c-a)y = (b-a)y'$. Combining these two identities, we obtain $(b-a)^2yy' = (c-a)(d-a)yy'$, i.e., $(b-a)^2 = (c-a)(d-a)$, which contradicts the fact that $\{a, b, c, d\}$ has the property $\mathcal{P}$.

Suppose $\{(b-a)y, (c-a)y\} = \{(a-b)y', (d-b)y'\}$. Since $-1 \in C_{2n}^{4n}$, we have $(b-a)y \neq (a-b)y'$. Then $(b-a)y = (d-b)y'$ and $(c-a)y = (a-b)y'$. Combining these two identities, we obtain $(c-b)y = (a-d)y'$, which contradicts Condition (1) in Lemma 2.1.

Suppose $\{(b-a)y, (c-a)y\} = \{(a-d)y', (b-d)y'\}$. By Condition (1) in Lemma 2.1, we have $(b-a)y \neq (a-d)y'$. Then $(b-a)y = (b-d)y'$ and $(c-a)y = (a-d)y'$. Combining these two identities, we obtain $(b-c)y = (b-a)y'$. Hence, $(a-b)^2yy' = (c-b)(d-b)yy'$, i.e., $(a-b)^2 = (c-b)(d-b)$, which contradicts the fact that $\{a, b, c, d\}$ has the property $\mathcal{P}$. □

Combining Lemmas 2.2–2.5, we have the following.

Lemma 2.6 *Let $p \equiv 1 \pmod 4$ be a prime. Suppose that n is an integer such that $4n|(p-1)$ and $-1 \in C_{2n}^{4n}$. Suppose also that $\{(a_i, b_i, c_i, d_i) : 0 \leq i \leq n-1\}$ is a set of quadruples over Z_p^* satisfying Conditions (1)–(2) in Lemma 2.1. Furthermore, suppose we have the following:*

(3) *each triple $\{a, b, c\} \subset \{a_i, b_i, c_i, d_i\}$, $0 \leq i \leq n-1$ satisfies the condition $a^2+b^2+c^2 \neq ab+bc+ac$;*
(4) *each quadruple $\{a_i, b_i, c_i, d_i\}$, $0 \leq i \leq n-1$ has property $\mathcal{P}$;*
(5) *if $n \geq 2$, then any two distinct triples $\{a, b, c\} \subset \{a_i, b_i, c_i, d_i\}$, $\{e, f, g\} \subset \{a_{i'}, b_{i'}, c_{i'}, d_{i'}\}$, satisfy the condition $E(a, b, c) \neq E(e, f, g)$, where $0 \leq i < i' \leq n-1$.*

Then $R = \{(a_i y, b_i y, c_i y, d_i y) : 0 \leq i \leq n-1, y \in C_0^{4n}\}$ forms an initial round of a Z-cyclic 3PDTWh(p).

To construct the initial round of a Z-cyclic 3PDTWh(p) with prime $p \equiv 1 \pmod 4$, we need to find a set of quadruples satisfying Conditions (1)–(5) in Lemmas 2.1 and 2.6 simultaneously. These conditions serve as the basic criteria for the existence of a Z-cyclic 3PDTWh(p) in our paper. In Sects. 3, 4, 5, we consider the constructions of three classes of Z-cyclic 3PDTWh(p)s for $p \equiv 5 \pmod 8$, $p \equiv 9 \pmod{16}$ and $p \equiv 1 \pmod{16}$ respectively. We will employ Weil's theorem as our main tool, which has been used extensively in the construction of other combinatorial objects, such as difference families [17], TWhs [12] and OOCs [14].

3 Existence of Z-cyclic 3PDTWh(p)s for prime $p \equiv 5 \pmod 8$

In this section, we investigate the existence of a Z-cyclic 3PDTWh(p) for any prime $p \equiv 5 \pmod 8$.

Lemma 3.1 *Let $p \equiv 5 \pmod 8$ be a prime. If there exists a quadruple (a, b, c, d) satisfying the following properties:*

(1) $\{a, b, c, d\}$ *is a representative system of the coset classes* $\{C_0^4, C_1^4, C_2^4, C_3^4\}$,
(2) $b - a \in C_0^4,\ c - b \in C_1^4,\ d - c \in C_3^4,\ a - d \in C_2^4,\ a - c \in C_0^4,\ b - d \in C_3^4$,
(3) $(c - a)^2 \not\equiv (b - a)(d - a) \pmod p,\ (a - d)^2 \not\equiv (b - d)(c - d) \pmod p$,

then $R = \{(ay, by, cy, dy) : y \in C_0^4\}$ forms an initial round of a Z-cyclic 3PDTWh(p).

Proof Since $p \equiv 5 \pmod 8$, we have $-1 \in C_2^4$. According to the hypothesis, it is easy to see that the quadruple (a, b, c, d) satisfies Conditions (1)–(2) of Lemma 2.1 with $n = 1$, and thus $R = \{(ay, by, cy, dy) : y \in C_0^4\}$ forms an initial round of a Z-cyclic DTWh(p). Now, we need only to check this Z-cyclic DTWh(p) satisfies the three-person property, namely, (a, b, c, d) satisfies Conditions (3)–(4) in Lemma 2.6.

For Condition (3) in Lemma 2.6, note that the expression $a^2 + b^2 + c^2 = ab + bc + ac$ is equivalent to $(a - c)^2 = (a - b)(b - c)$. Since $a - c \in C_0^4$, $a - b \in C_2^4$ and $b - c \in C_3^4$, we have $(a - c)^2 \neq (a - b)(b - c)$, i.e., $a^2 + b^2 + c^2 \neq ab + bc + ac$. Hence, the triple $\{a, b, c\}$ in $\{a, b, c, d\}$ satisfies the requirement of Condition (3). The other triples in $\{a, b, c, d\}$ can be checked similarly.

For Condition (4) in Lemma 2.6, we need to check that each element in $\{a, b, c, d\}$ satisfies property $\mathcal{P}$, that is, besides $(c - a)^2 \not\equiv (b - a)(d - a) \pmod p$ and $(a - d)^2 \not\equiv (b - d)(c - d) \pmod p$, ten other modular inequalities should also be satisfied. Here, we need only to do the routine check, which can be done similar to that for Condition (3). □

Lemma 3.1 enables us to use Weil's theorem to solve the existence of Z-cyclic 3PDTWh(p)s for large $p \equiv 5 \pmod 8$. Here is Weil's theorem on multiplicative character sums, which can be found in [32].

Theorem 3.2 ([32]) *Let ψ be a multiplicative character of $GF(q)$ of order $m > 1$ and let $f \in GF(q)[x]$ be a monic polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over $GF(q)$, then for every $a \in GF(q)$ we have*

$$\left| \sum_{c \in GF(q)} \psi(af(c)) \right| \leq (d - 1)\sqrt{q}.$$

Table 1 (p, c, d)

(269, 65, 259), (277, 268, 242), (293, 68, 173), (317, 95, 50), (349, 4, 246), (373, 4, 47), (389, 45, 273), (397, 43, 274), (421, 45, 280), (461, 54, 398), (509, 5, 15), (541, 235, 67), (557, 25, 128), (613, 4, 132), (653, 64, 37), (661, 4, 39), (677, 164, 366), (701, 5, 432), (709, 34, 56), (733, 41, 23), (757, 156, 31), (773, 61, 80), (797, 25, 116), (821, 5, 74), (829, 65, 304), (853, 4, 299), (877, 4, 542), (941, 70, 444), (997, 4, 188).

As an application of Weil's theorem, we quote a result which can be found in [13,14].

Theorem 3.3 ([14]) *Let $p \equiv 1 \ (mod\ q)$ be a prime satisfying the inequality*

$$p - \left[\sum_{i=0}^{s-2} \binom{s}{i}(s-i-1)(q-1)^{s-i}\right]\sqrt{p} - sq^{s-1} > 0.$$

Then, for any given s-tuple $(j_1, j_2, \ldots, j_s) \in \{0, 1, \ldots, q-1\}^s$ and any given s-tuple $(c_1, c_2, \ldots, c_s)$ of pairwise distinct elements of Z_p, there exists an element $x \in Z_p$ such that $x + c_i \in C_{j_i}^q$ for each i.

Lemma 3.4 *Let $p \equiv 5 \ (mod\ 8)$ be a prime. Then there exists an ordered quadruple $(a, b, c, d) \in Z_p^4$ for each $p > 241$ satisfying Conditions* (1)–(3) *of Lemma* 3.1.

Proof Since $p \equiv 5 \pmod 8$, 2 is a non-square element. Let $2 \in C_{i_0}^4$, then $i_0 = 1$ or 3. Without loss of generality, let $a = 1,\ b = 2$, then $b - a = 1 \in C_0^4$. If Conditions (1)–(2) of Lemma 3.1 are satisfied, then $c(c-2) \not\equiv d - 2 \pmod p$ and $(2-d)c \not\equiv 1 \pmod p$, i.e., $(c-a)^2 \not\equiv (b-a)(d-a) \pmod p$, $(a-d)^2 \not\equiv (b-d)(c-d) \pmod p$, Condition (3) is satisfied. Hence, we need only to prove that there exist two elements $c,\ d$ such that $c \in C_2^4,\ c-1 \in C_2^4,\ c-2 \in C_1^4,\ d \in C_{i_0+2}^4,\ d-1 \in C_0^4,\ d-2 \in C_1^4$ and $d - c \in C_3^4$.

Since $0,\ 1,\ 2$ are distinct elements in Z_p, we can apply Theorem 3.3 with $q = 4,\ s = 3$. Then, for any given prime $p \equiv 5 \pmod 8$ and $p \geq 6661$, there always exists an element c in Z_p satisfying $c \in C_2^4,\ c - 1 \in C_2^4$ and $c - 2 \in C_1^4$. Obviously, $c \neq 0,\ 1,\ 2$. Once the element c is determined, we can apply Theorem 3.3 again with $p \geq 263821,\ q = 4,\ s = 4$ to obtain the required element d.

For the remaining values of $p \equiv 5 \pmod 8$, $241 < p \leq 263821$, a computer search shows that the desired c's and d's all exist. To save space we only list the small primes up to 997 in Table 1. For the other values of p with $997 < p < 263821$, the interested reader may get a copy from the authors. □

Lemma 3.5 *There exists a Z-cyclic 3PDTWh(p) for any prime $p \equiv 5 \ (mod\ 8)$.*

Proof Combining Lemmas 1.8, 3.1 and 3.4, the conclusion then follows. □

4 Existence of Z-cyclic 3PDTWh(p)s for prime $p \equiv 9 \pmod{16}$

In this section, we investigate the existence of a Z-cyclic 3PDTWh(p) for any prime $p \equiv 9 \pmod{16}$.

Lemma 4.1 *Let $p \equiv 9 \pmod{16}$ be a prime. If there exist two quadruples (a, b, c, d) and (e, f, g, h) satisfying the following properties:*

(1) *$\{a, b, c, d, e, f, g, h\}$ is a representative system of the coset classes $\{C_0^8, C_1^8, \ldots, C_7^8\}$;*
(2) *$b-a \in C_0^8$, $c-b \in C_4^8$, $d-c \in C_1^8$, $a-d \in C_5^8$, $a-c \in C_0^8$, $b-d \in C_2^8$, $f-e \in C_2^8$, $g-f \in C_6^8$, $h-g \in C_3^8$, $e-h \in C_7^8$, $e-g \in C_3^8$, $f-h \in C_1^8$,*

then $R = \{(ay, by, cy, dy) : y \in C_0^8\} \cup \{(ey, fy, gy, hy) : y \in C_0^8\}$ forms an initial round of a Z-cyclic 3PDTWh(p).

Proof Since $p \equiv 9 \pmod{16}$, we have $-1 \in C_4^8$. According to the hypothesis, it is easy to see that the quadruples (a, b, c, d) and (e, f, g, h) satisfy Conditions (1)–(2) of Lemma 2.1 with $n = 2$, and thus $R = \{(ay, by, cy, dy) : y \in C_0^8\} \cup \{(ey, fy, gy, hy) : y \in C_0^8\}$ forms an initial round of a Z-cyclic DTWh(p). Now, we need only to check this Z-cyclic DTWh(p) satisfies the three-person property, that is (a, b, c, d) and (e, f, g, h) satisfy Conditions (3)–(5) in Lemma 2.6.

For Conditions (3)–(4), the proof is similar to that of Lemma 3.1.

For Condition (5), the eight sets $E(a, b, c)$, $E(a, b, d)$, $E(a, c, d)$, $E(b, c, d)$ and $E(e, f, g), E(e, f, h), E(e, g, h), E(f, g, h)$ of the two quadruples (a, b, c, d) and (e, f, g, h) are listed in the following two columns:

$$\begin{array}{ll} \{\{0,4\},\{4,4\},\{0,0\}\}, & \{\{2,7\},\{6,6\},\{3,2\}\}, \\ \{\{0,1\},\{4,6\},\{5,2\}\}, & \{\{2,3\},\{6,5\},\{7,1\}\}, \\ \{\{4,1\},\{0,1\},\{5,5\}\}, & \{\{7,3\},\{3,3\},\{7,7\}\}, \\ \{\{4,6\},\{0,1\},\{2,5\}\}, & \{\{6,5\},\{2,3\},\{1,7\}\}. \end{array}$$

It is easy to see that there do not exist two identical sets from the two different columns. □

Lemma 4.2 *Let $p \equiv 9 \pmod{16}$ be a prime. Suppose there are two different elements a, x in $GF(p)^*$ satisfying the following conditions:*

(1) *$a \in C_2^8$, $a-1 \in C_4^8$ and $a+1 \in C_4^8$,*
(2) *$x \in C_s^8$, $x-1 \in C_i^8$, $x+1 \in C_l^8$, $x-a \in C_j^8$ and $x+a \in C_k^8$, where $s \in \{1, 3, 5, 7\}$, $i-l \equiv 4 \pmod{8}$, $j-k \equiv 4 \pmod{8}$ and $i-j \equiv 1 \pmod{2}$,*
(3) *each triple $\{a, b, c\}$ in $\{1, x, a, -x\}$ or $\{ax, a^2, -ax, -a\}$ satisfies the condition $a^2 + b^2 + c^2 \neq ab + bc + ac$,*
(4) *both of the quadruples $\{1, x, a, -x\}$ and $\{ax, a^2, -ax, -a\}$ have property $\mathcal{P}$.*

Then $R = \{(y, xy, ay, -xy) : y \in C_0^8\} \cup \{(axy, a^2y, -axy, -ay) : y \in C_0^8\}$ forms an initial round of a Z-cyclic 3PDTWh(p).

Proof Since $p \equiv 9 \pmod{16}$, we have $-1 \in C_4^8$ and 2 is a quadratic residue. Let $2 \in C_t^8$, where $t \in \{0, 2, 4, 6\}$. Let $(a_1, b_1, c_1, d_1) = (1, x, a, -x)$ and $(a_2, b_2, c_2, d_2) = (ax, a^2, -ax, -a)$. Then we have $a_1 \in C_0^8$, $b_1 \in C_s^8$, $c_1 \in C_2^8$, $d_1 \in C_{s+4}^8$, $a_2 \in C_{s+2}^8$, $b_2 \in C_4^8$, $c_2 \in C_{s+6}^8$ and $d_2 \in C_6^8$. Furthermore, we have $b_1 - a_1 = x - 1 \in C_i^8$, $c_1 - b_1 = a - x \in C_{j+4}^8$, $d_1 - c_1 = -x - a \in C_{k+4}^8$, $a_1 - d_1 = 1 + x \in C_l^8$, $a_1 - c_1 = 1 - a \in C_0^8$, $b_1 - d_1 = 2x \in C_{s+t}^8$, $b_2 - a_2 = a(a - x) \in C_{j+6}^8$, $c_2 - b_2 = -a(x + a) \in C_{k+6}^8$, $d_2 - c_2 = a(x-1) \in C_{i+2}^8$, $a_2 - d_2 = a(1+x) \in C_{l+2}^8$, $a_2 - c_2 = 2ax \in C_{s+t+2}^8$ and $b_2 - d_2 = a(a+1) \in C_6^8$. It is easily checked that Conditions (1)–(2) of Lemma 2.1 with $n = 2$ are satisfied. Thus $R = \{(y, xy, ay, -xy) : y \in C_0^8\} \cup \{(axy, a^2y, -axy, -ay) : y \in C_0^8\}$ forms an initial round of a Z-cyclic DTWh(p). We still need to check that this Z-cyclic DTWh(p) has the three-person property.

Conditions (3)–(4) in Lemma 2.6 can be easily checked. Thus we need only to check Condition (5) in Lemma 2.6. The eight sets $E(a_1, b_1, c_1)$, $E(a_1, b_1, d_1)$, $E(a_1, c_1, d_1)$, $E(b_1, c_1, d_1)$ and $E(a_2, b_2, c_2)$, $E(a_2, b_2, d_2)$, $E(a_2, c_2, d_2)$, $E(b_2, c_2, d_2)$ of the two quadruples (a_1, b_1, c_1, d_1) and (a_2, b_2, c_2, d_2) are listed in the following two columns:

$$\begin{array}{ll}
\{\{i,4\},\{i+4,j+4\},\{0,j\}\}, & \{\{j+6,s+t+6\},\{j+2,k+6\},\{s+t+2,k+2\}\},\\
\{\{i,l+4\},\{i+4,s+t+4\},\{l,s+t\}\}, & \{\{j+6,l+6\},\{j+2,2\},\{l+2,6\}\},\\
\{\{4,l+4\},\{0,k+4\},\{l,k\}\}, & \{\{s+t+6,l+6\},\{s+t+2,i+2\},\{l+2,i+6\}\},\\
\{\{j+4,s+t+4\},\{j,k+4\},\{s+t,k\}\}, & \{\{k+6,2\},\{k+2,i+2\},\{6,i+6\}\}.
\end{array}$$

Based on the modular equations i, j, k, l satisfied and the fact that $s \in \{1, 3, 5, 7\}$ and $t \in \{0, 2, 4, 6\}$, we can show that any two sets from the above two different columns are distinct. Take the two sets $\{\{i, 4\}, \{i + 4, j + 4\}, \{0, j\}\}$ and $\{\{j + 6, s + t + 6\}, \{j + 2, k + 6\}, \{s + t + 2, k + 2\}\}$ as an example. First, suppose $\{i, 4\} = \{j + 6, s + t + 6\}$, then $i = s + t + 6$, since $s + t + 2$ is odd. Hence, $j + 6 = 4$, which means both j and k are even. Consequently, we have $\{i + 4, j + 4\} = \{s + t + 2, k + 2\}$. This leads to $j + 4 = k + 2$ which contradicts $j - k \equiv 4 \pmod 8$. Next, suppose $\{i, 4\} = \{j + 2, k + 6\}$, it is not true because $i - j \equiv 1 \pmod 2$ and $j - k \equiv 4 \pmod 8$. Finally, suppose $\{i, 4\} = \{s + t + 2, k + 2\}$, then we have $i = s + t + 2$, since $s + t + 2$ is odd. Hence, $k + 2 = 4$, which means both j and k are even. Consequently, $\{i + 4, j + 4\}$ should be equal to $\{j + 6, s + t + 6\}$. This leads to $j + 4 = j + 6$, which leads to a contradiction. Hence, $\{\{i, 4\}, \{i + 4, j + 4\}, \{0, j\}\}$ is not equal to $\{\{j + 6, s + t + 6\}, \{j + 2, k + 6\}, \{s + t + 2, k + 2\}\}$. The proofs for other pairs of sets from the above two different columns can be similarly done. □

Lemma 4.3 *Let $p \equiv 9$ (mod 16) be a prime and $p \geq 816169$. Then there exists a Z-cyclic 3PDTWh(p).*

Proof Applying Theorem 3.3 with $q = 8$, $s = 3$, we always have that there exists an element a in Z_p satisfying $a \in C_2^8$, $a - 1 \in C_4^8$ and $a + 1 \in C_4^8$ for any prime $p \equiv 9 \pmod{16}$ and $p \geq 694313$. Obviously, $a \neq 0,\ 1,\ -1$. Once the element a is determined, we still need to find an element x satisfying Conditions (2)–(4) in Lemma 4.2. Let

$$g_1(x) = x,\ g_2(x) = (x-1)(x-a),$$
$$g_3(x) = (x+1)(x-1)^3(x-a)^4,\ g_4(x) = (x+a)(x-1)^4(x-a)^3.$$

Since there are in total of 32 inequalities of degree 2 concerning the variable x in Conditions (3)–(4) in Lemma 4.2, it is easy to see that the requirements for Conditions (2)–(4) of Lemma 4.2 can be satisfied if there exist at least 65 different elements x satisfying the following conditions:

(i) for $k = 1, 2$, $g_k(x) \in C_1^8 \cup C_3^8 \cup C_5^8 \cup C_7^8$,

(ii) for $k = 3, 4$, $g_k(x) \in C_0^8$.

Let χ be a non-principal multiplicative character of order 8. That is $\chi(x) = \theta^t$ if $x \in C_t^8$ where $\theta = e^{\frac{2\pi i}{8}}$ is the 8-th root of unity. Let

$$A_k = \chi(g_k(x)),\ k = 1, 2, 3, 4.$$

Then, we have the following functions:
For $k = 1, 2$,

$$1 - A_k^4 = \begin{cases} 2, & g_k(x) \in C_1^8 \cup C_3^8 \cup C_5^8 \cup C_7^8, \\ 1, & g_k(x) = 0, \\ 0, & g_k(x) \notin \{0\} \cup C_1^8 \cup C_3^8 \cup C_5^8 \cup C_7^8. \end{cases}$$

For $k = 3, 4$,

$$1 + A_k + A_k^2 + \ldots + A_k^7 = \begin{cases} 8, & g_k(x) \in C_0^8, \\ 1, & g_k(x) = 0, \\ 0, & g_k(x) \notin \{0\} \cup C_0^8. \end{cases}$$

From these, let

$$S(x) = \left(1 - A_1^4\right)\left(1 - A_2^4\right)\left(1 + A_3 + A_3^2 + \ldots + A_3^7\right)\left(1 + A_4 + A_4^2 + \ldots + A_4^7\right)$$

and

$$S = \sum_{x \in GF(p)} S(x). \tag{1}$$

Let $X \subset GF(p)$ such that $S(x) \neq 0$ for any $x \in X$. Denote $X_1 = \{x \in X : g_1(x)g_2(x)g_3(x)g_4(x) = 0\}$ and $X_2 = X \setminus X_1$. Then, x satisfies the above Conditions (i)–(ii) if $x \in X_2$. Consider the sum $|S|$.

$$|S| \leq \sum_{x \in X_1} |S(x)| + \sum_{x \in X_2} |S(x)|.$$

Denote $\sum_{x \in X_1} |S(x)|$ as S_1. If $g_1(x) = x = 0$, then $g_2(x) = a \in C_2^8$, thus $1 - A_2^4 = 0$, the contribution to S_1 is 0. If $x \neq 0$ and $g_2(x) = (x-1)(x-a) = 0$, then $x = 1 \in C_0^8$ or $x = a \in C_2^8$, thus $1 - A_1^4 = 0$, the contribution to S_1 is 0. If $x \neq 0, 1, a$ and $g_3(x) = (x+1)(x-1)^3(x-a)^4 = 0$, then $x = -1 \in C_4^8$, thus $1 - A_1^4 = 0$, the contribution to S_1 is 0. If $x \neq 0, 1, -1, a$ and $g_4(x) = (x+a)(x-1)^4(x-a)^3$, then $x = -a \in C_6^8$, thus $1 - A_1^4 = 0$, the contribution to S_1 is 0. So, the contribution to S_1 is 0 for any $x \in X_1$. Then $|S| = \sum_{x \in X_2} |S(x)| = 2 \times 2 \times 8 \times 8 \times n = 256 \times n$ where $n = |X_2|$, i.e., the number of elements satisfying Conditions (i)–(ii).

Expanding the inner product in Eq. 1 we obtain

$$\begin{aligned} |S| \geq \sum_{x \in GF(p)} 1 - \left|\sum_{x \in GF(p)} A_1^4\right| - \left|\sum_{x \in GF(p)} A_2^4\right| - \left|\sum_{x \in GF(p)} A_1^4 A_2^4\right| \\ - \sum_{0 \leq r_2 \leq 1} \sum_{\substack{r_3 + r_4 > 0 \\ 0 \leq r_3, r_4 \leq 7}} \left|\sum_{x \in GF(p)} A_2^{4r_2} A_3^{r_3} A_4^{r_4}\right| - \sum_{0 \leq r_2 \leq 1} \sum_{\substack{r_3 + r_4 > 0 \\ 0 \leq r_3, r_4 \leq 7}} \left|\sum_{x \in GF(p)} A_1^4 A_2^{4r_2} A_3^{r_3} A_4^{r_4}\right|. \end{aligned} \tag{2}$$

In order to estimate the inner sums, we may use Weil's theorem on multiplicative character sums.

Suppose that $\chi(G(x)) = A_1^{4r_1} A_2^{4r_2} A_3^{r_3} A_4^{r_4}$, where $0 \leq r_1, r_2 \leq 1$, $0 \leq r_3, r_4 \leq 7$ and $r_2 + r_3 + r_4 > 0$. Then

$$G(x) = x^{4r_1}(x+1)^{r_3}(x-1)^{4r_2+3r_3+4r_4}(x+a)^{r_4}(x-a)^{4r_2+4r_3+3r_4}.$$

If there is a polynomial $P(x)$ such that $G(x) = [P(x)]^8$, then we have

$$x^{4r_1}(x+1)^{r_3}(x-1)^{4r_2+3r_3+4r_4}(x+a)^{r_4}(x-a)^{4r_2+4r_3+3r_4} = [P(x)]^8.$$

Since $x, x+1, x-1, x+a$ and $x-a$ are pairwise co-prime, then $r_1 \equiv r_2 \equiv 0 \pmod 2$, $r_3 \equiv r_4 \equiv 0 \pmod 8$. Hence, $r_1 = r_2 = r_3 = r_4 = 0$, which leads to a contradiction to

$r_2 + r_3 + r_4 > 0$. By Theorem 3.2, we have

$$\begin{cases} \left|\sum_{x\in GF(p)} A_1^4\right| \le 0, \\ \left|\sum_{x\in GF(p)} A_2^4\right| \le \sqrt{p}, \\ \left|\sum_{x\in GF(p)} A_1^4 A_2^4\right| \le 2\sqrt{p}, \\ \left|\sum_{x\in GF(p)} A_2^{4r_2} A_3^{r_3} A_4^{r_4}\right| \le 3\sqrt{p}, \\ \left|\sum_{x\in GF(p)} A_1^4 A_2^{4r_2} A_3^{r_3} A_4^{r_4}\right| \le 4\sqrt{p}. \end{cases}$$

Then

$$\begin{aligned} |S| &\ge p - \sqrt{p} - 2\sqrt{p} - \sum_{0\le r_2\le 1} \sum_{\substack{r_3+r_4>0 \\ 0\le r_3,r_4\le 7}} 3\sqrt{p} - \sum_{0\le r_2\le 1} \sum_{\substack{r_3+r_4>0 \\ 0\le r_3,r_4\le 7}} 4\sqrt{p} \\ &= p - 885\sqrt{p}. \end{aligned} \tag{3}$$

If $p - 885\sqrt{p} \ge 256 \times 65$, namely, $p \ge 816169$, we have $n \ge 65$. The proof is complete. □

Lemma 4.4 *Let $p \equiv 9$ (mod 16) be a prime and $241 < p < 816169$. Then there exists a Z-cyclic 3PDTWh(p).*

Proof For each given prime $p \equiv 9$ (mod 16) and $241 < p < 816169$, we find two quadruples (a, b, c, d) and (e, f, g, h) satisfying requirements in Lemma 4.1 by a computer search. Here, we just list the required quadruples (a, b, c, d) and (e, f, g, h) for $241 < p \le 1033$ in Table 2. For the other primes, the interested reader can get a copy from the authors. □

Table 2

p	(a,b,c,d), (e,f,g,h)	p	(a,b,c,d), (e,f,g,h)
281	(1, 2, 120, 74), (5, 19, 52, 225)	313	(1, 4, 37, 155), (8, 43, 67, 90)
409	(1, 2, 47, 94), (3, 124, 260, 45)	457	(1, 2, 8, 316), (5, 30, 290, 172)
521	(1, 2, 82, 4), (3, 65, 184, 217)	569	(1, 2, 171, 4), (3, 12, 381, 533)
601	(1, 5, 200, 214), (7, 105, 523, 396)	617	(1, 2, 168, 307), (6, 21, 60, 487)
761	(1, 2, 79, 477), (3, 69, 249, 166)	809	(1, 2, 20, 68), (3, 17, 188, 282)
857	(1, 2, 59, 392), (3, 28, 229, 773)	937	(1, 3, 30, 168), (5, 111, 769, 178)
953	(1, 2, 128, 4), (3, 11, 551, 286)	1033	(1, 2, 10, 406), (3, 27, 95, 413)

Lemma 4.5 *Let $p \equiv 9$ (mod 16) be a prime and $p \ge 41$. Then there exists a Z-cyclic 3PDTWh(p).*

Proof Combining Lemmas 1.8 and 4.3–4.4, the conclusion then follows. □

5 Existence of Z-cyclic 3PDTWh(p)s for prime $p \equiv 1 \pmod{16}$

In this section, we shall extend the useful construction displayed in [4, Example 6.4], which can be regarded as a special case of Lemma 2.1.

Let $p = 2^k t + 1$ be a prime and θ be a primitive root of Z_p, where $k \geq 3$, t odd and $t \geq 3$. The quadruples

$$(1, \theta, -\theta, \theta^{1+\alpha}) \times \theta^{4nj+2i} \quad (0 \leq j \leq t-1, 0 \leq i \leq n-1)$$

where $n = 2^{k-2}$, form an initial round of a Z-cyclic TWh(p) provided

(a) $\alpha \equiv 2^{k-1} - 1 \pmod{2^k}$,
(b) $\theta^{\alpha+1} - 1 = \square$,
(c) $(\theta + 1)(\theta^\alpha - 1) = \square$,
(d) $(\theta - 1)(\theta^\alpha + 1) = \square$.

Furthermore, if the following conditions can be satisfied

(e) $\dfrac{2\theta}{\theta - 1} \in C_0^{4n}$ and $\dfrac{\theta^{1+\alpha} - 1}{\theta(\theta^\alpha + 1)} \in C_0^{4n}$, or
(e') $\dfrac{2\theta}{\theta(\theta^\alpha + 1)} \in C_0^{4n}$ and $\dfrac{\theta^{1+\alpha} - 1}{\theta - 1} \in C_0^{4n}$, then we have the following lemma.

Lemma 5.1 *Let $p = 2^k t + 1$ be a prime, where $k \geq 3$, t odd and $t \geq 3$. θ and α are defined as above satisfying Conditions (a)–(d) and (e) (or (e′)). Then*

$$R = \{(1, \theta, -\theta, \theta^{1+\alpha}) \times \theta^{4nj+2i} : 0 \leq j \leq t-1, 0 \leq i \leq n-1\}$$

where $n = 2^{k-2}$, forms an initial round of a Z-cyclic DTWh(p).

Proof Let $a_i = \theta^{2i}$, $b_i = \theta^{2i+1}$, $c_i = -\theta^{2i+1}$ and $d_i = \theta^{2i+1+\alpha}$, where $0 \leq i \leq n-1$. Since $p = 2^k t + 1$, $k \geq 3$, t odd, $t \geq 3$, $-1 \in C_{2n}^{4n}$ and ± 2 are quadratic residues, the set of quadruples

$$\{(a_i, b_i, c_i, d_i) : 0 \leq i \leq n-1\}$$

satisfies Conditions (1)–(2) of Lemma 2.1, i.e., R forms an initial round of a Z-cyclic DTWh(p). □

In addition, we need more requirements to ensure the above Z-cyclic DTWh(p) satisfies the three-person property. First, we notice that Lemma 2.3 can be easily extended to the following:

Lemma 5.2 *Let $p = 2^k t + 1$ be a prime, where $k \geq 3$, t odd and $t \geq 3$. If $a^2 + b^2 + c^2 \neq ab + bc + ac$, then $G(a, b, c) \neq G(a, b, c) \times \theta^{4nj+2i}$, where $0 \leq i \leq n-1$, $0 \leq j \leq t-1$, $i^2 + j^2 \neq 0$ and $n = 2^{k-2}$.*

Proof The proof is similar to that of [18, Lemma 3.1]. Define $f(a, b, c) = 2[(a-b)^2 + (a-c)^2 + (b-c)^2]$. If $G(a, b, c) = G(a, b, c) \times \theta^{4nj+2i}$, where $0 \leq i \leq n-1$, $0 \leq j \leq t-1$, then $f(a, b, c) = f((a, b, c) \times \theta^{4nj+2i})$. So $4(1-\theta^{8nj+4i})(a^2+b^2+c^2-ab-bc-ac) = 0$. Thus we have $1 = \theta^{8nj+4i}$, which contradicts the fact that $0 \leq i \leq n-1$, $0 \leq j \leq t-1$ and $n = 2^{k-2}$. □

Lemma 5.3 *If* $\{a, b, c\}$ *and* $\{e, f, g\}$ *are different subsets of* $\{1, \theta, -\theta, \theta^{1+\alpha}\}$, *where* θ *and* α *satisfy Conditions* (a)–(d) *and* (e) *(or* (e')*), then* $G(a, b, c) \neq G(e, f, g) \times \theta^{4nj+2i}$, *where* $0 < i \leq n-1,\ 0 \leq j \leq t-1$ *and* $n = 2^{k-2}$.

Proof To save space, we only take the case of $\{a, b, c\} = \{1, \theta, -\theta\}$ and $\{e, f, g\} = \{\theta, -\theta, \theta^{1+\alpha}\}$ as an example. For the other cases, the proof can be similarly done. Here, $G(1, \theta, -\theta) = \{\{\theta-1, -\theta-1\}, \{1-\theta, -2\theta\}, \{\theta+1, 2\theta\}\}$ and $G(\theta, -\theta, \theta^{1+\alpha}) \times \theta^{4nj+2i} = \{\{-2\theta, \theta^{1+\alpha}-\theta\}, \{2\theta, \theta^{1+\alpha}+\theta\}, \{\theta-\theta^{1+\alpha}, -\theta-\theta^{1+\alpha}\}\} \times \theta^{4nj+2i}$. In this case, we will show that pair $\{1-\theta, -2\theta\}$ in $G(1, \theta, -\theta)$ can not be equal to any pair in $G(\theta, -\theta, \theta^{1+\alpha}) \times \theta^{4nj+2i}$.

It is easy to see that if $x = y \times \theta^{4nj+2i},\ x, y \in Z_p, 0 < i \leq n-1,\ 0 \leq j \leq t-1$ and $n = 2^{k-2}$, then $\frac{x}{y} \notin C_0^{4n} \cup C_{2n}^{4n}$. So we have that $(\pm 2\theta) \times \theta^{4nj+2i}$ can not be equal to any element in $\{1-\theta, -2\theta\}$ by Condition (e). Hence, $\{1-\theta, -2\theta\} \neq \{-2\theta, \theta^{1+\alpha}-\theta\} \times \theta^{4nj+2i}$ and $\{1-\theta, -2\theta\} \neq \{2\theta, \theta^{1+\alpha}+\theta\} \times \theta^{4nj+2i}$. Also we have that $(-\theta-\theta^{1+\alpha}) \times \theta^{4nj+2i}$ can not be equal to any element in $\{1-\theta, -2\theta\}$ by Conditions (d)–(e). Consequently, we have $\{1-\theta, -2\theta\} \neq \{\theta-\theta^{1+\alpha}, -\theta-\theta^{1+\alpha}\} \times \theta^{4nj+2i}$. The proof is complete. □

Combining Lemmas 2.6 and 5.1–5.3, we have the following.

Lemma 5.4 *Let* $p = 2^k t + 1$ *be a prime, where* $k \geq 3$, t *odd and* $t \geq 3$. *Suppose* θ *and* α *satisfy Conditions* (a)–(d) *and* (e) *(or* (e')*). If further,*

(f) *the quadruple* $\{1, \theta, -\theta, \theta^{1+\alpha}\}$ *has property* $\mathcal{P}$,
(g) *any triple* $\{a, b, c\} \subset \{1, \theta, -\theta, \theta^{1+\alpha}\}$ *satisfies the condition* $a^2+b^2+c^2 \neq ab+bc+ac$,

then

$$R = \{(1, \theta, -\theta, \theta^{1+\alpha}) \times \theta^{4nj+2i} : 0 \leq j \leq t-1, 0 \leq i \leq n-1\}$$

where $n = 2^{k-2}$, *forms an initial round of a Z-cyclic* 3*PDTWh*(p).

Applying the above construction, we have successfully constructed most of the Z-cyclic 3PDTWh(p)s for primes $p \equiv 1 \pmod{16},\ 241 < p < 10000$ with 19 possible exceptions. Here, we list the appropriate primitive root and corresponding parameter α for these primes, and tabulate the triples (p, θ, α) in Table 3.

For the unsolved primes p, we extend the construction in Lemma 5.4 to the following.

Let $p = 2^k t + 1$ be a prime and θ be a primitive root of Z_p, where $k \geq 3, t$ odd and $t \geq 3$. Suppose the quadruples

$$(a_m, b_m, c_m, d_m) \times \theta^{4i} \quad (0 \leq i \leq n/2-1,\ m = 0, 1)$$

where $n = 2^{k-2}$, satisfy

(i) $\bigcup_{m=0}^{1}\{a_m, b_m, c_m, d_m\}$ and $\bigcup_{m=0}^{1}\{b_m - a_m, c_m - b_m, d_m - c_m, a_m - d_m\}$ are representative systems of the coset classes $\cup\{C_{e_l}^{4n}\} \cup \{C_{e_l+2ns_l}^{4n}\}$ and $\cup\{C_{e_l'}^{4n}\} \cup \{C_{e_l'+2ns_l'}^{4n}\}$ respectively, where s_l and s_l' are odd integers, $0 \leq l \leq 3$ and each of the sets $\{e_0, e_1, e_2, e_3\}$, $\{e_0', e_1', e_2', e_3'\}$ covers the different residues modulo 4.

(ii) $\bigcup_{m=0}^{1}\{a_m - b_m, c_m - d_m\}$, $\bigcup_{m=0}^{1}\{a_m - c_m, b_m - d_m\}$ and $\bigcup_{m=0}^{1}\{a_m - d_m, b_m - c_m\}$ are representative systems of the coset classes $\cup\{C_{g_l}^{4n}\}$, $\cup\{C_{g_l'}^{4n}\}$ and $\cup\{C_{g_l''}^{4n}\}$ respectively, where $0 \leq l \leq 3$ and each of the sets $\{g_0, g_1, g_2, g_3\}$, $\{g_0', g_1', g_2', g_3'\}$, $\{g_0'', g_1'', g_2'', g_3''\}$ covers the different residues modulo 4.

Table 3 (p, θ, α)

(257, −), (337, 46, 279), (353, −), (401, 236, 343), (433, 57, 87), (449, −), (577, −), (593, 5, 487), (641, −),
(673, 485, 175), (769, −), (881, 15, 535), (929, 382, 239), (977, 5, 759), (1009, 33, 311), (1153, −), (1201, 29, 1063),
(1217, 896, 1119), (1249, 55, 1135), (1297, 15, 359), (1361, 24, 487), (1409, −), (1489, 29, 759), (1553, 5, 263),
(1601, −), (1697, 27, 815), (1777, 10, 407), (1873, 37, 903), (1889, 24, 1487), (2017, 107, 879), (2081, 17, 1327),
(2113, 413, 479), (2129, 3, 775), (2161, 69, 1143), (2273, 76, 175), (2417, 21, 583), (2593, 26, 623), (2609, 6, 1799),
(2657, 6, 1583), (2689, −), (2753, −), (2801, 3, 471), (2833, 10, 1383), (2897, 5, 1607), (3041, 132, 2351),
(3089, 3, 1287), (3121, 44, 215), (3137, −), (3169, 94, 2031), (3217, 15, 87), (3313, 35, 1335), (3329, −),
(3361, 31, 2415), (3457, −), (3617, 43, 2799), (3697, 20, 1767), (3761, 19, 2535), (3793, 19, 3687), (3889, 29, 2311),
(4001, 135, 1391), (4049, 3, 4023), (4129, 131, 3151), (4177, 11, 151), (4241, 51, 23), (4273, 7, 1367),
(4289, 368, 543), (4337, 12, 4151), (4481, −), (4513, 28, 3951), (4561, 11, 823), (4657, 35, 231), (4673, 872, 4447),
(4721, 7, 7), (4801, 861, 2207), (4817, 10, 1943), (4993, −), (5009, 29, 2887), (5153, 12, 2799), (5233, 13, 1975),
(5281, 91, 3119), (5297, 17, 695), (5393, 3, 1655), (5441, 332, 991), (5521, 11, 2743), (5569, 342, 3231),
(5857, 266, 4143), (5953, 1097, 5919), (6113, 44, 335), (6257, 3, 5111), (6337, 2332, 1887), (6353, 5, 5015),
(6449, 6, 3447), (6481, 28, 1639), (6529, 3732, 63), (6577, 30, 1575), (6673, 10, 6535), (6689, 13, 1103),
(6737, 10, 5575), (6833, 3, 1703), (6961, 13, 5015), (6977, 54, 1951), (7057, 5, 3255), (7121, 3, 3207),
(7297, 4522, 1087), (7393, 15, 3919), (7457, 31, 911), (7489, 69, 6751), (7537, 7, 1111), (7649, 56, 1071),
(7681, −), (7793, 5, 3495), (7841, 51, 4687), (7873, 14, 7519), (7937, −), (8017, 5, 631), (8081, 3, 119),
(8161, 97, 4847), (8209, 7, 6919), (8273, 3, 71), (8353, 15, 2447), (8369, 12, 23), (8513, 96, 5471),
(8609, 15, 2895), (8641, 47, 3295), (8689, 13, 5991), (8737, 37, 5199), (8753, 3, 5847), (8849, 3, 6103),
(8929, 19, 2959), (9041, 11, 3527), (9137, 3, 5319), (9281, 69, 6559), (9377, 24, 3087), (9473, −),
(9521, 3, 295), (9601, 1970, 1215), (9649, 7, 103), (9697, 88, 2447), (9857, 1876, 1087).

Then, it is easy to check that $(a_m, b_m, c_m, d_m) \times \theta^{4i}$ $(0 \le i \le n/2-1,\ m = 0, 1)$ satisfy Conditions (1)–(2) of Lemma 2.1 with n. Hence,

$$R = \{(a_m, b_m, c_m, d_m) \times \theta^{4nj+4i} : 0 \le j \le t-1, 0 \le i \le n/2-1,\ m = 0, 1\}$$

where $n = 2^{k-2}$, forms an initial round of a Z-cyclic DTWh(p).

Furthermore, if

(iii) any triple $\{a, b, c\} \subset \{a_m, b_m, c_m, d_m\}$, $m = 0, 1$, satisfies the condition $a^2+b^2+c^2 \ne ab + bc + ac$, and

(iv) any two different triples $\{a, b, c\} \subset \{a_m, b_m, c_m, d_m\} \times \theta^{4i}$ and $\{e, f, g\} \subset \{a_{m'}, b_{m'}, c_{m'}, d_{m'}\} \times \theta^{4i'}$, where $m, m' = 0, 1$ and $0 \le i, i' \le n/2-1$, satisfy the condition $E(a, b, c) \ne E(e, f, g)$,

then R forms an initial round of a Z-cyclic 3PDTWh(p).

Using the above extended construction, we find the required quadruples (a_m, b_m, c_m, d_m), $m = 0, 1$ for 17 of the 19 unsolved Z-cyclic 3PDTWh(p)s by a computer search. Here, we list them below.

$p = 353$:	$\theta = 3$,	(1, 3, 13, 115),	(9, 344, 263, 122),
$p = 449$:	$\theta = 3$,	(1, 2, 375, 273),	(3, 281, 103, 447),
$p = 577$:	$\theta = 5$,	(1, 5, 52, 544),	(41, 256, 126, 555),
$p = 641$:	$\theta = 3$,	(1, 6, 114, 418),	(32, 422, 331, 79),
$p = 1153$:	$\theta = 5$,	(1, 3, 480, 203),	(93, 862, 365, 839),
$p = 1409$:	$\theta = 3$,	(1, 2, 51, 336),	(43, 1317, 338, 472),
$p = 1601$:	$\theta = 3$,	(1, 3, 9, 37),	(61, 306, 1070, 99),
$p = 2689$:	$\theta = 19$,	(1, 3, 10, 1520),	(30, 510, 310, 1753),
$p = 2753$:	$\theta = 3$,	(1, 2, 5, 129),	(6, 1680, 607, 1986),
$p = 3137$:	$\theta = 3$,	(1, 3, 9, 76),	(139, 666, 2345, 141),
$p = 3329$:	$\theta = 3$,	(1, 2, 87, 956),	(234, 317, 2074, 336),
$p = 3457$:	$\theta = 7$,	(1, 2, 10, 153),	(158, 1594, 1217, 1463),
$p = 4481$:	$\theta = 3$,	(1, 3, 9, 1642),	(53, 1735, 785, 211),
$p = 4993$:	$\theta = 5$,	(1, 3, 15, 1438),	(211, 3086, 4265, 3840),
$p = 7681$:	$\theta = 17$,	(1, 2, 82, 4003),	(954, 5360, 4065, 477),
$p = 7937$:	$\theta = 3$,	(1, 2, 5, 2361),	(107, 4028, 6493, 799),
$p = 9473$:	$\theta = 3$,	(1, 3, 13, 4105),	(90, 6033, 8444, 3721).

Summarizing the discussion above and combining Lemma 1.8, we have

Lemma 5.5 *For each prime $p \equiv 1$ (mod 16), $97 \le p < 10{,}000$, and $p \ne 257{,}769$, there exists a Z-cyclic 3PDTWh(p).*

Now, Theorem 1.6 can be improved as follows:

Lemma 5.6 *A Z-cyclic DTWh(p) exists for any prime $p \equiv 5$ (mod 8), $p \ge 29$, or $p \equiv 1$ (mod 8), $29 \le p < 10{,}000$, $p \ne 257{,}769$.*

6 Concluding remarks

Combining Lemmas 3.5 and 4.5, we have

Theorem 6.1 *There exists a Z-cyclic* $3PDTWh(p)$ *for any p prime,* $p \equiv 5, 9, 13$ (*mod* 16) *and* $p \geq 29$.

In this paper, we investigate the existence of a Z-cyclic 3PDTWh(p) for any prime $p \equiv 1 \pmod 4$ and show that such a design exists whenever $p \equiv 5, 9, 13 \pmod{16}$ and $p \geq 29$. Weil's Theorem played an important role in obtaining this result. However, this approach fails for the case of $p \equiv 1 \pmod{16}$ due to the cyclotomic number can not be easily fixed. Particularly, there appears to be no easy way of obtaining a Z-cyclic DTWh(p) for p a prime of the form $2^m + 1$.

Acknowledgments The authors thank the anonymous reviewer for his valuable comments and suggestions.

References

1. Abel RJR, Bennett FE, Ge G, Existence of directed triplewhist tournaments with the three person property 3PDTWh(v), preprint
2. Abel RJR, Finizio NJ, Ge G, Greig M (2006) New Z-cyclic triplewhist frames and triplewhist tourment designs. Discrete Appl Math 154:1649–1673
3. Abel RJR, Ge G (2005) Some difference matrix constructions and an almost completion for the existence of triplewhist tournaments TWh(v). European J Combin 26:1094–1104
4. Anderson I (1995) A hundred years of whist tournaments. J Combin Math Combin Comput 19:129–150
5. Anderson I, Finizio NJ (1997) Triplewhist tournaments that are also Mendelsohn designs. J Combin Des 5:397–406
6. Anderson I, Finizio NJ (2000) On the construction of directed triplewhist tournaments. J Combin Math Combin Comput 35:107–115
7. Anderson I, Finizio NJ, Leonard P (1999) New product theorems for Z-cyclic whist tournaments. J Combin Theory Ser A 88:162–166
8. Baker RD (1975) Factorization of graphs, Doctoral Thesis, Ohio State University
9. Bennett FE, Ge G (2006) Existence of directedwhist tournaments with the three person property 3PDWh(v). Discrete Appl Math 154:1939–1946
10. Bennett FE, Zhu L (1992) Conjugate-orthogonal latin squares and related structures. In: Dinitz J, Stinson D (eds) Contemporary design theory: a collection of surveys. Wiley, New York, pp 41–96
11. Beth T, Jungnickel D, Lenz H (1999) Design theory. Cambridge University Press, Cambridge, UK
12. Buratti M (2000) Existence of Z-cyclic triplewhist tournaments for a prime number of players. J Combin Theory Ser A 90:315–325
13. Buratti M (2002) Cyclic designs with block size 4 and related optimal optical orthogonal codes. Des Codes Cryptogr 26:111–125
14. Chang Y, Ji L (2004) Optimal ($4up$, 5, 1) optical orthogonal codes. J Combin Des 5:135–146
15. Chen K (1995) On the existence of super-simple (v, 4, 3)-BIBDs. J Combin Math Combin Comput 17:149–159
16. Chen K (1996) On the existence of super-simple (v, 4, 4)-BIBDs. J Statist Plann Inference 51:339–350
17. Chen K, Zhu L (1998) Existence of (q, 6, 1) difference families with q a prime power. Des Codes Cryptogr 15:167–173
18. Feng T, Chang Y (2006) Existence of Z-cyclic 3PTWh(p) for any prime $p \equiv 1 \pmod 4$. Des Codes Cryptogr 39:39–49
19. Finizio NJ (1993) Whist tournaments–three person property. Discrete Appl Math 45:125–137
20. Finizio NJ (1995) Z-cyclic triplewhist tournaments-the noncompatible case, Part 1. J Combin Des 3: 135–146
21. Finizio NJ (1997) Z-cyclic triplewhist tournaments-the noncompatible case, Part 2. J Combin Des 5: 189–201
22. Finizio NJ, Lewis JT (1997) A criterion for cyclic whist tournaments with the three person property. Util Math 52:129–140
23. Ge G Triplewhist tournaments with the three person property. J Combin Theory Ser A (to appear)
24. Ge G, Lam CWH (2003) Some new triplewhist tournaments TWh(v). J Combin Theory Ser A 101: 153–159
25. Ge G, Lam CWH (2004) Super-simple resolvable balanced incomplete block designs with block size 4 and index 3. J Combin Des 12:1–11

26. Ge G, Lam CWH (2004) Whist tournaments with the three person property. Discrete Appl Math 138: 265–276
27. Ge G, Ling ACH (2003) A new construction for Z-cyclic whist tournaments. Discrete Appl Math 131:643–650
28. Ge G, Zhu L (2001) Frame constructions for Z-cyclic triplewhist tournaments. Bull Inst Combin Appl 32:53–62
29. Gronau H-DOF, Mullin RC (1992) On super-simple 2-$(v, 4, \lambda)$ designs. J Combin Math Combin Comput 11:113–121
30. Hartman A (1980) Doubly, orthogonally resolvable quadruple systems, combinatorial mathematics, VII (Proc. Seventh Australian Conf., Univ. Newcastle, Newcastle, 1979), pp 157–164. Lecture Notes in Math. 829, Springer, Berlin
31. Liaw YS (1996) Construction of Z-cyclic triplewhist tournaments. J Combin Des 4:219–233
32. Lidl R, Niederreiter H (1997) Finite fields.. Cambridge University Press, Cambridge, UK
33. Lu Y, Zhang S (2000) Existence of whist tournaments with the three-person property 3PWh(v). Discrete Appl Math 101:207–219
34. Lu Y, Zhu L (1997) On the existence of triplewhist tournaments TWh(v). J Combin Des 5:249–256
35. Moore EH (1896) Tactical memoranda I–III. Amer J Math 18:264–303
36. Zhang X (1996) On the existence of $(v, 4, 1)$-RPMD. Ars Combin 42:3–31
37. Zhang X (2005) A few more RPMDs with $k = 4$. Ars Combin 74:187–200
38. Zhang X, Ge G (2007) Super-simple resolvable balanced incomplete block designs with block size 4 and index 2. J Combin Des 15:341–356