Some Constructions of Combinatorial Designs

by

Leigh H. M. Ellison

A thesis submitted to the
Faculty of Information and Mathematical Sciences
at the University of Glasgow
for the degree of
Doctor of Philosophy

January 2006

To my mum;

for teaching me all of the things that really matter.

I love you and miss you.

Statement

This thesis is submitted in accordance with the regulations for the degree of Doctor of Philosophy in the University of Glasgow. It is the record of research carried out at the University of Glasgow between October 2002 and September 2005. No part of it has been submitted by me for a degree at any other university.

The results from Chapter 2 have been accepted for publication in [7], [8] and [9], while those from Chapter 4 have been submitted for publication.

Acknowledgements

I would like to begin by thanking my supervisor, Dr. Ian Anderson, for his help, guidance and encouragement throughout the period of my research. It is a collaboration that I have greatly enjoyed. Thanks also to the Department of Mathematics at the University of Glasgow, and the E.P.S.R.C for their funding of my research.

On a personal note, I'd like to thank all of my friends and family for their love and support. I'd especially like to thank Mark, Jane and Kay for being there for me throughout the last year in particular. Thanks also to Katie, Andrew and Fraser for always being able to make me smile.

My biggest thanks are reserved for someone that I will not be able to pass them along to in person. She has been the most influential figure in my life, and is responsible for any good qualities that I may possess. Thanks Mum; for everything.

Summary

The objects of study of this thesis are combinatorial designs. Chapters 2 and 3 deal with various refinements of whist tournament, while Chapters 3 and 4 focus on terraces.

Chapter 2 is devoted to the investigation of $\mathbb{Z}$-cyclic ordered triplewhist tournaments on p elements, where $p \equiv 5 \pmod 8$; $\mathbb{Z}$-cyclic ordered triplewhist and directed triplewhist tournaments on p elements, where $p \equiv 9 \pmod{16}$; and $\mathbb{Z}$-cyclic directed moore $(2, 6)$ generalised whist tournament designs on p elements, where $p \equiv 7 \pmod{12}$. In each of these cases, p is prime. In an effort to prove the existence of an infinite family of each of these tournaments, constructions are introduced and the conditions under which they give the initial round of a tournament of the kind we desire are found. A bound above which these conditions are always satisfied is then obtained, and we try to fill in the appropriate gaps below that bound.

In Chapter 3 we investigate the existence of tournaments of the type seen in Chapter 2 which involve four players per game, with an additional property. This is known as the three person property and is defined in Chapter 1. Here, we focus on one of the constructions introduced in Chapter 2 for each type of tournament. Then we find a new bound using only that construction with the additional conditions introduced by the three person property, and again try to fill in the appropriate gaps below the bound.

Chapter 4 is an investigation of logarithmic terraces and their properties. Very little work has been done on them previously, so this was really an opportunity to look at them more closely in an effort to find as many interesting properties as possible. Some general results and examples are given, with the focal point of the chapter being the study of terraces which are simultaneously logarithmic for two different primitive roots.

In Chapter 5, a more specific problem is addressed which involves training schedules for athletes. Here we want $n(n-1)$ athletes to carry out n tasks in some order, then keep repeating them in different orders in blocks of n as many times as possible so that certain conditions are satisfied. These conditions are listed in Chapter 5. We make use of the Williams terrace and the Owens terrace in our attempt to find a general method which allows the given conditions to be satisfied and gets as close as possible to the theoretical limit where each athlete carries out the n tasks $n-1$ times.

Chapter 1

Introduction

In the course of this thesis, we will be looking at a number of constructions of combinatorial designs. Before looking at each one in more detail, it is first necessary to introduce some of the ideas, results and definitions which will be needed later.

1.1 Whist Tournaments

It would seem that the study of whist tournaments began in the 1890s, with the journal 'Whist' appearing in 1891 and work by J. T. Mitchell and R. F. Foster (in [30] and [22] respectively) providing examples of whist tournaments for $4m$ players for all $m \leq 10$. In 1896, a large step forward was taken when E. H. Moore proved the existence of $Wh(4m)$ whenever $4m = 3p+1$ (p prime, $p \equiv 1 \pmod 4$) and whenever $4m = 2^\alpha$ ($\alpha \geq 2$). This was to be the only major contribution to the subject for over half a century. The existence of a $Wh(4m)$ and a $Wh(4m+1)$ was established for all positive integers m in the 1970s by R. M. Wilson, R. D. Baker and H. Hanani. These results are discussed in [5]. Further information on the history of whist tournaments can be found in [4]. For the purposes of this work, we will be looking at specific types of whist tournament which will now be introduced.

A whist tournament Wh($4m+1$) for $4m+1$ players is a schedule of games (or tables) (a, b, c, d) involving two players a, c opposing two other players b, d such that

i. the games are arranged into $4m+1$ rounds each of m games;

ii. each player plays in exactly one game in all but one round;

iii. each player partners every other player exactly once;

iv. each player opposes every other player exactly twice.

Example 1.1.1 A $Wh(13)$ is given by the initial round

Round 1	$(1,8,12,5)$	$(2,3,11,10)$	$(4,6,9,7)$
Round 2	$(2,9,0,6)$	$(3,4,12,11)$	$(5,7,10,8)$
$\vdots$			
Round 13	$(0,7,11,4)$	$(1,2,10,9)$	$(3,5,8,6)$

In Chapter 2 we shall first of all be concerned with three refinements of the structure, called triplewhist tournaments, directed whist tournaments and ordered whist tournaments. Call the pairs $\{a,b\}$ and $\{c,d\}$ pairs of *opponents of the first kind*, and call the pairs $\{a,d\}$ and $\{b,c\}$ pairs of *opponents of the second kind.* We further say that b is a's *left hand opponent* and c's *right hand opponent*, and make similar definitions for each of a, c and d (imagining the 4 players to be sitting clockwise around a table). In addition, we also say that a and c are *partners of the first kind* while b and d are *partners of the second kind.*

Then a *triplewhist tournament* $TWh(4m+1)$ is a $Wh(4m+1)$ in which every player is an opponent of the first (resp., second) kind exactly once with every other player; an *ordered whist tournament* $OWh(4m+1)$ is a $Wh(4m+1)$ in which each player opposes every other player exactly once while being a partner of the first (resp., second) kind; and a *directed whist tournament* $DWh(4m+1)$ is a $Wh(4m+1)$ in which each player is a left (resp., right) hand opponent of every other player exactly once. Directed whist tournaments have also been widely studied under the alternative name of resolvable perfect Mendelsohn designs with block size 4. If the players are elements of $\mathbb{Z}_{4m+1}$, and if the *ith* round is obtained from the initial (first) round by adding $i-1$ to each element (mod $4m+1$), then we say that the tournament is $\mathbb{Z}$*-cyclic.* It can now be seen that Example 1.1.1 is $\mathbb{Z}$-cyclic. By convention we always take the initial round to be the round from which 0 is absent. The games (tables)

$$(a_1,b_1,c_1,d_1),\dots,(a_m,b_m,c_m,d_m)$$

form the initial round of a $\mathbb{Z}$-cyclic triplewhist tournament if

$$\bigcup_{i=1}^{m}\{a_i,b_i,c_i,d_i\}=\mathbb{Z}_{4m+1}\setminus\{0\}, \qquad (1.1.1)$$

$$\bigcup_{i=1}^{m}\{\pm(a_i-c_i),\pm(b_i-d_i)\}=\mathbb{Z}_{4m+1}\setminus\{0\}, \tag{1.1.2}$$

$$\bigcup_{i=1}^{m}\{\pm(a_i-b_i),\pm(c_i-d_i)\}=\mathbb{Z}_{4m+1}\setminus\{0\}, \tag{1.1.3}$$

$$\bigcup_{i=1}^{m}\{\pm(a_i-d_i),\pm(b_i-c_i)\}=\mathbb{Z}_{4m+1}\setminus\{0\}. \tag{1.1.4}$$

The name 'triplewhist' tournament came to be because from such a whist tournament, three can be derived. This is due to the fact that the partner pairs, or the opponent pairs of the first kind, or the opponent pairs of the second kind, can be taken as partner pairs of a $Wh(4m)$ or $Wh(4m+1)$.

The games given above form a $\mathbb{Z}$-cyclic ordered whist tournament if, in addition to forming the initial round of a Wh$(4m+1)$,

$$\bigcup_{i=1}^{m}\{(a_i-b_i),(a_i-d_i),(c_i-b_i),(c_i-d_i)\}=\mathbb{Z}_{4m+1}\setminus\{0\}. \tag{1.1.5}$$

Alternatively, they form a $\mathbb{Z}$-cyclic directed whist tournament if, in addition to satisfying (1.1.1) and (1.1.2),

$$\bigcup_{i=1}^{m}\{(b_i-a_i),(c_i-b_i),(d_i-c_i),(a_i-d_i)\}=\mathbb{Z}_{4m+1}-\{0\}. \tag{1.1.6}$$

1.2 Starters

The whist tournaments that we will be looking at in more detail later are all $\mathbb{Z}$-cyclic. Such designs rely on the idea of a *starter*. As seen in [4, p. 136], the pairs $\{a_1,b_1\},\ldots,\{a_{2m},b_{2m}\}$ of non-zero elements of $\mathbb{Z}_{4m+1}$ are said to form a starter in $\mathbb{Z}_{4m+1}$ if

$$\bigcup_{i=1}^{2m}\{a_i,b_i\}=\mathbb{Z}_{4m+1}\setminus\{0\},$$

$$\bigcup_{i=1}^{2m}\{\pm(a_i-b_i)\}=\mathbb{Z}_{4m+1}\setminus\{0\}.$$

The pairs $\{a_1,b_1\},\ldots,\{a_{4m},b_{4m}\}$ of $\mathbb{Z}_{4m+1}$ form a 2-*fold starter* if

the elements a_i, b_i are the non-zero elements of $\mathbb{Z}_{4m+1}$ each occurring twice, the elements $\pm(a_i - b_i)$ are all the non-zero elements of $\mathbb{Z}_{4m+1}$ each twice.

As mentioned previously, convention dictates that we take the initial round of a $\mathbb{Z}$-cyclic $Wh(4m+1)$ on $\mathbb{Z}_{4m+1}$ to be the round in which 0 does not play. So the condition for

$$(a_1, b_1, c_1, d_1), \ldots, (a_m, b_m, c_m, d_m)$$

to be the initial round games for a $\mathbb{Z}$-cyclic $Wh(4m+1)$ are precisely

the pairs $\{a_i, c_i\}$, $\{b_i, d_i\}$, $1 \le i \le m$, form a starter,

the pairs $\{a_i, b_i\}$, $\{b_i, c_i\}$, $\{c_i, d_i\}$, $\{d_i, a_i\}$, $1 \le i \le m$ form a 2-fold starter.

It can now be seen by looking at (1.1.1) and (1.1.2) that the partner pairs of a $\mathbb{Z}$-cyclic triplewhist tournament form a starter. Similarly for (1.1.1) and (1.1.3) with respect to the first opponent pairs, and (1.1.1) and (1.1.4) with respect to the second opponent pairs.

1.3 Primitive Roots

When trying to prove the existence of particular types of whist tournaments, we will be making use of constructions which involve the idea of a *primitive root.* The following definition can be found in [5, p. 32].

Definition 1.3.1 A non-zero element θ of $GF(q)$ is called a *primitive element* if θ, θ^2, $\theta^3, \ldots, \theta^{q-1} = 1$ are precisely all the non-zero elements of $GF(q)$; i.e. if the (multiplicative) order of θ is $q-1$. If $q = p$, so that $GF(q)$ is just $\mathbb{Z}_p$, such a θ is called a *primitive root* of p.

Every prime p has a primitive root, but the primitive root itself is not necessarily unique. In the course of trying to find elements which satisfy particular conditions (which we will be doing in an attempt to prove the existence of certain types of whist tournament), it is sometimes helpful to try different primitive roots before you come across an element with the properties you desire.

Example 1.3.1 The primitive roots for $p = 11$ are 2, 6, 7 and 8.

The original proof by Anderson, Cohen and Finizio, which dealt with the existence of $\mathbb{Z}-$cyclic TWh(p) with $p = 8n+5$ prime [6], contained a requirement that certain elements be primitive roots of $\mathbb{Z}_p$. This requirement was shown by Buratti in [18] to be an additional, but not necessary one. The elements in question need only be non-square over $\mathbb{Z}_p$, and a less difficult proof is the result. Primitive roots are still used in the constructions however, as can be seen in Chapters 2 and 3, or alternatively in [7] and [8].

1.4 Weil's Theorem

Definition 1.4.1 A *character* of a finite field F is a function $\psi : F \longrightarrow \mathbb{C}$, satisfying the following conditions:

i. $\psi(0) = 0$;

ii. $\psi(1) = 1$;

iii. $\psi(xy) = \psi(x)\psi(y)$ for all $x,\ y \in F$.

The key result which is applied in Chapters 2 and 3 of this thesis is Weil's thorem on multiplicative character sums [28, Theorem 5.41, p. 225]. It is extremely helpful in the field of combinatorics when you wish to prove existence by the use of explicit constructions, as we do here. In this theorem, our field is GF(q). Following on from the above definition, the convention is understood that if ψ is a multiplicative character of GF(q), then $\psi(0) = 0$. Adopting this convention we have $\psi(xy) = \psi(x)\psi(y)$ for all $(x, y) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$.

Theorem 1.4.1 *Let ψ be a multiplicative character of order $m > 1$ of the finite* GF(q). *Let f be a polynomial of* GF$(q)[x]$ *which is not of the form kg^m for some $k \in \mathrm{GF}(q)$ and some $g \in \mathrm{GF}(q)[x]$. Then we have*

$$\left| \sum_{x \in \mathrm{GF}(q)} \psi(f(x)) \right| \le (d-1)\sqrt{q}$$

where d is the number of distinct roots of f in its splitting field over GF(q).

The results involving whist tournaments which this theorem has been successfully used to help prove include the existence of $\mathbb{Z}$-cyclic $TWh(p)$ with $p \equiv 5 \pmod 8$, $p \ge 29$ in [6], and the extension of this to the existence of $\mathbb{Z}$-cyclic $TWh(v)$ for any v whose prime factors are congruent to 1 (mod 4) and distinct from 5, 13 and 17 in [18]. We will be making use of it to prove further results.

1.5 Balanced Designs

A link between whist tournaments and other types of construction which we will be making use of, is the fact that *pairwise balanced designs* can be used to combine smaller whist tournaments into larger ones.

Definition 1.5.1 *A $PBD(K, v)$ is a collection of subsets (blocks) of a v-set, with each block size being in the set K, such that each pair of elements occurs as a subset of precisely one block.*

So for example we can take a finite projective plane of order 4, i.e. a $PBD(\{5\}, 21)$, and from it construct a $Wh(21)$ by constructing a $Wh(5)$ on each block and arranging the games suitably in rounds.

Definition 1.5.2 *A balanced incomplete block design (BIBD) is a collection of k-subsets (called blocks) of a v-set S, $k < v$, such that each pair of elements of S occur together in exactly λ of the blocks.*

Such a design is often described as a (v, k, λ)-*design*. In Chapters 2 and 3, we will be looking at specific variations of triplewhist tournaments of order v where $v = 4m + 1$, so it is worth noting that these are, in turn, special classes of $(v, 4, 3)$-$BIBD$.

1.6 Three Person Property

Definition 1.6.1 A whist tournament is said to have the *three person property* if the intersection of any two games (tables) in the tournament is at most two. If a $Wh(v)$ has the three person property it is called a *three person whist tournament* $3PWh(v)$.

Work done involving the three person property includes the proof by Lu and Shengyuan in [29] that whist tournaments satisfying the three person property exist for v players, $v \equiv 0$ or $1 \pmod 4$, $v > 472$. They also showed that below the bound of 472, there are at most 38 exceptions. In Chapter 3 we take a closer look at the infinite families of triplewhist tournaments encountered in Chapter 2. In particular, we are looking to see whether the above definition can be applied to them.

Tournaments which satisfy the three person property can also be thought of as *super-simple* $(v, 4, 3)$-$BIBD$s. If a design contains no repeated blocks then it is regarded as being *simple*, while it is super-simple if the intersection of any two blocks contains at most two elements. Super-simple designs were introduced by Gronau and Mullin in [24].

Example 1.6.1 The initial round of a $\mathbb{Z}$-cyclic $Wh(13)$ which satisfies the three person property is given by

$$(1,2,4,8),\ (3,6,12,11),\ (5,9,7,10).$$

If all 13 rounds of this tournament are looked at, it can be seen that no two games have more than two players in common.

1.7 Terraces

The idea of a *terrace* was first introduced by Bailey in [17, p. 325]. Let G be a finite group of order n with identity element e, let the group operation be multiplication, let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ be an arrangement of the elements of G, and let $\mathbf{b} = (b_1, b_2, \ldots, b_{n-1})$ be the ordered sequence where $b_i = a_i^{-1}a_{i+1}$ for $i = 1, 2, \ldots, n-1$. Then $\mathbf{a}$ is a terrace for G, and $\mathbf{b}$ the corresponding 2-*sequencing*, if $\mathbf{b}$ and $\mathbf{b}^{-1}$, when looked at together, contain each element x of $G \setminus \{e\}$ exactly twice.

If G is $\mathbb{Z}_n$, with addition as the group operation, then x^{-1} in the above becomes $-x$, and the elements of the 2-sequencing are $b_i = a_{i+1} - a_i$ $(i = 1, 2, \ldots, n-1)$.

Notation: Where terraces and 2-sequencings are printed as displays, we follow previous practice by omitting brackets and commas. The reverse of a terrace $\mathbf{a}$ will be denoted by $\mathbf{a}_{rev}$.

Example 1.7.1 The following is an example of a $\mathbb{Z}_6$ terrace:

$$1\ 2\ 6\ 3\ 5\ 4.$$

It has the 2-sequencing

$$1\ 4\ 3\ 2\ 5.$$

A terrace for G is *directed* if its 2-sequencing contains each element of $G \setminus \{e\}$ exactly once, in which case the 2-sequencing is then a *sequencing*. It can now be seen that Example 1.7.1 is a directed terrace.

Having introduced the idea of terraces, we are now going to take that definition a step further. For any odd prime p we now say that a terrace $\mathbf{l} = (l_1, l_2, \ldots, l_{p-1})$ for $\mathbb{Z}_{p-1}$, when written with $1 \le l_i \le p-1$ for all $i = 1, 2, \ldots, p-1$, is *logarithmic* or *x-logarithmic* if, for some primitive root x of p, the ordered sequence $\mathbf{e} = (x^{l_1}, x^{l_2}, \ldots, x^{l_{p-1}})$ becomes a further terrace for $\mathbb{Z}_{p-1}$ when its entries x^{l_i} are evaluated modulo p (not modulo $p-1$) so as to satisfy $1 \leq x^{l_i} \leq p-1$ for all $i = 1, 2, \ldots, p-1$. We call the terrace $\mathbf{e}$ the *exponent terrace* of $\mathbf{l}$.

Example 1.7.2 If we consider the $\mathbb{Z}_6$ terrace

$$1\ 5\ 4\ 3\ 6\ 2,$$

we can see that it has the 2-sequencing

$$4\ 5\ 5\ 3\ 2.$$

In turn it can be seen that this is 5-logarithmic by evaluating the sequence

$$5^1\ 5^5\ 5^4\ 5^3\ 5^6\ 5^2,$$

with each entry reduced modulo 7 to lie in $\{1, 2, \ldots, 6\}$, giving us the $\mathbb{Z}_6$ terrace

$$5\ 3\ 2\ 6\ 1\ 4.$$

This terrace has the 2-sequencing

$$4\ 5\ 4\ 1\ 3$$

and is the exponent terrace corresponding to the logarithmic terrace that we started from.

The following theorems appear in [16, Theorems 1.3 and 1.1 respectively].

Theorem 1.7.1 *If $\mathbf{e} = (e_1, e_2, \ldots, e_{p-1})$ is an exponent terrace for $\mathbb{Z}_{p-1}$ where p is any odd prime, then so is $-\mathbf{e} = (p - e_1, p - e_2, \ldots, p - e_{p-1})$.*

Definition 1.7.1 The terrace $-\mathbf{e}$ is called the *p-complement* of $\mathbf{e}$.

Theorem 1.7.2 *If, for a given prime p with distinct primitive roots x and y, there exists an x-logarithmic terrace for $\mathbb{Z}_{p-1}$, then its exponent terrace is also the exponent terrace for a y-logarithmic terrace for $\mathbb{Z}_{p-1}$. Thus, each exponent terrace gives an x-logarithmic terrace for each primitive root x of p, and so the number of x-logarithmic terraces is independent of the choice of x. Further, if we have an x-logarithmic terrace, $\mathbf{a}$, and we know that $x \equiv y^d \pmod{p}$ for some integer d, then $\mathbf{c}$ defined by $c_i \equiv da_i \pmod{p-1}$, is a y-logarithmic terrace.*

It is also clearly the case that the reverse of a logarithmic terrace is a logarithmic terrace.

In Chapter 4, we will be looking more closely at these terraces in an effort to find some of the interesting properties it is hoped they possess.

Terraces can also be used in the construction of Latin squares. We will be looking more closely at this in Chapter 5.

1.8 Latin Squares

Latin squares are closely related to block designs and are defined as follows:

Definition 1.8.1 A *Latin square* on n symbols is an $n \times n$ array such that each of the n symbols occurs once in each row and in each column. The number n is called the *order* of the square.

We then say that a Latin square $A = (a_{ij})_{nxn}$ is *row complete* or *Roman* if the $n(n-1)$ ordered pairs $(a_{i,j}, a_{i,j+1})$, $1 \leq i \leq n$, $1 \leq j < n$, are all distinct.

Example 1.8.1 A row complete Latin square of order 6 is given by

$$\begin{array}{cccccc} 1 & 2 & 6 & 3 & 5 & 4 \\ 2 & 3 & 1 & 4 & 6 & 5 \\ 6 & 1 & 5 & 2 & 4 & 3 \\ 3 & 4 & 2 & 5 & 1 & 6 \\ 5 & 6 & 4 & 1 & 3 & 2 \\ 4 & 5 & 3 & 6 & 2 & 1 \end{array}$$

It can be seen that each of the 30 ordered pairs in this Latin square occur only once. The first row gives us the pairs $\{1,2\}, \{2,6\}, \{6,3\}, \{3,5\}$ and $\{5,4\}$. Then each of the other five rows give us five ordered pairs in the same way.

This idea is related to what we will be doing in Chapter 5. There, we will be looking at how n activities can be repeated as many times as possible, while satisfying certain conditions. These include the requirement that each of the n activities must be carried out in some order before moving on and repeating any of them, i.e., they are repeated in blocks of n. We also do not want any repeated carryovers (which occur when one particular activity is carried out immediately following another particular activity, on more than one occasion), and we also want each activity to have a different position within respective blocks of n each time they are repeated.

If we regard each block of n as a new row in a Latin rectangle, the relationship with the above definition is clear. In addition to the pairs given by successive entries within a row being distinct, we are also interested in the pairs given by the final entry in each row, and the first entry in the next row.

We will regard an *addition Latin square* as being one where each row is formed by adding 1 to the corresponding element in the previous row (modulo n). If we consider a Latin square of order 4, then the most obvious example is

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array}$$

1.9 Williams Squares

Williams [34] gave a simple way of constructing a row complete Latin square of any even order: writing $n = 2m$, simply form the addition Latin square whose first row is the directed terrace

$$1 \ 2 \ 2m \ 3 \ 2m-1 \ \ldots \ m \ m+2 \ m+1.$$

It is a directed terrace because the differences $a_{1,j+1} - a_{1,j}$ between consecutive elements are all distinct. They are

$$1 \ -2 \ 3 \ -4 \ \ldots \ -(2m-2) \ 2m-1.$$

Example 1.9.1 A (directed) Williams terrace for $n = 8$ is given by

$$1 \ 2 \ 8 \ 3 \ 7 \ 4 \ 6 \ 5.$$

Whenever $n = 2m + 1$ is odd, we cannot get a directed terrace since the even number of differences would cancel each other out in pairs, leaving the sum of the differences to be 0. This means that the first and last elements would have to be the same if the terrace were directed. So when n is odd, if we take the first row of a Latin square to be the Williams terrace

$$1 \quad 2 \quad 2m+1 \quad 3 \quad 2m \quad \ldots \quad m+1 \quad m+2,$$

then the differences are

$$1 \quad 2m-1 \quad 3 \quad 2m-3 \quad \ldots \quad 2m-1 \quad 1.$$

Example 1.9.2 A Williams terrace for $n = 11$ is given by

$$1 \quad 2 \quad 11 \quad 3 \quad 10 \quad 4 \quad 9 \quad 5 \quad 8 \quad 6 \quad 7.$$

1.10 Owens Terraces

The Owens terrace $\mathbf{a}_{Owens}$ for $\mathbb{Z}_n$ where $n = 2m+1$ was reported by Prescott ([32, p.146] and [33, p.269]), and is given by

$$\mathbf{a}_{Owens} = (1, 2, n-1, 4, n-3, \ldots, n-2, 5, n, 3),$$

where the last m elements are the elements from positions 2 to m taken in reverse, with 1 added to each. The 2-sequencing thus includes every element of $\mathbb{Z}_n$ exactly once, except that -1 is missing and $+1$ appears twice. The fact that the differences between elements are almost all different means that the Owens terrace is very close to being directed, a property which will be of use in Chapter 5.

Let $n = p = 2m+1$ and let $\mathbf{a}$ be an Owens terrace. If i is even, then

$a_i = i$ if $i \leq \frac{p-1}{2}$ when $p \equiv 1 \pmod 4$, or if $i \leq \frac{p+1}{2}$ when $p \equiv 3 \pmod 4$;

$a_i = i+1$ if $i \geq \frac{p+3}{2}$ when $p \equiv 1 \pmod 4$, or if $i \geq \frac{p+5}{2}$ when $p \equiv 3 \pmod 4$.

If i is odd, then

$a_i = 2-i$ if $i \leq \frac{p+1}{2}$ when $p \equiv 1 \pmod 4$ or if $i \leq \frac{p-1}{2}$ when $p \equiv 3 \pmod 4$;

$a_i = 3-i$ if $i \geq \frac{p+5}{2}$ when $p \equiv 1 \pmod 4$ or if $i \geq \frac{p+3}{2}$ when $p \equiv 3 \pmod 4$.

Example 1.10.1 An Owens terrace for $n = p = 11$ is given by

$$1 \quad 2 \quad 10 \quad 4 \quad 8 \quad 6 \quad 7 \quad 9 \quad 5 \quad 11 \quad 3.$$

In the above example (as in any example of an Owens terrace), it can be seen that the repeated difference of $+1$ is preceded by the first element in the block, and by the $(\frac{n+1}{2})$th element in the block. It can also be seen that the difference between these two elements here is $\frac{n-1}{2}$. For examples where $n \equiv 1 \pmod 4$, the difference between them is $\frac{n+1}{2}$. In addition it should be noted that in both cases the m elements immediately following the first element, 1, are even, while the last m are odd.

Chapter 2

Whist Tournaments

2.1 Introduction

Having introduced in Chapter 1 the basic ideas required to prove the existence of different varieties of whist tournament for particular primes, we now set about doing so. In each case, we will firstly introduce one or more general constructions which represent the initial round of a tournament. Then, we will look at each construction more closely in order to find the conditions which must be satisfied in order for it to yield whatever kind of whist tournament we are interested in. Having done that, if more than one construction was used, we then combine these conditions as much as possible. We are then left with conditions which, if satisfied, tell us that one of our constructions can be used to build a whist tournament of the kind we want. It is at this stage that Theorem 1.4.1 will be used to give a bound above which a value can always be found which satisfies the relevant conditions (thus showing that a whist tournament of the kind we want exists). Having done that, it is then the aim to show that a whist tournament of the kind we are interested in exists for all appropriate values less than the bound.

2.2 $\mathbb{Z}$-Cyclic Ordered Triplewhist Tournaments on p elements, where $p \equiv 5 \pmod 8$

First of all we are going to look at whist tournaments which are simultaneously both triplewhist and ordered. Such designs will be called *ordered triplewhist tournaments* and will be denoted by OTWh(v). We shall show that an OTWh(v) exists for all v whenever v is a prime $p \equiv 5 \pmod 8$, and $p \geq 29$. Finizio [19] has verified that there is no $\mathbb{Z}$-cyclic

TWh(p) for primes $p < 29$.

Example 2.2.1 A $\mathbb{Z}$-cyclic OTWh(29) is given by the initial round

$$(1, 3, 26, 13) \times 1, 3^4, \ldots, 3^{24}.$$

Taking a closer look at this example, it should be noted that 3 is a primitive root of 29, while $26 = 3^{15} \pmod{29}$ and $13 = 3^{26} \pmod{29}$. Since 0, 1, 15 and 26 are all incongruent modulo 4, this construction clearly contains all of the non-zero elements of $\mathbb{Z}_{29}$, and so satisfies (1.1.1). It is now necessary to check the differences given by (1.1.2) to (1.1.5) in order to confirm that this is the initial round of a $\mathbb{Z}$-cyclic OTWh(29).

The differences given by (1.1.2) are ± 4, $\pm 10 \times 1, 3^4, \ldots, 3^{24}$, i.e. 3^6, 3^{20}, 3^{27}, $3^{13} \times 1, 3^4, \ldots, 3^{24}$. Since 6, 20, 27 and 13 are incongruent modulo 4, condition (1.1.2) is satisfied.

(1.1.3) and (1.1.4) are satisfied similarly.

For (1.1.5), the differences are 27, 17, 23, $13 \times 1, 3^4, \ldots, 3^{24}$, i.e. 3^3, 3^{21}, 3^4, $3^{26} \times 1, 3^4, \ldots, 3^{24}$. Here, 3, 21, 4 and 26 are incongruent modulo 4 and so (1.1.5) is satisfied.

Thus (1.1.1) to (1.1.5) are satisfied and it has been confirmed that our construction is the initial round of a $\mathbb{Z}$-cyclic OTWh(29).

2.3 The Existence Theorem

We now take a closer look at some constructions which were presented by Anderson and Finizio in [12], and find the conditions which must be satisfied in order for them to produce a $\mathbb{Z}-$cyclic OTWh(p) for primes $p \equiv 5 \pmod 8$.

So let $p = 8t + 5$ be prime, let x be a non-square element of $\mathbb{Z}_p$, and let θ be a primitive root of p. We now present six constructions.

Construction 1 $(1, x, -1, x^3) \times 1, \theta^4, \ldots, \theta^{8t}$.

First we find the conditions under which this forms a TWh(p). The partner differences are pairs ± 2, $\pm x(x^2 - 1) \times 1, \theta^4, \ldots, \theta^{8t}$, and so the partner pairs form a starter provided

$2x(x^2-1)$ is not a square. Similarly the first kind opponent pairs form a starter provided $(x-1)(x^3+1)$ is not a square, and the second kind opponent pairs form a starter provided $(x+1)(x^3-1)$ is not a square. We now use the fact that 2 is a non-square since $p \equiv 5 \pmod 8$. So Construction 1 yields a $\mathbb{Z}-$cyclic TWh(p) provided x^2-1 is not a square, $x^2 \pm x + 1$ are squares.

Now we find the conditions under which this also forms an OWh(p).

Let $a = -(x-1)$, $b = -(x^2+x+1)(x-1)$, $c = -(x+1)$, $d = -(x^2-x+1)(x+1)$. We require that a, b, c, d lie in distinct cyclotomic classes of index 4. Since a/c is not a square, we require b/d to be a non-square, and, to guarantee that the two squares (non-squares) lie in distinct cyclotomic classes, we also require that each of $x^2 \pm x + 1$, although squares, are not fourth powers.

So, Construction 1 gives the initial round tables of a TWh(p) provided x^2-1 is not a square, $x^2 \pm x + 1$ are squares. They also yield an OWh(p) provided $x^2 \pm x + 1$ are both not fourth powers.

Construction 2 $(1, x^3, x^2, -x^3) \times 1, \theta^4, \ldots, \theta^{8t}$.

These are the initial round tables of a TWh(p) provided x^2-1 is not a square, $x^2 \pm x + 1$ are squares. They also yield an OWh(p) provided $x^2 \pm x + 1$ are both fourth powers.

Construction 3 $(1, x^3, -x^4, -x^3) \times 1, \theta^4, \ldots, \theta^{8t}$.

These are the initial round tables of a TWh(p) provided x^4+1 is not a square, $x^2 \pm x + 1$ are squares. We also get an OWh(p) provided $(x-1)/(x+1)$ is a square but not a fourth power and exactly one of $x^2 \pm x + 1$ is a fourth power.

Construction 4 $(1, x, -x^4, -x) \times 1, \theta^4, \ldots, \theta^{8t}$.

These are the initial round tables of a TWh(p) provided x^4+1 is not a square, $x^2 \pm x + 1$ are both squares. We also get an OWh(p) provided $(x-1)/(x+1)$ is a fourth power, and exactly one of $x^2 \pm x + 1$ is a fourth power.

Construction 5 $(1, x, -x^4, x^3) \times 1, \theta^4, \ldots, \theta^{8t}$.

For a TWh(p), we require $x^2 - 1$ is a square, $x^4 + 1$ is a square, $(x^2 + x + 1)(x^2 - x + 1)$ is a square. We also get an OWh(p) provided $x^2 + x + 1$ is not a fourth power, but $x^2 - x + 1$ is.

Construction 6 $(1, -x, -x^4, -x^3) \times 1, \theta^4, \ldots, \theta^{8t}$.

For a TWh(p), we require $x^2 - 1$ is a square, $x^4 + 1$ is a square, $(x^2 + x + 1)(x^2 - x + 1)$ is a square. We also get an OWh(p) provided $x^2 - x + 1$ is not a fourth power, but $x^2 + x + 1$ is.

Theorem 2.3.1 *Let $p = 8t + 5$ be prime. If there exists a non-square element x of $\mathbb{Z}_p$ such that $x^2 \pm x + 1$ are both squares and either*

$x^2 - 1$ is not a square and $(x^2 + x + 1)(x^2 - x + 1)$ is a fourth power, or

$x^2 - 1$ is a square and $(x^2 + x + 1)(x^2 - x + 1)$ is not a fourth power,

then a $\mathbb{Z}-$cyclic OTWh(p) exists.

Proof

Suppose there exists such a non-square x. If it happens that $x^2 - 1$ is not a square, use Construction 2 if both $x^2 \pm x + 1$ are fourth powers and use Construction 1 otherwise. So suppose now that $x^2 - 1$ is a square, i.e., $(x - 1)/(x + 1)$ is a square. Next suppose $x^4 + 1$ is not a square. Since exactly one of $x^2 \pm x + 1$ is a fourth power, we can use Construction 4 if $(x - 1)/(x + 1)$ is a fourth power and Construction 3 otherwise. Finally, if $x^2 - 1$ is a square and $x^4 + 1$ is a square, use Construction 6 if $x^2 + x + 1$ is a fourth power and Construction 5 otherwise.

□

It therefore remains to show that a non-square x satisfying the conditions of Theorem 2.3.1 can be obtained.

Let λ denote the quadratic character mod p, so that $\lambda(y) = -1$ if y is not a square. Let ψ be any fixed character of order 4 exactly; then $\psi(y) = 1$ if y is a fourth power, and

$\psi(y) = -1$ if y is a square but not a fourth power. Let

$$S = \sum_{x \in \mathrm{GF}(p)} (1-\lambda(x))(\lambda(x^2-x+1)+1)(\lambda(x^2+x+1)+1) \times (1-\psi((x^2+x+1)(x^2-x+1)(x^2-1)^2)).$$

There is no contribution to S when $x = 0$ since $\psi((x^2+x+1)(x^2-x+1)(x^2-1)^2) = 1$. Similarly, there is no contribution when $x^2 - 1 = 0$ or $x^2 \pm x + 1 = 0$. To see this, we let $x = \theta^\alpha$. Then,

$$\text{if } x^2 - 1 = 0,$$
$$x^2 = 1.$$

$$\text{If } x^2 + x + 1 = 0,$$
$$x^2 = -x - 1,$$
$$x^3 = -x^2 - x = -(x^2 + x) = 1.$$

$$\text{If } x^2 - x + 1 = 0,$$
$$x^2 = x - 1,$$
$$x^3 = x^2 - x = -1,$$
$$\text{i.e. } x^6 = 1.$$

So $\theta^{2\alpha} = 1$ or $\theta^{3\alpha} = 1$ or $\theta^{6\alpha} = 1$. Since $\theta^{8t+4} = 1$, $4|2\alpha$ or $4|3\alpha$ or $4|6\alpha$. This means that x must be a square and so $1 - \lambda(x) = 0$ and thus the overall contribution to S is 0.

So $S = 16|A|$ where A is the set of non-square elements of $\mathbb{Z}_p$ satisfying the conditions of Theorem 2.3.1.

Since $\lambda(x) = \psi(x^2)$,

$$S = \sum_{x \in \mathrm{GF}(p)} (1-\psi(x^2))(\psi((x^2-x+1)^2)+1)(\psi((x^2+x+1)^2)+1) \times (1-\psi((x^2+x+1)(x^2-x+1)(x-1)^2(x+1)^2)).$$

Thus,

$$
\begin{aligned}
S \geq p - & \left| \sum_{x \in \mathrm{GF}(p)} \psi\left((x^2-x+1)^2(x^2+x+1)^2\right) \right| \\
& - \left| \sum_{x \in \mathrm{GF}(p)} \psi\left((x^2-x+1)^2\right) \right| - \left| \sum_{x \in \mathrm{GF}(p)} \psi((x^2+x+1)^2) \right| \\
& - \left| \sum_{x \in \mathrm{GF}(p)} \psi\left((x^2-x+1)^3(x^2+x+1)^3(x-1)^2(x+1)^2\right) \right| \\
& - \left| \sum_{x \in \mathrm{GF}(p)} \psi\left((x^2-x+1)^3(x^2+x+1)(x-1)^2(x+1)^2\right) \right| \\
& - \left| \sum_{x \in \mathrm{GF}(p)} \psi\left((x^2-x+1)(x^2+x+1)^3(x-1)^2(x+1)^2\right) \right| \\
& - \left| \sum_{x \in \mathrm{GF}(p)} \psi\left((x^2-x+1)(x^2+x+1)(x-1)^2(x+1)^2\right) \right| \\
& - \Bigg| \sum_{x \in \mathrm{GF}(p)} (\psi(x^2))(\psi((x^2-x+1)^2)+1)(\psi((x^2+x+1)^2)+1) \times \\
& \qquad (1-\psi((x^2+x+1)(x^2-x+1)(x-1)^2(x+1)^2)) \Bigg|.
\end{aligned}
$$

After multiplying this out fully and making the appropriate substitutions (using Theorem 1.4.1), it can be seen that

$$
\begin{gathered}
S \geq p - (25\sqrt{p} + 32\sqrt{p}), \\
\text{i.e. } S \geq p - 57\sqrt{p}.
\end{gathered}
$$

Thus,

$$
\begin{gathered}
S = 16|A| \geq p - 57\sqrt{p} > 0 \text{ if } p \geq 57\sqrt{p}, \\
\text{i.e. if } p > 3,249.
\end{gathered}
$$

It was then checked by computer that appropriate values of x existed for all primes $29 \leq p < 3,249$ where $p \equiv 5 \pmod 8$, excluding $p = 29$. But an OTWh(p) has already been constructed for this value of p in Section 2.2. Here, we list (p, x_p) where p is the prime and x_p is the smallest suitable value of x for that prime. Some further information about one of the programming techniques which can be used to obtain the following results is given in Appendix A.

$(37,2)$, $(53,14)$, $(61,8)$, $(101,32)$, $(109,14)$, $(149,34)$, $(157,32)$, $(173,7)$, $(181,22)$, $(197,12)$, $(229,21)$, $(269,29)$, $(277,2)$, $(293,8)$, $(317,8)$, $(349,8)$, $(373,18)$, $(389,3)$,

$(397,6)$, $(421,2)$, $(461,10)$, $(509,7)$, $(541,2)$, $(557,11)$, $(613,2)$, $(653,12)$, $(661,6)$, $(677,12)$, $(701,3)$, $(709,22)$, $(733,8)$, $(757,24)$, $(773,12)$, $(797,7)$, $(821,12)$, $(829,40)$, $(853,6)$, $(877,2)$, $(941,7)$, $(997,44)$, $(1013,41)$, $(1021,43)$, $(1061,14)$, $(1069,26)$, $(1093,22)$, $(1109,42)$, $(1117,2)$, $(1181,15)$, $(1213,5)$, $(1229,17)$, $(1237,15)$, $(1277,28)$, $(1301,39)$, $(1373,12)$, $(1381,10)$, $(1429,2)$, $(1453,18)$, $(1493,11)$, $(1549,40)$, $(1597,2)$, $(1613,57)$, $(1621,18)$, $(1637,41)$, $(1669,10)$, $(1693,11)$, $(1709,40)$, $(1733,32)$, $(1741,6)$, $(1789,37)$, $(1861,39)$, $(1877,52)$, $(1901,10)$, $(1933,14)$, $(1949,27)$, $(1973,26)$, $(1997,20)$, $(2029,24)$, $(2053,5)$, $(2069,15)$, $(2141,8)$, $(2213,18)$, $(2221,2)$, $(2237,20)$, $(2269,2)$, $(2293,24)$, $(2309,8)$, $(2333,8)$, $(2341,54)$, $(2357,5)$, $(2381,47)$, $(2389,23)$, $(2437,5)$, $(2477,5)$, $(2549,8)$, $(2557,2)$, $(2621,7)$, $(2677,79)$, $(2693,27)$, $(2741,18)$, $(2749,10)$, $(2789,13)$, $(2797,2)$, $(2837,3)$, $(2861,26)$, $(2909,10)$, $(2917,52)$, $(2957,61)$, $(3037,22)$, $(3061,2)$, $(3109,2)$, $(3181,28)$, $(3221,8)$, $(3229,33)$.

Thus the following theorem is established.

Theorem 2.3.2 *A $\mathbb{Z}$-cyclic* OTWh(p) *exists for all primes* $p \equiv 5 \pmod 8$, $p \geq 29$.

Example 2.3.1 A $\mathbb{Z}$−cyclic OTWh(37) is given by the initial round
$(1,8,21,29)$, $(7,19,36,18)$, $(9,35,4,2)$, $(10,6,25,31)$, $(12,22,30,15)$,
$(16,17,3,20)$, $(26,23,28,14)$, $(33,5,27,32)$, $(34,13,11,24)$.

Example 2.3.2 The suitable values of x when $p = 37$ are $2, 18, 19, 35$.

We are now in a position to state the following, as similarly given for DTWh(v) in [12]. The existence of an OTWh(29) and an OTWh(37) is enough to guarantee the existence of an OTWh(v) for all sufficiently large $v \equiv 1 \pmod 4$.

Theorem 2.3.3 *An* OTWh(v) *exists for all sufficiently large* $v \equiv 1 \pmod 4$.

Proof

It follows from the results of Wilson [35] that a pairwise balanced design, PBD($\{29,37\}, v$) exists for all sufficiently large $v \equiv 1 \pmod 4$. On each block B of this PBD, form an OTWh($|B|$). Then for each x, take the blocks B containing x and, for each such B, take all the tables of the round of the OTWh on B in which x sits out. These games will form a round, which we label as round x, of the required OTWh(v). It is clear that the triplewhist and ordered whist properties are preserved by this construction.

□

2.4 $\mathbb{Z}$-Cyclic Ordered Triplewhist and Directed Triplewhist Tournaments on p elements, where $p \equiv 9 \pmod{16}$

Abel, Costa and Finizio [1] have dealt with whist tournaments which are simultaneously directed and ordered. We shall now look at whist tournaments which are simultaneously either both triplewhist and directed tournaments, or triplewhist and ordered tournaments. The former will be called *directed triplewhist tournaments* and will be denoted by $DTWh(v)$. The latter we have already seen in Sections 2.2 and 2.3. First of all though, it should be noted that it is not possible for a $\mathbb{Z}$-cyclic tournament to be triplewhist, ordered and directed at the same time.

Theorem 2.4.1 *It is not possible for a $\mathbb{Z}$-cyclic tournament to be triplewhist, ordered and directed simultaneously.*

Proof

Firstly we will assume that such a tournament does exist. The fact that it is an ordered and directed tournament means that from (1.1.5) and (1.1.6) we can deduce that

$$\bigcup_{i=1}^{m}\{(a_i - b_i), (c_i - d_i)\} = \bigcup_{i=1}^{m}\{-(a_i - b_i), -(c_i - d_i)\} \qquad (2.4.1)$$

and that both sides of the equation (2.4.1) give the same half of the non-zero elements of $\mathbb{Z}_p$. Since the tournament is also triplewhist, (1.1.3) tells us that

$$\bigcup_{i=1}^{m}\{\pm(a_i - b_i), \pm(c_i - d_i)\} = \mathbb{Z}_{4m+1} - \{0\}.$$

This contradicts (2.4.1).

□

We shall now show that both $\mathbb{Z}$-cyclic $DTWh(v)$ and $\mathbb{Z}$-cyclic $OTWh(v)$ exist for all v whenever v is a prime $p \equiv 9 \pmod{16}$. For $p \equiv 5 \pmod 8$, the directed case has been dealt with in [12] while the ordered case has been dealt with in [7] (and in Section 2.3 above).

Notation. Any non-zero element k of $\mathbb{Z}_p$ can be expressed as θ^m where θ is a primitive root of p. If $b \mid p-1$ and if $m \equiv a \pmod b$, we say that $k \in C_a^b$.

2.5 The Existence Theorem

We now take a closer look at two constructions and find the conditions which must be satisfied in order for them to produce a $\mathbb{Z}$-cyclic $DTWh(p)$ and a $\mathbb{Z}$-cyclic $OTWh(p)$ for primes $p \equiv 9 \pmod{16}$.

So let $p = 16t + 9$ be prime, let x be a non-square element of $\mathbb{Z}_p$, and let θ be a primitive root of p. We now present two constructions, the first of which is a variation of a construction found in [27, p. 222].

Construction 7 $(1, x, x^4, -x) \times \theta^{8i+2j}$, $0 \leq i \leq 2t$, $0 \leq j \leq 1$.

It can be seen that this is a suitable construction since if 1, x, x^4 and $-x$ are expressed in terms of θ, we have two square terms whose indices differ by 4 (mod 8), and two non-square terms whose indices differ by 4 (mod 8). This means that when they are multiplied by θ^{8i+2j} for appropriate values of i and j, we get all of the non-zero elements of $\mathbb{Z}_p$ as required. First we find the conditions under which this forms a $TWh(p)$. The partner differences are pairs $\pm 2x$, $\pm(x^4 - 1) \times \theta^{8i+2j}$, and so the partner pairs form a starter provided $2x(x^4 - 1)$ is not a square. Similarly the first kind opponent pairs form a starter provided $x(x-1)(x^3+1)$ is not a square, and the second kind opponent pairs form a starter provided $x(x+1)(x^3-1)$ is not a square. We now use the fact that 2 is a square since $p \equiv 9 \pmod{16}$. So Construction 7 yields the initial round tables of a $\mathbb{Z}$-cyclic $TWh(p)$ provided $x^4 - 1$, $(x-1)(x^3+1)$ and $(x+1)(x^3-1)$ are all square.

Now we find the conditions under which this also forms a $DWh(p)$. Here, the differences we are interested in are

$$x - 1, \tag{2.5.1}$$

$$x^4 - x = x(x^3 - 1) = x(x-1)(x^2 + x + 1), \tag{2.5.2}$$

$$-x - x^4 = -x(x^3 + 1) = -x(x+1)(x^2 - x + 1), \tag{2.5.3}$$

$$x + 1. \tag{2.5.4}$$

We now make the assumption that $x^2 - 1$ is not a square. It follows from such an assumption that one of $x-1$ and $x+1$ is a square, while the other is non-square. Using this information together with the conditions for $TWh(p)$, it can be seen that (2.5.1) and (2.5.2) are both square (non-square), while (2.5.3) and (2.5.4) are both non-square (square). For the construction to work, the indices of the two square (non-square) values must also differ by 4 (working mod 8).

Thus, we obtain a $DWh(p)$ using this construction when

$$\frac{x(x-1)(x^2+x+1)}{(x-1)} \in C_4^8, \text{ i.e. } x(x^2+x+1) \in C_4^8,$$
$$\text{i.e. } x^5(x^2+x+1) \in C_0^8,$$

and,

$$\frac{-x(x+1)(x^2-x+1)}{(x+1)} \in C_4^8, \text{ i.e. } -x(x^2-x+1) \in C_4^8,$$
$$\text{i.e. } x(x^2-x+1) \in C_0^8.$$

So, using all of the above information we can say that Construction 7 gives the initial round tables of a $\mathbb{Z}$-cyclic $DTWh(p)$ when x is not a square, x^2-1 is not a square, x^2+1 is not a square, $x^5(x^2+x+1) \in C_0^8$, $x(x^2-x+1) \in C_0^8$.

Now we go back and find the conditions under which Construction 7 gives the initial round tables of what is also an $OWh(p)$. Here, the differences we are interested in are

$$1-x = -(x-1), \tag{2.5.5}$$

$$x+1, \tag{2.5.6}$$

$$x^4 - x = x(x^3-1) = x(x-1)(x^2+x+1), \tag{2.5.7}$$

$$x^4 + x = x(x^3+1) = x(x+1)(x^2-x+1). \tag{2.5.8}$$

Again we assume that x^2-1 is not a square. Using the same process as above it is seen that (2.5.6) and (2.5.8) are both square (non-square) elements of $\mathbb{Z}_p$ while (2.5.5) and (2.5.7) are non-square (square). Again, the indices of the two square (non-square) values must differ by 4 (working mod 8), so it can be seen that we obtain an $OWh(p)$ using this construction when

$$\frac{x(x-1)(x^2+x+1)}{-(x-1)} \in C_4^8 \text{ i.e. } -x(x^2+x+1) \in C_4^8$$
$$\text{i.e. } x(x^2+x+1) \in C_0^8,$$

and,

$$\frac{x(x+1)(x^2-x+1)}{(x+1)} \in C_4^8 \text{ i.e. } x(x^2-x+1) \in C_4^8$$
$$\text{i.e. } x^5(x^2-x+1) \in C_0^8.$$

So, using all of the above information we can say that Construction 7 gives us the initial round tables of a $\mathbb{Z}$-cyclic $OTWh(p)$ when x is not a square, x^2-1 is not a square, x^2+1 is not a square, $x^5(x^2-x+1) \in C_0^8$, $x(x^2+x+1) \in C_0^8$.

Construction 8 $(1, x^3, x^4, -x^3) \times \theta^{8i+2j}$, $0 \le i \le 2t$, $0 \le j \le 1$.

It can be seen that this is a suitable construction since if 1, x^3, x^4 and $-x^3$ are expressed in terms of θ, we have two square terms whose indices differ by 4 (mod 8), and two non-square terms whose indices differ by 4 (mod 8). This means that when they are multiplied by θ^{8i+2j} for appropriate values of i and j, we get all of the non-zero elements of $\mathbb{Z}_p$ as required. These are the initial round tables of a $\mathbb{Z}$-cyclic $TWh(p)$ provided x^4-1, $(x-1)(x^3+1)$ and $(x+1)(x^3-1)$ are all square. Combining this with the assumption that x^2-1 is not a square, we see that Construction 8 gives the initial round tables of a $\mathbb{Z}$-cyclic $DTWh(p)$ when x is not a square, x^2-1 is not a square, x^2+1 is not a square, $x^5(x^2-x+1) \in C_0^8$, $x(x^2+x+1) \in C_0^8$. It is also the case that it gives a $\mathbb{Z}$-cyclic $OTWh(p)$ when x is not a square, x^2-1 is not a square, x^2+1 is not a square, $x^5(x^2+x+1) \in C_0^8$, $x(x^2-x+1) \in C_0^8$.

Theorem 2.5.1 *Let $p = 16t+9$ be prime. If there exists a non-square element x of $\mathbb{Z}_p$ such that $x^2 \pm 1$ are both non-square and either*

$x(x^2+x+1) \in C_0^8$ and $x^5(x^2-x+1) \in C_0^8$, or

$x(x^2-x+1) \in C_0^8$ and $x^5(x^2+x+1) \in C_0^8$,

then a $\mathbb{Z}$-cyclic $DTWh(p)$ ($\mathbb{Z}$-cyclic $OTWh(p)$) exists.

Proof

Suppose there exists such a non-square x. If $x(x^2-x+1) \in C_0^8$ and $x^5(x^2+x+1) \in C_0^8$

then use Construction 7 (Construction 8). If $x(x^2+x+1) \in C_0^8$ and $x^5(x^2-x+1) \in C_0^8$ then use Construction 8 (Construction 7).

□

It therefore remains to show that a non-square x satisfying the conditions of Theorem 2.5.1 can be obtained.

It can be seen that this task is assisted by the fact that working with Construction 7 and Construction 8 results in the same conditions being required in order to show that a suitable x exists in order for a directed triplewhist and an ordered triplewhist tournament to be built. Thus, if x is not a square, $x^2 \pm 1$ are not square, $x(x^2+x+1) \in C_0^4$ and $x^2(x^2+x+1)(x^2-x+1) \in C_4^8$ then a suitable value of x exists such that a $\mathbb{Z}$-cyclic $DTWh(p)$ and a $\mathbb{Z}$-cyclic $OTWh(p)$ can be constructed using either Construction 7 or Construction 8.

Let λ denote the quadratic character mod p, so that

$$\lambda(y) = \begin{cases} 1 & \text{if } y \in C_0^2; \\ -1 & \text{if } y \in C_1^2; \\ 0 & \text{if } y = 0. \end{cases}$$

Let ψ be the character of order 4 exactly which is defined by

$$\psi(y) = \begin{cases} 1 & \text{if } y \in C_0^4; \\ -1 & \text{if } y \in C_2^4; \\ i & \text{if } y \in C_1^4; \\ -i & \text{if } y \in C_3^4; \\ 0 & \text{if } y = 0. \end{cases}$$

Let χ be the character of order 8 exactly which is defined by

$$\chi(y) = \begin{cases} \omega^j & \text{if } y \in C_j^8; \\ 0 & \text{if } y = 0. \end{cases}$$

where $\omega = e^{\frac{\pi i}{4}}$.

It follows from these definitions that

$$1 - \lambda(y) = \begin{cases} 2 & \text{if } y \in C_1^2; \\ 1 & \text{if } y = 0; \\ 0 & \text{otherwise,} \end{cases}$$

$$1 + \psi(y) + \psi(y^2) + \psi(y^3) = \begin{cases} 4 & \text{if } y \in C_0^4; \\ 1 & \text{if } y = 0; \\ 0 & \text{otherwise,} \end{cases}$$

and

$$1 + \chi(y) + \ldots + \chi(y^7) = \begin{cases} 8 & \text{if } y \in C_0^8; \\ 1 & \text{if } y = 0; \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we let $f(x) = x(x^2 + x + 1)$, $g(x) = x^6(x^2 + x + 1)(x^2 - x + 1)$ and

$$S = \sum_{x \in GF(p)} (1 - \lambda(x))(1 - \lambda(x^2 - 1))(1 - \lambda(x^2 + 1)) \times$$
$$(1 + \psi(f(x)) + \ldots + \psi(f^3(x)))(1 + \chi(g(x)) + \ldots + \chi(g^7(x))).$$

Substituting in the fact that $\lambda(x) = \psi(x^2) = \chi(x^4)$ it is seen that

$$S = \sum_{x \in GF(p)} (1 - \chi(x^4))(1 - \chi(x^2 - 1)^4)(1 - \chi(x^2 + 1)^4) \times$$
$$(1 + \chi(f^2(x)) + \ldots + \chi(f^6(x)))(1 + \chi(g(x)) + \ldots + \chi(g^7(x))),$$

i.e.

$$S = \sum_{x \in \mathrm{GF}(p)} (1 - \chi(x^4) - \chi((x^2 - 1)^4) - \chi((x^2 + 1)^4) + \chi(x^4(x^2 - 1)^4)$$
$$+\chi(x^4(x^2 + 1)^4) + \chi((x^2 - 1)^4(x^2 + 1)^4) - \chi(x^4(x^2 - 1)^4(x^2 + 1)^4) \times$$
$$(1 + \chi(f^2(x)) + \ldots + \chi(f^6(x)))(1 + \chi(g(x)) + \ldots + \chi(g^7(x))).$$

After multiplying this out and making the appropriate substitutions (using Theorem 1.4.1), it can be seen that,

$$S \geq p - 1453\sqrt{p}.$$

It is also clearly the case that,

$$S = 256|A|,$$

where elements in A are of the form given in Theorem 2.5.1. As in the $p \equiv 5 \pmod 8$ case, there is no contribution when $x = 0$. Nor is there one when $x^2 \pm 1 = 0$, $f(x) = 0$ or $g(x) = 0$.

Thus,

$$S = 256|A| \geq p - 1453\sqrt{p} > 0 \text{ if } p \geq 1453\sqrt{p},$$
$$\text{i.e. if } \sqrt{p} \geq 1453,$$
$$\text{i.e. if } p > 2,111,209.$$

It was then checked by computer that appropriate values of x existed for all primes $p < 2,111,209$ where $p \equiv 9 \pmod{16}$, excluding $p =$ 41, 73, 89, 137, 233, 281, 313, 521, 569, 617, 809, 1097, 2729, 2953, 3001. Here, we list (p, x_p) where p is the prime and x_p is a suitable value of x for that prime for all relevant primes $p < 10,000$.

(409, 79), (457, 10), (601, 142), (761, 142), (857, 268), (937, 132), (953, 344), (1033, 103), (1049, 82), (1129, 119), (1193, 27), (1289, 208), (1321, 76), (1433, 605), (1481, 29), (1609, 479), (1657, 164), (1721, 12), (1753, 89), (1801, 130), (1913, 171), (1993, 542), (2089, 194), (2137, 157), (2153, 888), (2281, 402), (2297, 520), (2377, 454), (2393, 259), (2441, 411), (2473, 812), (2521, 34), (2617, 19), (2633, 5), (2713, 163), (2777, 659), (2857, 106), (2969, 505), (3049, 153), (3209, 383), (3257, 68), (3433, 14), (3449, 350), (3529, 115), (3593, 84), (3673, 115), (3769, 1344), (3833, 38), (3881, 24), (3929, 375), (4057, 111), (4073, 871), (4153, 71), (4201, 130), (4217, 329), (4297, 193), (4409, 709), (4441, 467), (4457, 377), (4649, 102), (4729, 218), (4793, 122), (4889, 1197), (4937, 21), (4969, 21), (5081, 164), (5113, 79), (5209, 218), (5273, 606), (5417, 56), (5449, 570), (5641, 616), (5657, 496), (5689, 190), (5737, 173), (5801, 165), (5849, 24), (5881, 351), (5897, 104), (6073, 60), (6089, 381), (6121, 29), (6217, 383), (6329, 651), (6361, 272), (6473, 173), (6521, 124), (6553, 88), (6569, 953), (6761, 243), (6793, 181), (6841, 164), (6857, 111), (7001, 108), (7129, 332), (7177, 805), (7193, 39), (7321, 138), (7369, 127), (7417, 335), (7433, 10), (7481, 295), (7529, 528), (7561, 52), (7577, 117), (7673, 996), (7753, 519), (7817, 113), (7993, 114), (8009, 328), (8089, 61), (8233, 245), (8297, 443), (8329, 88), (8377, 233), (8521, 109), (8537, 258), (8681, 29), (8713, 59), (8761, 344), (8969, 583), (9001, 29), (9049, 656), (9161, 473), (9209, 54), (9241, 174), (9257, 57), (9337, 207), (9433, 77), (9497, 888), (9689, 803), (9721, 688), (9769, 426), (9817, 515), (9833, 14), (9929, 603).

It has been already been shown in [13] that for all primes $p \equiv 1 \pmod 4$, $29 \leq p \leq 10,000$, $p \neq$ 97, 193, 257, 449, 641, 769, 1153, 1409, 7681, there exist $\mathbb{Z}$-cyclic $DTWh(p)$. This takes care of the 15 values for which a suitable value of x was not found by the computer (as listed above).

Thus the following theorem is established.

Theorem 2.5.2 *A $\mathbb{Z}$-cyclic $DTWh(p)$ exists for all primes $p \equiv 9 \ (mod\ 16)$.*

In order to have proved a similar theorem for $\mathbb{Z}$-cyclic $OTWh(p)$ where $p \equiv 9 \pmod{16}$ is prime, all that is left to do is show that a $\mathbb{Z}$-cyclic $OTWh(p)$ exists for each of the 15 values listed above. To assist in this task, the following construction (as given in [27, p. 224]) is used.

Construction 9 Let $p = 2^k t + 1$ be prime, $k \geq 3$, t odd and let θ be a primitive root of p . For the purposes of working with this construction, we write $d = 2^k$, $n = 2^{k-2}$ and $a \equiv 2^{k-1} - 1 \pmod{d}$. Then we consider the following initial round games

$$(1, \theta, -\theta, \theta^{a+1}) \times \theta^{2i+dj},\ 0 \leq i \leq n-1,\ 0 \leq j \leq t-1.$$

For 13 of the 15 values that we are interested in, it is now possible to list (p, θ, a) where p is the prime, θ is a suitable primitive root and a is a suitable value which, when substituted into Construction 9, give the initial round games of a $\mathbb{Z}$-cyclic $OTWh(p)$.

$$(89,35,51),\ (137,45,11),\ (233,138,11),\ (281,178,11),\ (313,268,19),\ (521,85,3),$$
$$(569,96,3),\ (617,337,3),\ (809,396,3),\ (1097,382,3),\ (2729,27,3),\ (2953,1264,3),$$
$$(3001,1305,3).$$

Thus it has now been shown that a $\mathbb{Z}$-cyclic $OTWh(p)$ exists for all $p \equiv 9 \pmod{16}$ where p is prime, with the possible exception of $p = 41$ and $p = 73$.

Using two constructions given in [26], the following initial round games were found which generate $\mathbb{Z}$-cyclic $OTWh(p)$ for $p = 41$ and 73.

Example 2.5.1 A $\mathbb{Z}$-cyclic $OTWh(41)$ is given by the initial round

$$\{\{1,27,40,28\},\{20,30,39,19\}\} \times \{1, 26^8, \ldots, 26^{32}\}.$$

Example 2.5.2 A $\mathbb{Z}$-cyclic $OTWh(73)$ is given by the initial round

$$\{\{1,18,59,43\},\{50,6,30,5\}\} \times \{1, 59^8, \ldots, 59^{64}\}.$$

Thus the following theorem is established.

Theorem 2.5.3 *A $\mathbb{Z}$-cyclic $OTWh(p)$ exists for all primes $p \equiv 9 \pmod{16}$.*

Having proved the existence of a $\mathbb{Z}$-cyclic $OTWh(p)$ for $p \equiv 5 \pmod 8$, $p \geq 29$ and for $p \equiv 9 \pmod{16}$, the following seems to be a sensible suggestion.

Conjecture 2.5.1 *A $\mathbb{Z}$-cyclic $OTWh(p)$ exists for all primes $p \equiv 1 \pmod 4$, $p \geq 29$.*

2.6 $\mathbb{Z}$-Cyclic Directed Moore $(2,6)$ Generalised Whist Tournament Designs on p elements, where $p \equiv 7 \pmod{12}$

A generalised whist tournament design, as discussed in [3], is a schedule of games for a tournament involving v players to be played in $v-1$ or v rounds (depending on the number of players involved). For the purposes of this work, which will be dealing with tournaments on p elements, where $p \equiv 7 \pmod{12}$ is prime, the tournaments will be arranged into v rounds. A game involves k players in a multi-team game with teams of t players competing, and a round consists of $(v-1)/k$ (or v/k) simultaneous games, with a player playing in at most one of these. The schedule must also be balanced in the sense that each pair of players play together as teammates in $(t-1)$ games, and as opponents in $(k-t)$ games. Such a schedule of games will be denoted by (t,k) $GWhD(v)$.

Here, we will be looking at a specific type of $(2,6)$ $GWhD(6m+1)$ on $6m+1$ players. $(2,6)$ $GWhD(v)$ are discussed in [2]. Such a design is a schedule of games (or tables) $(a, b; c, d; e, f)$ involving three teams of two players competing against each other such that

i. the games are arranged into $6m+1$ rounds each of m games;

ii. each player plays in exactly one game in all but one round;

iii. each player partners every other player exactly once;

iv. each player opposes every other player exactly four times.

If we consider the players as being seated around a circular table, then we can think of $(a, b; c, d; e, f)$ as the ordered block $\{a, c, e, b, d, f\}$. Suppose that $(a, b; c, d; e, f)$ is a game in a $(2,6)$ $GWhD(6m+1)$. Then we say that the pairs $\{a,b\}$, $\{c,d\}$, $\{e,f\}$ are *partners.* $\{a,c\}$, $\{b,e\}$, $\{d,f\}$ are said to be pairs of *opponents of the first kind.* $\{a,e\}$, $\{b,d\}$, $\{c,f\}$ are said to be pairs of *opponents of the second kind.* $\{a,f\}$, $\{b,c\}$, $\{d,e\}$ are said to be pairs of *opponents of the third kind.* $\{a,d\}$, $\{b,f\}$, $\{c,e\}$ are said to be pairs of *opponents of the fourth kind.* This $(2,6)$ $GWhD(6m+1)$ is described as a *moore* $(2,6)$ $GWhD(6m+1)$ if every player has every other player exactly once as an opponent of the first kind, opponent of the second kind, opponent of the third kind and opponent of the fourth kind. These are called *moore tournaments* because of E. H. Moore's discussion of a similar specialisation of whist tournaments in [31], and were first referred to as such in [21]. If we consider our block $\{a, c, e, b, d, f\}$ as players sitting at a circular table in the given order, then we can refer to c as a's *first left hand opponent*, e as a's *second left hand opponent*, f as a's *first right hand opponent* and d as a's *second right hand opponent*. We can make similar definitions for each of b, c, d, e and f. A *directed* $(2,6)$ $GWhD(6m+1)$ is a $(2,6)$ $GWhD(6m+1)$ in which each player is a first left hand opponent, second left hand opponent, first right hand opponent and second right hand opponent of every other player exactly once.

This time, we say that the tournament is $\mathbb{Z}$-cyclic if the players are elements of $\mathbb{Z}_{6m+1}$, and if the ith round is obtained from the initial (first) round by adding $i-1$ to each element (mod $6m+1$). The games (tables)

$$(a_1, b_1; c_1, d_1; e_1, f_1), \ldots, (a_m, b_m; c_m, d_m; e_m, f_m)$$

form the initial round of a $\mathbb{Z}$-cyclic moore $(2,6)$ generalised whist tournament design if

$$\bigcup_{i=1}^{m} \{a_i, b_i; c_i, d_i; e_i, f_i\} = \mathbb{Z}_{6m+1} - \{0\}, \tag{2.6.1}$$

$$\bigcup_{i=1}^{m} \{\pm(a_i - b_i), \pm(c_i - d_i), \pm(e_i - f_i)\} = \mathbb{Z}_{6m+1} - \{0\}, \tag{2.6.2}$$

$$\bigcup_{i=1}^{m} \{\pm(a_i - c_i), \pm(b_i - e_i), \pm(d_i - f_i)\} = \mathbb{Z}_{6m+1} - \{0\}, \tag{2.6.3}$$

$$\bigcup_{i=1}^{m} \{\pm(a_i - e_i), \pm(b_i - d_i), \pm(c_i - f_i)\} = \mathbb{Z}_{6m+1} - \{0\}, \tag{2.6.4}$$

$$\bigcup_{i=1}^{m} \{\pm(a_i - f_i), \pm(b_i - c_i), \pm(d_i - e_i)\} = \mathbb{Z}_{6m+1} - \{0\}, \tag{2.6.5}$$

$$\bigcup_{i=1}^{m} \{\pm(a_i - d_i), \pm(b_i - f_i), \pm(c_i - e_i)\} = \mathbb{Z}_{6m+1} - \{0\}. \tag{2.6.6}$$

These games form a directed $(2,6)$ $GWhD(6m+1)$ if, in addition to satisfying (2.6.1) and (2.6.2),

$$\bigcup_{i=1}^{m} \{(c_i - a_i), (e_i - c_i), (b_i - e_i), (d_i - b_i), (f_i - d_i), (a_i - f_i)\}$$

$$= \mathbb{Z}_{6m+1} - \{0\}, \qquad (2.6.7)$$

$$\bigcup_{i=1}^{m} \{(e_i - a_i), (b_i - c_i), (d_i - e_i), (f_i - b_i), (a_i - d_i), (c_i - f_i)\}$$

$$= \mathbb{Z}_{6m+1} - \{0\}. \qquad (2.6.8)$$

We shall now show that a $\mathbb{Z}$-cyclic directed moore $(2,6)$ $GWhD(v)$ exists for all v whenever v is a prime $p \equiv 7 \pmod{12}$, with the definite exception of $p = 7$, and the possible exception of $p = 19$ and $p = 31$.

Notation. As seen previously, any non-zero element k of $\mathbb{Z}_p$ can be expressed as θ^m where θ is a primitive root of p. If $b \mid p-1$ and if $m \equiv a \pmod{b}$, we say that $k \in C_a^b$.

2.7 The Existence Theorem

We now take a close look at a construction and find the conditions which must be satisfied for it to produce a directed moore $(2,6)$ $GWhD(6m+1)$.

So let $p = 12t+7$ be prime and let θ be a primitive root of p. We now present a construction.

Construction 10 $(1, -1; x, -x; x^2, -x^2) \times 1, \theta^6, \ldots, \theta^{12t}$.

It can be seen that this may be a suitable construction if x is not a cube since if 1, -1, x, $-x$, x^2 and $-x^2$ are expressed in terms of θ, multiplying by θ^{6i} for appropriate values of i gives all of the non-zero elements of $\mathbb{Z}_p$ as required. First we find the conditions under which this forms a $\mathbb{Z}$-cyclic moore $(2,6)$ $GWhD(6m+1)$. The partner differences are ± 2, $\pm 2x$, $\pm 2x^2$. Looking at these in conjunction with (2.6.2) we see that, as above, they give every non-zero element of $\mathbb{Z}_p$ when x is not a cube. The differences involving opponents of the first kind are $\pm(x-1)$, $\pm(x^2+1)$, $\pm x(x-1)$. Considering these in conjunction with (2.6.3) allows us to conclude that if $(x^2+1)/x^2(x-1)$ is a cube, then the differences give every non-zero element of $\mathbb{Z}_p$. The differences involving opponents of the third kind are $\pm(x^2+1)$, $\pm(x+1)$, $\pm x(x+1)$. Considering these in conjunction with (2.6.5) allows us to conclude that $(x^2+1)/x^2(x+1)$ being a cube suffices. Combining these two pieces of information it can now be seen that we require $(x-1)/(x+1)$ to be a cube. The differences involving opponents of the second kind are $\pm(x^2-1)$, $\pm(x-1)$, $\pm x(x+1)$. But we can now express these as $\pm(x^2-1)$, $\pm(x+1)y$ where $y \in C_0^3$, $\pm x(x+1)$. Considering these in conjunction with (2.6.4) it can be seen that it is sufficient to require that

$$\begin{aligned}(x^2-1)/x^2(x+1) &\text{ is a cube,}\\ \text{i.e. } (x-1)/x^2 &\text{ is a cube,}\\ \text{i.e. } (x+1)/x^2 &\text{ is a cube.}\end{aligned}$$

The differences involving opponents of the fourth kind are $\pm(x^2-1)$, $\pm(x+1)$, $\pm x(x-1)$. We can express these as $\pm(x^2-1)$, $\pm(x-1)y$ where $y \in C_0^3$, $\pm x(x-1)$. Considering these in conjunction with (2.6.6) allows us to see that again it is sufficient for $(x-1)/x^2$ to be a cube.

So we can now see that Construction 10 gives us the initial round tables of a $\mathbb{Z}$-cyclic moore $(2,6)$ $GWhD(6m+1)$ when

$$\begin{aligned}&x \text{ is not a cube,}\\ (x-1)/x^2 \text{ is a cube,}\quad &\text{i.e.}\quad x(x-1) \text{ is a cube;}\\ (x+1)/x^2 \text{ is a cube,}\quad &\text{i.e.}\quad x(x+1) \text{ is a cube;}\\ (x^2+1)/x \text{ is a cube,}\quad &\text{i.e.}\quad x^2(x^2+1) \text{ is a cube.}\end{aligned}$$

Now we want to look at the conditions under which such a $\mathbb{Z}$-cyclic moore $(2,6)$ $GWhD(6m+1)$ will also be directed. In order to find the conditions under which it would also satisfy (2.6.7), the differences we're interested in are

$$\begin{aligned}&x-1,\\ &x^2-x = x(x-1),\\ &-1-x^2 = -(x^2+1),\\ &-x+1 = -(x-1),\\ &-x^2+x = -(x^2-x) = -x(x-1),\\ &x^2+1.\end{aligned}$$

It can be seen that these are the same as the differences involving opponents of the first kind (as seen above). In order to find the conditions under which this construction would also satisfy (2.6.8), the differences we're interested in are

$$x^2-1 = (x-1)(x+1),$$

$$-(x+1),$$
$$-(x^2+x) = -x(x+1),$$
$$-x^2+1 = -(x^2-1) = -(x-1)(x+1),$$
$$x+1,$$
$$x+x^2 = x(x+1).$$

So here we have $\pm(x+1)$, $\pm x(x+1)$, $\pm(x^2-1)$, and it can be seen that we require $(x-1)/x^2$ to be a cube, i.e. we require $x(x-1)$ to be a cube.

This means that if the conditions are satisfied such that Construction 10 gives us the initial round tables of a $\mathbb{Z}$-cyclic moore $(2,6)$ $GWhD(6m+1)$, the resulting design is also directed.

Thus the following theorem is established.

Theorem 2.7.1 *Let $p = 12t+7$ be prime. If there exists an element x of $\mathbb{Z}_p$ such that x is not a cube, $x(x+1)$ is a cube, $x(x-1)$ is a cube and $x^2(x^2+1)$ is a cube, then a directed moore $(2,6)$ $GWhD(p)$ exists.*

It therefore remains to show that a value of x which satisfies the conditions of Theorem 2.7.1 can be obtained.

Let χ be the character of order 3 exactly which is defined by

$$\chi(y) = \begin{cases} \omega^j & \text{if } y \in C_j^3; \\ 0 & \text{if } y = 0, \end{cases}$$

where $\omega = e^{\frac{2\pi i}{3}}$.

If we now let $\psi(y) = 1 + \chi(y) + \chi(y^2)$ and $\delta(y) = 2 - \chi(y) - \chi(y^2)$, then it follows that

$$\psi(y) = \begin{cases} 3 & \text{if } y \in C_0^3; \\ 1 & \text{if } y = 0; \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\delta(y) = \begin{cases} 0 & \text{if } y \in C_0^3; \\ 2 & \text{if } y = 0; \\ 3 & \text{otherwise.} \end{cases}$$

Consider the sum,

$$S = \sum_{x \in \mathbb{Z}_p} \delta(x) \times \psi(x(x-1)) \times \psi(x(x+1)) \times \psi(x^2(x^2+1)),$$

i.e.

$$S = \sum_{x \in \mathbb{Z}_p} (2 - \chi(x) - \chi(x^2))(1 + \chi(x(x-1)) + \chi(x^2(x-1)^2))(1 + \chi(x(x+1)) + \chi(x^2(x+1)^2))(1 + \chi(x^2(x^2+1)) + \chi(x^4(x^2+1)^2)),$$

i.e.

$$S = \sum_{x \in \mathbb{Z}_p} (2 - 2\chi(x) + 4\chi(x(x-1)) - 4\chi(x^2(x-1)))(1 + \chi(x(x+1)) + \chi(x^2(x+1)^2) + \chi(x^2(x^2+1)) + \chi(x^3(x+1)(x^2+1)) + \chi(x^4(x+1)^2(x^2+1)) + \chi(x^4(x^2+1)^2) + \chi(x^5(x+1)(x^2+1)^2) + \chi(x^6(x+1)^2(x^2+1)^2).$$

After multiplying this out and making the appropriate substitutions (using Theorem 1.4.1), it can be seen that,

$$S \geq 2p - 288\sqrt{p}.$$

It is also clearly the case that,

$$S = 81|A| + 2,$$

where elements in A are of the form given in Theorem 2.7.1. In the case where $x = 0$, there is a contribution of 2 to the value of S. When $x = 1$, $x = -1$ (i.e. $x^2 = 1$) or $x^2 = -1$ (i.e. $x^4 = 1$), there is no contribution to S. We can see this if we again let $x = \theta^\alpha$. So $\theta^\alpha = 1$ or $\theta^{2\alpha} = 1$ or $\theta^{4\alpha} = 1$. Since $\theta^{12t+6} = 1$, this means that $6|\alpha$ or $6|2\alpha$ or $6|4\alpha$. Thus, $\alpha \in C_0^3$ and so $\delta(x) = 0$, which means that the contribution to S in each case is 0.

So,

$$S = 81|A| + 2 \geq 2p - 288\sqrt{p} > 2,$$
$$\text{i.e. } p > 20,738.$$

It was then checked by computer that appropriate values of x existed for all primes $p < 20,738$ where $p \equiv 7 \pmod{12}$, excluding $p = 7$, 19, 31, 43, 79, 127, 139, 199, 271, 283, 463. Here, we list (p, x_p) where p is the prime and x_p is a suitable value of x for that prime for all relevant primes $p < 5,000$.

(67, 29), (103, 46), (151, 22), (163, 50), (211, 32), (223, 19), (307, 14), (331, 42), (367, 33), (379, 19), (439, 39), (487, 69), (499, 45), (523, 132), (547, 12), (571, 33), (607, 13), (619, 67), (631, 16), (643, 115), (691, 58), (727, 51), (739, 44), (751, 12), (787, 11), (811, 23), (823, 53), (859, 51), (883, 15), (907, 37), (919, 44), (967, 47), (991, 11), (1039, 85), (1051, 22), (1063, 30), (1087, 230), (1123, 53), (1171, 74), (1231, 29), (1279, 4), (1291, 11), (1303, 13), (1327, 23), (1399, 111), (1423, 76), (1447, 112), (1459, 166), (1471, 82), (1483, 145), (1531, 30), (1543, 45), (1567, 5), (1579, 47), (1627, 35), (1663, 14), (1699, 36), (1723, 77), (1747, 24), (1759, 140), (1783, 17), (1831, 22), (1867, 30), (1879, 19), (1951, 37), (1987, 93), (1999, 60), (2011, 70), (2083, 54), (2131, 45), (2143, 118), (2179, 38), (2203, 70), (2239, 67), (2251, 40), (2287, 220), (2311, 87), (2347, 10), (2371, 85), (2383, 119), (2467, 47), (2503, 49), (2539, 59), (2551, 34), (2647, 24), (2659, 21), (2671, 75), (2683, 22), (2707, 43), (2719, 60), (2731, 20), (2767, 83), (2791, 14), (2803, 67), (2851, 47), (2887, 5), (2971, 79), (3019, 33), (3067, 11), (3079, 13), (3163, 25), (3187, 14), (3259, 91), (3271, 97), (3307, 5), (3319, 15), (3331, 35), (3343, 20), (3391, 6), (3463, 41), (3499, 22), (3511, 83), (3547, 67), (3559, 74), (3571, 95), (3583, 32), (3607, 176), (3631, 70), (3643, 55), (3691, 59), (3727, 56), (3739, 17), (3823, 118), (3847, 17), (3907, 11), (3919, 25), (3931, 12), (3943, 49), (3967, 17), (4003, 61), (4027, 21), (4051, 37), (4099, 74), (4111, 22), (4159, 200), (4219, 16), (4231, 29), (4243, 116), (4327, 57), (4339, 14), (4363, 143), (4423, 97), (4447, 30), (4483, 66), (4507, 194), (4519, 76), (4567, 45), (4591, 21), (4603, 12), (4639, 109), (4651, 58), (4663, 47), (4723, 14), (4759, 123), (4783, 141), (4831, 14), (4903, 18), (4951, 22), (4987, 71), (4999, 12).

A computer programme was then constructed using the Magma computational algebra package, and the following examples were found for 8 of the 11 remaining values of p.

Example 2.7.1 A $\mathbb{Z}$-cyclic directed moore $GWhD(43)$ is given by the initial round $(1, 39; 19, 6; 36, 28) \times 1, 3^6, \ldots, 3^{36}$.

Example 2.7.2 A $\mathbb{Z}$-cyclic directed moore $GWhD(79)$ is given by the initial round $(1, 15; 29, 23; 55, 35) \times 1, 29^6, \ldots, 29^{72}$.

Example 2.7.3 A $\mathbb{Z}$-cyclic directed moore $GWhD(127)$ is given by the initial round $(1, 63; 56, 115; 17, 90) \times 1, 56^6, \ldots, 56^{120}$.

Example 2.7.4 A $\mathbb{Z}$-cyclic directed moore $GWhD(139)$ is given by the initial round $(1, 95; 110, 67; 4, 102) \times 1, 2^6, \ldots, 2^{132}$.

Example 2.7.5 A $\mathbb{Z}$-cyclic directed moore $GWhD(199)$ is given by the initial round $(1,147;71,180;70,113) \times 1,22^6,\ldots,22^{192}$.

Example 2.7.6 A $\mathbb{Z}$-cyclic directed moore $GWhD(271)$ is given by the initial round $(1,30;26,20;77,226) \times 1,26^6,\ldots,26^{264}$.

Example 2.7.7 A $\mathbb{Z}$-cyclic directed moore $GWhD(283)$ is given by the initial round $(1,156;20,11;121,220) \times 1,46^6,\ldots,46^{276}$.

Example 2.7.8 A $\mathbb{Z}$-cyclic directed moore $GWhD(463)$ is given by the initial round $(1,366;245,371;316,369) \times 1,245^6,\ldots,245^{456}$.

It was also verified by computer that there is not a $\mathbb{Z}$-cyclic moore $GWhD(7)$, and so it follows that there also isn't a design of this type which is also directed.

Thus the following theorem is established.

Theorem 2.7.2 *A $\mathbb{Z}$-cyclic directed moore* $(2,6)$ $GWhD(p)$ *exists for all primes* $p \equiv 7 \pmod{12}$, $p \geq 43$.

Definition 2.7.1 A (cyclic) *difference matrix*, $(v,k,1)$-DM, is a $k \times v$ matrix $A = [a_{ij}]$, a_{ij} in $\mathbb{Z}_v$, such that for $r \neq s$ the differences $a_{rj} - a_{sj}$, $1 \leq j \leq v$, comprise all the elements of $\mathbb{Z}_v$. If, in addition, the elements of each row comprise all the elements of $\mathbb{Z}_v$, we speak of a *homogeneous* $(v,k,1)$-DM.

It is shown in [2] that the existence of a homogeneous $(p,6,1)$ difference matrix follows from the existence of a $\mathbb{Z}$-cyclic directed $(2,6)$ $GWhD(p)$.

The following product theorem is also given in [2], and can be used to prove the existence of a great many further generalised whist designs which are $\mathbb{Z}$-cyclic, directed and moore.

Theorem 2.7.3 *If n_1 and n_2 are positive integers of the form $6m+1$ such that there exist $\mathbb{Z}$-cyclic directed (alt. moore)* $(2,6)$ $GWhD(n_i)$, $i = 1,2$ *and if there exists a homogeneous* $(n_1,6,1)$ *difference matrix then there exists a $\mathbb{Z}$-cyclic directed (alt. moore)* $(2,6)$ $GWhD(n_1 n_2)$.

Clearly it follows that our $\mathbb{Z}$-cyclic directed moore $(2,6)$ $GWhD(p)$ can be combined in this way to generate others.

Corollary 2.7.4

There exists a $\mathbb{Z}$-cyclic directed moore $(2,6)$ $GWhD(p_1^{\alpha_1}p_2^{\alpha_2}\ldots)$ *for all* $\alpha_i \geq 1$ *and* $p_i \equiv 7 \pmod{12}$, $p_i \geq 43$.

Chapter 3

The Three Person Property

3.1 Introduction

Let us recall Definition 1.6.1 which states that a whist tournament is said to have the three person property if the intersection of any two games (tables) in the tournament is at most two. This property has been studied with respect to ordinary whist tournaments in [23] and [29]. In [29], it was shown that necessary conditions for the existence of tournaments which satisfy the three person property are also sufficient whenever $v > 472$, while [23] proved the following:

Theorem 3.1.1 *The necessary conditions for the existence of a $Wh(v)$ which satisfies the three person property, namely, $v \equiv 0, 1 \pmod 4$ and $v \geq 8$, are also sufficient with one definite exception for $v = 12$.*

The following definition is essential to proving the existence of tournaments which satisfy the three person property.

Definition 3.1.1 Let (a, b, c, d) be a table in the initial round of a $Wh(v)$. The *a-centred difference sets* corresponding to that table are the three sets $\{b - a, c - a\}$, $\{b - a, d - a\}$, $\{c - a, d - a\}$.

Similarly we define b-centred, c-centred and d-centred difference sets. Armed with these definitions, the following result which appears in [20] is the basis for the method of proof used throughout this chapter.

Theorem 3.1.2 *A $\mathbb{Z}$-cyclic $Wh(v)$ has the three person property if and only if the centred difference sets formed from the tables of the initial round are all different.*

If we now look at the 36 centred difference sets which correspond to Example 1.6.1, it can be seen that they are all different.

3.2 The Three Person Property for $OTWh(p)$ where $p \equiv 5 \pmod 8$

We are now going to look at this property with respect to our $\mathbb{Z}$-cyclic OTWh(p) where $p \equiv 5 \pmod 8$. In order to show that there is a $\mathbb{Z}$-cyclic ordered triplewhist tournament which satisfies the three person property for all primes $p \equiv 5 \pmod 8$, $p \geq 29$, we will let $p = 8t + 5$ and look more closely at Construction 1 from Section 2.3.

Construction 1 $\quad (\theta^{4i}, x\theta^{4i}, -\theta^{4i}, x^3\theta^{4i}), \qquad 0 \leq i \leq 2m,$

where $x^2 - 1$ is not a square, $x^2 \pm x + 1$ are squares and $x^2 \pm x + 1$ are both not fourth powers.

$$\theta^{4i} \text{ centred differences} = \begin{cases} (\theta^{4i}(x-1), \theta^{4i}(-2)), & (3.2.1) \\ (\theta^{4i}(x-1), \theta^{4i}(x^3-1)), & (3.2.2) \\ (\theta^{4i}(-2), \theta^{4i}(x^3-1)). & (3.2.3) \end{cases}$$

$$\theta^{4i+1} \text{ centred differences} = \begin{cases} (\theta^{4i}(1-x), \theta^{4i}(-1-x)), & (3.2.4) \\ (\theta^{4i}(1-x), \theta^{4i}(x^3-x)), & (3.2.5) \\ (\theta^{4i}(-1-x), \theta^{4i}(x^3-x)). & (3.2.6) \end{cases}$$

$$-\theta^{4i} \text{ centred differences} = \begin{cases} (\theta^{4i}(2), \theta^{4i}(x+1)), & (3.2.7) \\ (\theta^{4i}(2), \theta^{4i}(x^3+1)), & (3.2.8) \\ (\theta^{4i}(x+1), \theta^{4i}(x^3+1)). & (3.2.9) \end{cases}$$

$$\theta^{4i+3} \text{ centred differences} = \begin{cases} (\theta^{4i}(1-x^3), \theta^{4i}(x-x^3)), & (3.2.10) \\ (\theta^{4i}(1-x^3), \theta^{4i}(-1-x^3)), & (3.2.11) \\ (\theta^{4i}(x-x^3), \theta^{4i}(-1-x^3)). & (3.2.12) \end{cases}$$

We want to show that each of these (unordered) pairs are distinct. In order to do so, we will go through the sets one by one and suppose that each of them in turn is equal to one of the other sets. We will then hopefully find a contradiction which shows that they cannot be equal. We shall not give full details of every case, but sufficient examples to illustrate the different arguments required.

(3.2.1) and **(3.2.1)**: Suppose that

$$\theta^{4i}(x-1) = \theta^{4j}(x-1)$$
$$\text{and } \theta^{4i}(-2) = \theta^{4j}(-2).$$

For both of these to hold, we would require $i = j$. The definition of an initial round means that this is not possible and so we have a contradiction. The other possibility would be to suppose that

$$\theta^{4i}(x-1) = \theta^{4j}(-2)$$
$$\text{and } \theta^{4i}(-2) = \theta^{4j}(x-1).$$
$$\text{But then } (x-1)^2 = 4,$$
$$\text{i.e. } x-1 = \pm 2.$$

Neither of these two possible solutions can hold. For example, if $x = 3$ then we would have $\theta^{4i} = -\theta^{4j}$, so $\theta^{4(i-j)} = -1$ and thus $4(i-j) = 4t+2$. This is impossible.

(3.2.1) and **(3.2.2)**: Suppose that

$$\theta^{4i}(x-1) = \theta^{4j}(x-1)$$
$$\text{and } \theta^{4i}(-2) = \theta^{4j}(x^3-1).$$

The first of these equations is satisfied when $i = j$. As seen previously, this is a contradiction due to the definition of an initial round. The other possibility would be to suppose that

$$\theta^{4i}(x-1) = \theta^{4j}(x^3-1) = \theta^{4j}(x^2+x+1)(x-1)$$
$$\text{and } \theta^{4i}(-2) = \theta^{4j}(x-1).$$
$$\text{Then } \theta^{4i-4j} = x^2+x+1.$$

Since x^2+x+1 is not a fourth power, we again have a contradiction.

(3.2.1) and **(3.2.4)**: Suppose that

$$\theta^{4i}(x-1) = -\theta^{4j}(x+1)$$
$$\text{and } \theta^{4i}(-2) = -\theta^{4j}(x-1).$$

Since we know that $x^2 - 1$ is not a square, it can be seen that there is a contradiction straight away in the first of these two equations. The other possibility would be to suppose that

$$\theta^{4i}(x-1) = -\theta^{4j}(x-1)$$
$$\text{and } \theta^{4i}(2) = \theta^{4j}(x+1).$$

The first of these gives

$$\theta^{4i} = -\theta^{4j} = \theta^{4j+4t+2},$$

which is a contradiction, since the right hand side is not a fourth power.

(3.2.1) and **(3.2.11)**: Suppose that

$$\theta^{4i}(x-1) = \theta^{4j}(-1-x^3) = -\theta^{4j}(x^2-x+1)(x+1)$$
$$\text{and } \theta^{4i}(2) = \theta^{4j}(x^3-1).$$

It can be seen that there is a contradiction in the first of these equations since $x^2 - 1$ is not a square while $x^2 - x + 1$ is. The other possibility would be to suppose that

$$\theta^{4i}(x-1) = \theta^{4j}(1-x^3)$$
$$\text{and } \theta^{4i}(2) = \theta^{4j}(x^3+1).$$

By adding the respective sides of these equations, we see that

$$\theta^{4i}(x+1) = \theta^{4j}(2),$$
$$\text{i.e. } \tfrac{x+1}{2} \text{ is a fourth power.}$$

The second of the two equations tells us that $\frac{x^3+1}{2}$ is a fourth power. By dividing, it can now be seen that $x^2 - x + 1$ must be a fourth power. This contradicts what we already know about $x^2 - x + 1$ which is that it is a square but not a fourth power.

In the examples above, we have checked both possibilities in each case and found a contradiction each time (there are two possibilities since the pairs are unordered). In the examples which follow, we will simply look at the more interesting possibilities.

(3.2.3) and **(3.2.6)**: Suppose that

$$\theta^{4i}(2) = \theta^{4j}(x+1)$$
$$\text{and } \theta^{4i}(x^2+x+1) = \theta^{4j}x(x+1).$$

The first of the two equations here tells us that $(x+1)$ is not a square. If we then cross multiply the two equations, we see that

$$2x = x^2 + x + 1,$$
$$\text{i.e. } x^2 - x + 1 = 0,$$
$$\text{i.e. } x(x-1) = -1.$$

Since $(x+1)$ is not a square, we know that $(x-1)$ is. Thus, -1 is not a square. As a result, we have a contradiction here.

(3.2.3) and **(3.2.12)**: Suppose that

$$\theta^{4i}(2) = \theta^{4j}(x^3+1)$$
$$\text{and } \theta^{4i}(x^3-1) = -\theta^{4j}(x^3-x).$$

By adding the respective sides of these equations, we see that

$$\theta^{4i}(x^3+1) = \theta^{4j}(x+1),$$
$$\text{i.e. } \theta^{4i}(x^2-x+1) = \theta^{4j},$$
$$\text{i.e. } x^2-x+1 \text{ is a fourth power.}$$

This is a contradiction since we know that x^2-x+1 is a square but not a fourth power.

(3.2.4) and **(3.2.8)**: Suppose that

$$-\theta^{4i}(x-1) = \theta^{4j}(2)$$
$$\text{and } -\theta^{4i} = \theta^{4j}(x^2-x+1).$$

If we now cross multiply, it can be seen that

$$2 = (x-1)(x^2-x+1) = x^3 - 2x^2 + 2x - 1,$$
$$\text{i.e. } x^3 - 1 = 2(x^2-x+1),$$
$$\text{i.e. } (x^2+x+1)(x-1) = (x-1)(x^2-x+1)^2,$$
$$\text{i.e. } x^2+x+1 = (x^2-x+1)^2.$$

This is a contradiction since $(x^2-x+1)^2$ is a fourth power, while we know that x^2+x+1 isn't.

(3.2.7) and **(3.2.8)**: Suppose that

$$\theta^{4i}(2) = \theta^{4j}(x^2 - x + 1)(x + 1)$$
$$\text{and } \theta^{4i}(x + 1) = \theta^{4j}(2),$$

so that $x + 1$ is not a square. If we cross multiply, we see that

$$(x^2 - x + 1)(x + 1)^2 = 2^2.$$

The left hand side here is a fourth power while the right hand side is a square but not a fourth power. As a result, we have a contradiction.

We have now seen a number of examples whereby a contradiction was found when sets of differences were assumed to be equal. This was done for all possible combinations of sets (remembering that for each combination, there are two possibilities which must be checked), and a contradiction was found in all but six cases. We will now look at these six special cases more closely, showing that they can arise for only four possible values of x.

(3.2.2) and **(3.2.5)**: Suppose that

$$\theta^{4i} = \theta^{4j} x(x + 1)$$
$$\text{and } \theta^{4i}(x^2 + x + 1) = -\theta^{4j},$$
$$\text{so that } -1 = x(x + 1)(x^2 + x + 1).$$

If we now let $y = x(x + 1)$ we have

$$-1 = y(y + 1),$$
$$\text{i.e. } y^2 + y + 1 = 0.$$

(3.2.2) and **(3.2.10)**: Suppose that

$$\theta^{4i} = -\theta^{4j}(x^2 + x + 1)$$
$$\text{and } \theta^{4i}(x^2 + x + 1) = -\theta^{4j} x(x + 1).$$
$$\text{Then } x(x + 1) = (x^2 + x + 1)^2,$$

If we now let $y = x(x + 1)$ we again have

$$y^2 + y + 1 = 0.$$

(3.2.5) and **(3.2.10)**: Suppose that

$$\theta^{4i} = \theta^{4j} x(x + 1)$$
$$\text{and } \theta^{4i} x(x + 1) = -\theta^{4j}(x^2 + x + 1),$$
$$\text{so that } -(x^2 + x + 1) = x^2(x + 1)^2,$$

If we now let $y = x(x+1)$ we again have

$$y^2 + y + 1 = 0.$$

(3.2.6) and **(3.2.9)**: Suppose that

$$-\theta^{4i} = \theta^{4j}(x^2 - x + 1)$$
$$\text{and } \theta^{4i}x(x-1) = \theta^{4j},$$
$$\text{so that } -1 = x(x-1)(x^2 - x + 1),$$

Now, if we let $y = x(x-1)$ we have

$$-1 = y(y+1),$$
$$\text{i.e. } y^2 + y + 1 = 0.$$

(3.2.6) and **(3.2.12)**: Suppose that

$$\theta^{4i} = \theta^{4j}x(x-1)$$
$$\text{and } \theta^{4i}x(x-1) = -\theta^{4j}(x^2 - x + 1).$$
$$\text{So } -(x^2 - x + 1) = x^2(x-1)^2.$$

If we let $y = x(x-1)$ we have

$$-(y+1) = y^2,$$
$$\text{i.e. } y^2 + y + 1 = 0.$$

(3.2.9) and **(3.2.12)**: Suppose that

$$\theta^{4i} = -\theta^{4j}(x^2 - x + 1)$$
$$\text{and } \theta^{4i}(x^2 - x + 1) = -\theta^{4j}x(x-1).$$
$$\text{So } x(x-1) = (x^2 - x + 1)^2.$$

If we let $y = x(x-1)$ we have

$$y = y^2 + 2y + 1,$$
$$\text{i.e. } y^2 + y + 1 = 0.$$

There are two possible solutions to the equation $y^2+y+1 = 0$. For each y, $y = x(x+1)$ or $y = x(x-1)$. So there are four possible values of x corresponding to each y. This means that we have eight possible values of x which would satisfy $y^2 + y + 1 = 0$. So if $|A| > 8$, then there must be a solution of the kind we want. Let λ and ψ be defined as in Section 2.3, and let

$$S = \sum_{x \in \mathrm{GF}(p)} (1-\lambda(x))(1-\lambda(x^2-1))(\lambda(x^2-x+1)+1) \times \\ (\lambda(x^2+x+1)+1)(1-\psi(x^2+x+1))(1-\psi(x^2-x+1)).$$

Then $S = 64|A|$ where A is the set of non-square elements, x of $\mathbb{Z}_p$, satisfying the required conditions for Construction 1 to give an $OTWh(p)$. We want to show that $|A| > 8$, thus ensuring that at least one of the values of x will give an $OTWh(p)$ which satisfies the three person property.

Since $\lambda(x) = \psi(x^2)$,

$$S = \sum_{x \in \mathrm{GF}(p)} (1-\psi(x^2))(1-\psi(x^2-1)^2)(\psi((x^2-x+1)^2)+1) \times \\ (\psi((x^2+x+1)^2)+1)(1-\psi(x^2-x+1))(1-\psi(x^2+x+1)),$$

i.e.

$$S = \sum_{x \in \mathrm{GF}(p)} (\psi((x^2-x+1)^2) - \psi(x^2(x^2-x+1)^2) - \psi((x^2-1)^2(x^2-x+1)^2) + \\ \psi(x^2(x^2-1)^2(x^2-x+1)^2) + 1 - \psi(x^2) - \psi((x^2-1)^2) + \psi(x^2(x^2-1)^2)) \times \\ (\psi((x^2+x+1)^2)+1)(1-\psi(x^2-x+1))(1-\psi(x^2+x+1)).$$

After multiplying this out fully and making the appropriate substitutions (using Theorem 1.4.1), it can be seen that

$$S \geq p - 227\sqrt{p}.$$

So $|A| > 8$ provided,

$$p - 227\sqrt{p} > 64 \times 8,$$
$$\text{i.e. } \sqrt{p}(\sqrt{p} - 227) > 512,$$
$$\text{i.e. } p > 52,549.$$

It was then checked by computer that appropriate values of x existed for all primes $29 \leq p < 52,549$ where $p \equiv 5 \pmod 8$, excluding $p = 29, 37, 53, 101, 157$. Here, we list (p, x_p) where p is the prime and x_p is the smallest suitable value of x for that prime for all relevant primes $p < 3,000$ excluding the five values already mentioned.

$$(61,23),\ (109,14),\ (149,72),\ (173,44),\ (181,41),\ (197,30),\ (229,21),\ (269,29),\ (277,37),$$
$$(293,110),\ (317,140),\ (349,8),\ (373,18),\ (389,14),\ (397,180),\ (421,126),\ (461,10),$$
$$(509,147),\ (541,67),\ (557,11),\ (613,60),\ (653,102),\ (661,6),\ (677,12),\ (701,93),$$
$$(709,22),\ (733,8),\ (757,31),\ (773,41),\ (797,114),\ (821,90),\ (829,54),\ (853,245),$$
$$(877,20),\ (941,155),\ (997,297),\ (1013,41),\ (1021,209),\ (1061,15),\ (1069,321),$$
$$(1093,105),\ (1109,132),\ (1117,205),\ (1181,191),\ (1213,88),\ (1229,19),\ (1237,349),$$
$$(1277,28),\ (1301,203),\ (1373,12),\ (1381,138),\ (1429,139),\ (1453,56),\ (1493,44),$$
$$(1549,157),\ (1597,5),\ (1613,79),\ (1621,90),\ (1637,41),\ (1669,10),\ (1693,23),\ (1709,40),$$
$$(1733,34),\ (1741,73),\ (1789,93),\ (1861,39),\ (1877,80),\ (1901,101),\ (1933,14),\ (1949,48),$$
$$(1973,111),\ (1997,47),\ (2029,177),\ (2053,15),\ (2069,17),\ (2141,8),\ (2213,68),\ (2221,38),$$
$$(2237,115),\ (2269,13),\ (2293,240),\ (2309,8),\ (2333,50),\ (2341,74),\ (2357,32),\ (2381,48),$$
$$(2389,23),\ (2437,42),\ (2477,48),\ (2549,160),\ (2557,15),\ (2621,7),\ (2677,80),\ (2693,27),$$
$$(2741,253),\ (2749,17),\ (2789,13),\ (2797,83),\ (2837,27),\ (2861,26),\ (2909,75),\ (2917,92),$$
$$(2957,72).$$

In the case of the five problem values remaining, it was found that the $\mathbb{Z}$-cyclic ordered triplewhist tournaments given in Chapter 2 also satisfy the three person property.

Thus the following theorem is established.

Theorem 3.2.1 *A $\mathbb{Z}$-cyclic* OTWh(p) *which satisfies the three person property exists for all primes* $p \equiv 5 \pmod 8$, $p \geq 29$.

Note The extra condition which ensures that a $\mathbb{Z}$-cyclic ordered triplewhist tournament will also satisfy the three person property, i.e. $y^2 + y + 1 \neq 0$, is easily shown to be necessary in this case since there are values for x which satisfy all of the $\mathbb{Z}$-cyclic ordered triplewhist conditions for Construction 1, and where $y^2 + y + 1 = 0$.

Example 3.2.1 For $p = 181$, $x = 57$ satisfies all of the $\mathbb{Z}$-cyclic ordered triplewhist conditions for Construction 1, and in addition, $x^3(x+1)^3 = 1$. Similarly, $x = 58$ satisfies all of the $\mathbb{Z}$-cyclic ordered triplewhist conditions for Construction 1, and in addition $x^3(x-1)^3 = 1$.

3.3 The Three Person Property for $OTWh(p)$ and $DTWh(p)$ where $p \equiv 9 \pmod{16}$

We are now going to investigate the three person property with respect to our $\mathbb{Z}$-Cyclic OTWh(p) and DTWh(p), where $p \equiv 9 \pmod{16}$. In order to show that there are such tournaments which satisfy the three person property for all primes $p \equiv 9 \pmod{16}$, we will let $p = 16t + 9$ and look more closely at Construction 7 from Section 2.5.

Construction 7 $(\theta^{8i+2j}, x\theta^{8i+2j}, x^4\theta^{8i+2j}, -x\theta^{8i+2j})$, $\quad 0 \le i \le 2t,$
$\quad 0 \le j \le 1.$

$$\theta^{8i+2j} \text{ centred differences} = \begin{cases} (\theta^{8i+2j}(x-1), \theta^{8i+2j}(x^4-1)), & (3.3.1) \\ (\theta^{8i+2j}(x-1), \theta^{8i+2j}(-x-1)), & (3.3.2) \\ (\theta^{8i+2j}(x^4-1), \theta^{8i+2j}(-x-1)). & (3.3.3) \end{cases}$$

$$x\theta^{8i+2j} \text{ centred differences} = \begin{cases} (\theta^{8i+2j}(1-x), \theta^{8i+2j}(x^4-x)), & (3.3.4) \\ (\theta^{8i+2j}(1-x), \theta^{8i+2j}(-2x)), & (3.3.5) \\ (\theta^{8i+2j}(x^4-x), \theta^{8i+2j}(-2x)). & (3.3.6) \end{cases}$$

$$x^4\theta^{8i+2j} \text{ centred differences} = \begin{cases} (\theta^{8i+2j}(1-x^4), \theta^{8i+2j}(x-x^4)), & (3.3.7) \\ (\theta^{8i+2j}(1-x^4), \theta^{8i+2j}(-x-x^4)), & (3.3.8) \\ (\theta^{8i+2j}(x-x^4), \theta^{8i+2j}(-x-x^4)). & (3.3.9) \end{cases}$$

$$-x\theta^{8i+2j} \text{ centred differences} = \begin{cases} (\theta^{8i+2j}(x+1), \theta^{8i+2j}(2x)), & (3.3.10) \\ (\theta^{8i+2j}(x+1), \theta^{8i+2j}(x^4+x)), & (3.3.11) \\ (\theta^{8i+2j}(2x), \theta^{8i+2j}(x^4+x)). & (3.3.12) \end{cases}$$

Again we want to show that all of these (unordered) pairs are distinct. As in the previous section, we will go through the sets one by one and suppose that each of them in turn is equal to one of the other sets. Then, we will hope to find contradictions which show that the sets cannot be equal (with there again being two possibilities which must be checked for each pair of sets). As before, we will give some typical cases.

(3.3.1) and **(3.3.6)**: Suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(x^4 - x)$$
$$\text{and } \theta^{8i+2j}(x^4-1) = \theta^{8m+2n}(-2x).$$

The second of these equations tells us that x must be a square, but x is not a square and so we have a contradiction. The other possibility is to suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(-2x)$$
$$\text{and } \theta^{8i+2j}(x^4-1) = \theta^{8m+2n}(x^4 - x).$$

The first of these equations tells us that $x-1$ is not a square, while the second tells us that

$$x^4 - x \text{ is a square,}$$
$$\text{i.e. } x(x-1)(x^2+x+1) \text{ is a square,}$$
$$\text{i.e.} (x^2+x+1) \text{ is a square.}$$

This contradicts what we already know about x^2+x+1.

(3.3.1) and **(3.3.12)**: Suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(2x)$$
$$\text{and } \theta^{8i+2j}(x^4-1) = \theta^{8m+2n}(x^4 + x).$$

If we cross multiply, we see that

$$2x(x^4-1) = x(x-1)(x+1)(x^2-x+1),$$
$$\text{i.e. } 2(x^2+1) = x^2 - x + 1,$$
$$\text{i.e. } x^2 + x = -1,$$
$$\text{i.e. } x^2 = -x - 1,$$
$$\text{i.e. } x^3 = -(x^2+x) = -1.$$

Since -1 is a square, this gives us a contradiction. The other possibility is to suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(x^4 + x)$$
$$\text{and } \theta^{8i+2j}(x^4-1) = \theta^{8m+2n}(2x).$$

The second of these tells us that x must be a square which is a contradiction.

(3.3.2) and **(3.3.4)**: Suppose that

$$\theta^{8i+2j}(x-1) = -\theta^{8m+2n}(x-1)$$
$$\text{and } -\theta^{8i+2j}(x+1) = \theta^{8m+2n}(x^4-x).$$

If the common factor of $x-1$ is cancelled from both sides in the first of these, we end up with

$$\theta^{8i+2j} = -\theta^{8m+2n} = \theta^{8m+2n+8t+4}.$$

Thus $8i+2j$ and $8m+2n+8t+4$ must differ by a multiple of $p-1$ since the order of θ is $p-1$. But $p-1 = 16t+8$ is a multiple of 8. So $2j \equiv 2n+4 \pmod 8$. If we recall that $j=0$ or 1 and $n=0$ or 1, then it can be seen that we have a contradiction. The other possibility is to suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(x^4-x)$$
$$\text{and } \theta^{8i+2j}(x+1) = \theta^{8m+2n}(x-1).$$

The second of these gives us a contradiction since x^2-1 is not a square.

(3.3.2) and **(3.3.6)**: Suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(x^4-x)$$
$$\text{and } -\theta^{8i+2j}(x+1) = \theta^{8m+2n}(-2x).$$

The second equation tells us that $x+1$ is not a square, which in turn means that $x-1$ is, x^3-1 isn't and x^3+1 is. If we then cross multiply, we see that

$$-2x(x-1) = -x(x+1)(x-1)(x^2+x+1),$$
$$\text{i.e. } 2 = (x+1)(x^2+x+1),$$
$$\text{i.e. } -2x(x+1) = x^3-1.$$

This gives us a contradiction since the left hand side is a square, while the right hand side isn't. The other possibility is to suppose that

$$\theta^{8i+2j}(x-1) = \theta^{8m+2n}(-2x)$$
$$\text{and } -\theta^{8i+2j}(x+1) = \theta^{8m+2n}(x^4-x).$$

The first of these equations tells us that $x-1$ is not a square, which in turn means that $x+1$ is, x^3-1 is and x^3+1 isn't. This gives us a contradiction in the second equation since the left hand side is a square, while the right hand side isn't.

As in the previous section, we will now simply look at the more interesting possibilities instead of looking at both in each case.

(3.3.6) and **(3.3.6)**: Suppose that

$$\theta^{8i+2j}(x^4 - x) = \theta^{8m+2n}(x^4 - x)$$
$$\text{and } \theta^{8i+2j}(-2x) = \theta^{8m+2n}(-2x).$$

This is only possible if $i = m$ and $j = n$. So we have a contradiction due to the definition of the initial round.

(3.3.6) and **(3.3.12)**: Suppose that

$$\theta^{8i+2j}(x^4 - x) = \theta^{8m+2n}(2x)$$
$$\text{and } \theta^{8i+2j}(-2x) = \theta^{8m+2n}(x^4 + x).$$

The first of these equations tells us that $x^3 - 1$ is a square, while the second tells us that $x^3 + 1$ is a square. This is a contradiction since $x^6 - 1$ is not a square.

(3.3.7) and **(3.3.7)**: Suppose that

$$-\theta^{8i+2j}(x^4 - 1) = -\theta^{8m+2n}(x^4 - x)$$
$$\text{and } -\theta^{8i+2j}(x^4 - x) = -\theta^{8m+2n}(x^4 - 1).$$

If we cross multiply and then take the square root, we see that

$$x^4 - 1 = \pm(x^4 - x).$$

Now we need to consider both of these possibilities. Firstly

$$x^4 - 1 = x^4 - x,$$
$$\text{i.e. } x = 1.$$

This is a contradiction since x is not a square while 1 is. Alternatively

$$x^4 - 1 = x - x^4.$$

If we substitute this back into either of our original equations, we end up with

$$\theta^{8i+2j} = -\theta^{8m+2n}.$$

As we have seen previously, this is a contradiction.

(3.3.7) and **(3.3.10)**: Suppose that

$$-\theta^{8i+2j}(x^4-1) = \theta^{8m+2n}(x+1)$$
$$\text{and } -\theta^{8i+2j}(x^4-x) = -\theta^{8m+2n}(2x).$$

If we cross multiply, it can be seen that

$$2(x^2+1) = x^2+x+1,$$
$$\text{i.e. } x^2-x+1=0.$$

From here it can be seen that $x^2 - x = -1$. Multiplying throughout by x also shows us that $x^3 = x^2 - x = -1$. Here we have a contradiction since x^3 is not a square, while -1 is.

As was the case previously, all pairs of sets were looked at (with there being two possibilities in each case) and there are again some examples where a contradiction cannot be found. These reduce down to the 11 equations below. If any of them hold for a particular tournament, then the three person property does not.

If we suppose that **(3.3.1)** and **(3.3.4)** are equal, **(3.3.1)** and **(3.3.7)** are equal, and **(3.3.4)** and **(3.3.7)** are equal, then one of the two possibilities in each case will not lead to an obvious contradiction. The pairs are then seen to be equal if

$$x^6+2x^5+3x^4+3x^3+2x^2+x+1=0.$$

If we suppose that **(3.3.1)** and **(3.3.9)** are equal, and **(3.3.7)** and **(3.3.12)** are equal, then one of the options is only possible if

$$x^5+x^3-2x^2+x-2=0.$$

If we suppose that **(3.3.1)** and **(3.3.10)** are equal, **(3.3.2)** and **(3.3.7)** are equal, and **(3.3.4)** and **(3.3.5)** are equal, then one of the options is only possible if

$$2x(x^2+1)=1.$$

If we suppose that **(3.3.3)** and **(3.3.5)** are equal, then one of the options is only possible if

$$-2x(x^2+1)=1.$$

If we suppose that **(3.3.3)** and **(3.3.8)** are equal, **(3.3.3)** and **(3.3.11)** are equal, and **(3.3.8)** and **(3.3.11)** are equal, then one of the options is only possible if

$$x^6 - 2x^5 + 3x^4 - 3x^3 + 2x^2 - x + 1 = 0.$$

If we suppose that **(3.3.3)** and **(3.3.9)** are equal, and **(3.3.11)** and **(3.3.12)** are equal, then one of the options is only possible if

$$x^5 + x^3 + 2x^2 + x + 2 = 0.$$

If we suppose that **(3.3.4)** and **(3.3.6)** are equal, then one of the options is only possible if

$$x^6 + x^5 + x^4 - x^3 - x^2 - x + 2 = 0.$$

If we suppose that **(3.3.5)** and **(3.3.6)** are equal, then one of the options is only possible if

$$x^3 - 2x^2 + 2x + 1 = 0.$$

If we suppose that **(3.3.5)** and **(3.3.9)** are equal, and **(3.3.10)** and **(3.3.12)** are equal, then one of the options is only possible if

$$x^3 + 2x^2 + 2x - 1 = 0.$$

If we suppose that **(3.3.10)** and **(3.3.11)** are equal, then one of the options is only possible if

$$2x^4 - 2x^3 + 2x^2 - x - 1 = 0.$$

If we suppose that **(3.3.12)** and **(3.3.12)** are equal, then one of the options is only possible if

$$x^3 + x^2 + x - 1 = 0.$$

So in order to ensure that the three person property holds for the tournaments we are interested in, we want to avoid these 47 values of x. So if $|A| > 47$, then there must be a solution of the kind we want. For the ordered case we let $f(x) = x(x^2 + x + 1)$ and $g(x) = x^5(x^2 - x + 1)$. Thus,

$$S = \sum_{x \in \mathrm{GF}(p)} (1 - \lambda(x))(1 - \lambda(x^2 - 1))(1 - \lambda(x^2 + 1))(1 + \chi(f(x)) + \chi(f^2(x)) + \ldots + \chi(f^7(x)))(1 + \chi(g(x)) + \chi(g^2(x)) + \ldots + \chi(g^7(x))).$$

Then $S = 512|A|$ where A is the set of non-square elements of $\mathbb{Z}_p$ satisfying the required conditions for Construction 7 to give an $OTWh(p)$. We want to show that $|A| > 47$, thus ensuring that at least one of the values of x will give an $OTWh(p)$ which satisfies the three person property.

Since $\lambda(x) = \psi(x^2) = \chi(x^4)$,

$$S = \sum_{x \in \mathrm{GF}(p)} (1-\chi(x^4))(1-\chi(x^2-1)^4)(1-\psi(x^2+1)^4)(1+\chi(f(x))+$$
$$\chi(f^2(x)) + \ldots + \chi(f^7(x)))(1+\chi(g(x))+\chi(g^2(x))+\ldots+\chi(g^7(x))).$$

After multiplying this out and making the appropriate substitutions (using Theorem 1.4.1), it can be seen that,

$$S \geq p - 2813\sqrt{p}.$$

Thus, $|A| > 47$ provided

$$p - 2813\sqrt{p} > 512 \times 47,$$
$$\text{i.e. if } \sqrt{p}(\sqrt{p} - 2813) > 24,064,$$
$$\text{i.e. if } p > 7,961,025.$$

Since the substitutions made using Weil's Theorem involve the number of distinct roots of the relevant polynomial, it turns out that the directed case has the same bound. The calculation is exactly the same as that involving the ordered case, with the exception that $f(x) = x(x^2 - x + 1)$ and $g(x) = x^5(x^2 + x + 1)$.

It was then checked by computer that appropriate values of x exist for all primes $p < 7,961,025$ where $p \equiv 9 \pmod{16}$. A suitable value was found for all but the same 15 values for which a suitable x wasn't found by computer initially in Section 2.5. Here, we list (p, x_o, x_d) where p is the prime, x_o is the smallest suitable value of x for that prime in the ordered case, and x_d is the smallest suitable value of x for that prime in the directed case. We will look at these values for appropriate primes, $p < 3,000$ (excluding those for which a suitable value was not found).

$(409, 88, 79)$, $(457, 137, 10)$, $(601, 182, 142)$, $(761, 142, 209)$, $(857, 268, 291)$, $(937, 433, 132)$, $(953, 374, 344)$, $(1033, 103, 251)$, $(1049, 371, 82)$, $(1129, 119, 370)$, $(1193, 27, 75)$, $(1289, 208, 362)$, $(1321, 365, 76)$, $(1433, 605, 694)$, $(1481, 499, 29)$, $(1609, 739, 479)$,

$(1657, 164, 293)$, $(1721, 297, 12)$, $(1753, 89, 291)$, $(1801, 568, 130)$, $(1913, 171, 179)$,
$(1993, 820, 542)$, $(2089, 358, 194)$, $(2137, 157, 245)$, $(2153, 948, 888)$, $(2281, 505, 402)$,
$(2297, 520, 561)$, $(2377, 822, 454)$, $(2393, 656, 259)$, $(2441, 411, 879)$, $(2473, 812, 1203)$,
$(2521, 371, 34)$, $(2617, 132, 19)$, $(2633, 5, 622)$, $(2713, 331, 163)$, $(2777, 906, 659)$,
$(2857, 566, 106)$, $(2969, 505, 876)$.

In the ordered case, it turns out that the 15 values of x given in Chapter 2 for the primes that we haven't yet dealt with here do, in fact, satisfy the three person property. So that leaves us with the directed case, for which we must still check that appropriate values of x exist in these 15 cases. It turns out that such values do exist, and can be found using constructions given in [13].

The $\mathbb{Z}$-cyclic directed triplewhist tournaments for $p = 41$, 73 and 89 given in [13, p. 109] satisfy the three person property. The same is true for the $\mathbb{Z}$-cyclic directed triplewhist tournaments for the 12 problem values greater than or equal to 233 which are given in [13, p. 113]. So that leaves us with $p = 137$ for which a $\mathbb{Z}$-cyclic directed triplewhist tournament which satisfies the three person property still needs to be found. Using Construction GC1 in [13, p. 111] with $c = 4$, $e = 13$, $f = 13$, $w = 5$, $d = 3$, we get such a tournament which is given by

$$(1, 77, 29, 108) \times 5^{2i+8j},\ 0 \leq i \leq 1,\ 0 \leq j \leq 16.$$

Thus the following theorem is established.

Theorem 3.3.1 *A $\mathbb{Z}$-cyclic* OTWh(p) *and a $\mathbb{Z}$-cyclic* DTWh(p) *which satisfy the three person property exist for all primes $p \equiv 9 \pmod{16}$.*

Chapter 4

Logarithmic Terraces

4.1 Introduction

Let us recall the definitions of a terrace and a logarithmic terrace from Section 1.7. Logarithmic terraces have been looked at by Anderson and Preece in [16]. Other than that, very little work has been done on this particular variety of terrace. In the course of this chapter, we will be looking at these terraces more closely in an effort to highlight some of the interesting properties which they possess. In particular, we will be looking at terraces which are simultaneously logarithmic for two different primitive roots. Later in the chapter, we will also introduce the idea of rejoinable and pseudo-rejoinable terraces which are further variations of logarithmic terraces. To begin with, we will first consider some basic results involving both terraces and logarithmic terraces.

4.2 Some General Results

Theorem 4.2.1 *If we add $2n$ to the odd or to the even elements of a terrace in $\mathbb{Z}_{4n}$, the resulting arrangement is another terrace.*

Proof

$2n$ is always even. So the change made to the odd or even elements will not alter their odd or even status. Adding $2n$ to all odd or even elements of a terrace only impacts the odd differences in the 2-sequencing. Any odd difference x becomes $x+2n$ and so each still occurs twice and the structure of a terrace is maintained.

□

Example 4.2.1 An example of a terrace in $\mathbb{Z}_{12}$ is given by

$$4\ 3\ 9\ 6\ 1\ 2\ 11\ 7\ 5\ 10\ 8\ 12.$$

Adding 6 to all odd elements gives

$$4\ 9\ 3\ 6\ 7\ 2\ 5\ 1\ 11\ 10\ 8\ 12,$$

while adding 6 to all even elements gives

$$10\ 3\ 9\ 12\ 1\ 8\ 11\ 7\ 5\ 4\ 2\ 6.$$

It can be seen that both of these are also terraces.

Theorem 4.2.2 *The difference between the first and last element of any terrace for* $\mathbb{Z}_{p-1}$ *is even when* $p \equiv 1 \pmod 4$*, and odd when* $p \equiv 3 \pmod 4$*.*

Proof

By the definition of a terrace, the 2-sequencing contains exactly one occurence of $x = \frac{p-1}{2}$, and two entries, identical or distinct, from $\{x, -x\}$ when $x \not\equiv -x \pmod{p-1}$.

So when $x \not\equiv -x \pmod{p-1}$, if we have x and $-x$ appearing once each in the 2-sequencing, then they cancel out with respect to the overall difference between the first and last elements. If x or $-x$ appear twice, then they contribute $2x$ or $-2x$ respectively to the difference between the first and last elements.

So it is the value of $\frac{p-1}{2}$ which decides whether this difference is odd or even. When $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ is even. When $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd.

□

Theorem 4.2.3 *For primes* $p \equiv 1 \pmod 4$*, the difference between the first and last element in a logarithmic terrace cannot be* $\frac{p-1}{2}$*.*

Proof

Assume that a y-logarithmic terrace, $\mathbf{a}$, exists where y is a primitive root of p, with $a_{p-1} \equiv a_1 + \frac{p-1}{2} \pmod{p-1}$. Also let (y^{a_i}) be the corresponding exponent terrace.

Then,

$$y^{a_{p-1}} \equiv y^{a_1}.y^{\frac{p-1}{2}} \equiv -y^{a_1} \pmod{p}.$$

Let w be the "reduced" value of y^{a_1} which lies in $[1, p-1]$ when it is evaluated modulo p. Thus,

$$\begin{aligned} y^{a_{p-1}} - y^{a_1} &= (p-w) - w \\ &= p - 2w \\ &\equiv 1 - 2w \pmod{p-1}. \end{aligned}$$

This is an odd number contradicting Theorem 4.2.2.

□

Such terraces do exist when $p \equiv 3 \pmod 4$ however.

Example 4.2.2 A 2-log terrace for $p = 11$ with a difference of $\frac{p-1}{2} = 5$ between the first and last elements is given by

1 2 4 3 8 5 9 7 10 6.

4.3 Some Examples

In this section, we will look at some examples of logarithmic terraces for primes $p \leq 29$.

Example 4.3.1 A 3-logarithmic terrace for $p = 7$ is given by

2 3 6 4 5 1

which has exponent terrace

2 6 1 4 5 3.

Note: There are 14 exponent terraces when $p = 7$ (and so 14 logarithmic terraces for each primitive root by Theorem 1.7.2). The total number of terraces for $\mathbb{Z}_6$ is 132.

Example 4.3.2 A 2-logarithmic terrace for $p = 11$ is given by

2 4 8 5 6 1 3 9 10 7

which has exponent terrace

4 5 3 10 9 2 8 6 1 7.

Note: There are 1,184 exponent terraces when $p = 11$, out of a total of 60,680 terraces for $\mathbb{Z}_{10}$. Some further information about one of the programming techniques that can be used to obtain these exponent terraces is given in Appendix A.

Example 4.3.3 A 2-logarithmic terrace for $p = 13$ is given by

$$2\ 4\ 8\ 11\ 9\ 10\ 5\ 12\ 1\ 7\ 3\ 6$$

which has exponent terrace

$$4\ 3\ 9\ 7\ 5\ 10\ 6\ 1\ 2\ 11\ 8\ 12.$$

Note: There are 6,284 exponent terraces when $p = 13$, out of a total of 1,954,656 terraces for $\mathbb{Z}_{12}$.

Example 4.3.4 A 3-logarithmic terrace for $p = 17$ is given by

$$3\ 9\ 10\ 13\ 5\ 7\ 4\ 14\ 2\ 11\ 6\ 8\ 1\ 12\ 16\ 15$$

which has exponent terrace

$$10\ 14\ 8\ 12\ 5\ 11\ 13\ 2\ 9\ 7\ 15\ 16\ 3\ 4\ 1\ 6.$$

Example 4.3.5 A 2-logarithmic terrace for $p = 19$ is given by

$$2\ 4\ 8\ 16\ 13\ 7\ 14\ 3\ 5\ 18\ 17\ 9\ 10\ 1\ 6\ 12\ 15\ 11$$

which has exponent terrace

$$4\ 16\ 9\ 5\ 3\ 14\ 6\ 8\ 13\ 1\ 10\ 18\ 17\ 2\ 7\ 11\ 12\ 15.$$

Example 4.3.6 A 5-logarithmic terrace for $p = 23$ is given by

$$9\ 22\ 3\ 2\ 10\ 16\ 6\ 4\ 5\ 20\ 14\ 17\ 12\ 21\ 13\ 15\ 11\ 7\ 19\ 8\ 1\ 18$$

which has exponent terrace

$$11\ 1\ 10\ 2\ 9\ 3\ 8\ 4\ 20\ 12\ 13\ 15\ 18\ 14\ 21\ 19\ 22\ 17\ 7\ 16\ 5\ 6.$$

Example 4.3.7 A 2-logarithmic terrace for $p = 29$ is given by

$$2\ 4\ 8\ 16\ 3\ 6\ 12\ 24\ 19\ 22\ 1\ 21\ 7\ 26\ 15\ 11\ 27\ 25\ 10\ 5\ 23\ 17\ 18\ 28\ 9\ 20\ 13\ 14$$

which has exponent terrace

$$4\ 16\ 24\ 25\ 8\ 6\ 7\ 20\ 26\ 5\ 2\ 17\ 12\ 22\ 27\ 18\ 15\ 11\ 9\ 3\ 10\ 21\ 13\ 1\ 19\ 23\ 14\ 28.$$

It is worth noting that finding such an example for $p = 29$ took a reasonable amount of computer time due to the extremely large number of possible arrangements of the elements of $\mathbb{Z}_{28}$. In the end, it was decided to set some of the elements while bearing in mind the definition of a logarithmic terrace and results such as Theorems 4.2.2 and 4.2.3. This left the computer with significantly fewer possibilities to search through, yet we could be fairly confident that a logarithmic terrace did exist which contained those set values in their respective places.

In general, x-logarithmic terraces for fixed p fall into sets of 4. These are

$$\mathbf{c},\ \mathbf{c}_{rev},\ \mathbf{c} + \tfrac{p-1}{2},\ \mathbf{c}_{rev} + \tfrac{p-1}{2}.$$

In cases where $\mathbf{c}_{rev} \equiv \mathbf{c} + \frac{p-1}{2} \pmod{p-1}$, we get a set of only 2.

Thinking of this in terms of exponent terraces, our sets consist of

$$\mathbf{e},\ \mathbf{e}_{rev},\ -\mathbf{e},\ -\mathbf{e}_{rev},$$

where $-\mathbf{e}$ is the p-complement of $\mathbf{e}$ as defined previously. Here, our sets of 2 arise when $\mathbf{e}_{rev} \equiv -\mathbf{e} \pmod{p}$.

As mentioned above, in the case where $p = 7$, there are 14 exponent terraces. Since 14 is not a multiple of 4, there must be an odd number of sets of size 2. It turns out that there is one set of terraces of size 2 for $p = 7$ where $-\mathbf{e} \equiv \mathbf{e}_{rev} \pmod{p}$. This is given by:

$$\mathbf{e} = 3\ 1\ 2\ 5\ 6\ 4.$$

Such terraces exist in the case of other primes also. As stated previously, when $p = 11$, there are $1,184$ exponent terraces. This is a multiple of 4, which tells us that if there are any sets of 2, there must be an even number of them. In this case, there are actually 4 sets of 2, given by:

$$1\ 9\ 6\ 7\ 3\ 8\ 4\ 5\ 2\ 10,$$
$$2\ 4\ 5\ 1\ 8\ 3\ 10\ 6\ 7\ 9,$$
$$2\ 10\ 4\ 5\ 8\ 3\ 6\ 7\ 1\ 9,$$
$$5\ 1\ 4\ 2\ 3\ 8\ 9\ 7\ 10\ 6.$$

The 6,284 exponent terraces for $p = 13$ were also checked, and it was found that in this case there were no examples where $\mathbf{e}_{rev} = -\mathbf{e} \pmod{p}$. Having found this to be the case, it was natural to wonder if there was an explanation.

Theorem 4.3.1 *The p-complement of an exponent terrace for $\mathbb{Z}_{p-1}$ can be equal to the reverse of that same exponent terrace only when $p \equiv 3 \pmod 4$. In this case, $a_{\frac{p-1}{2}} = \frac{p+1}{4}$ or $\frac{3p-1}{4}$.*

Proof

Assume that such an exponent terrace exists for a prime p, and call it $\mathbf{a}$. In the 2-sequencing for our exponent terrace, the difference $\frac{p-1}{2}$ must appear once (by the definition of a terrace). $\mathbf{a}$ must also satisfy the condition that $\mathbf{a}_{rev} = -\mathbf{a} \pmod{p}$. In order to do so, $\frac{p-1}{2}$ must be the middle difference in the 2-sequencing, and so it is the difference between $a_{\frac{p-1}{2}}$ and $p - a_{\frac{p-1}{2}}$. So we have,

$$\begin{gathered} p - 2a_{\frac{p-1}{2}} \equiv \tfrac{p-1}{2} \pmod{p-1} \\ \text{i.e. } 2p - 4a_{\frac{p-1}{2}} \equiv p - 1 \pmod{2p-2} \\ \text{i.e. } p \equiv 4a_{\frac{p-1}{2}} - 1 \pmod{2p-2} \\ \text{i.e. } p \equiv 3 \pmod 4 \\ \text{and } 4a_{\frac{p-1}{2}} = p + 1 \text{ or } p + 1 + 2p - 2 = 3p - 1. \end{gathered}$$

□

4.4 Terraces which are Simultaneously Logarithmic for Two different Primitive Roots

It is possible to find terraces with respect to a given prime, p, which are logarithmic for two primitive roots simultaneously. There are no examples for $p = 7$.

Example 4.4.1 A 2-logarithmic and 6-logarithmic terrace for $p = 11$ is given by

$$1\ 2\ 6\ 8\ 5\ 10\ 7\ 9\ 3\ 4.$$

Taking it to be 2-logarithmic gives the exponent terrace

$$2\ 4\ 9\ 3\ 10\ 1\ 7\ 6\ 8\ 5,$$

while taking it to be 6-logarithmic gives the exponent terrace

$$6\ 3\ 5\ 4\ 10\ 1\ 8\ 2\ 7\ 9.$$

Looking more closely at the primitive roots of $p = 11$, it can be seen that 2 and 6 are inverses (working modulo 11), as are 7 and 8. For $p = 11$ there are 32 terraces which are both 2-logarithmic and 6-logarithmic, and the same number which are both 7-logarithmic and 8-logarithmic. In cases where the two primitive roots are not inverses modulo 11, there are 20 terraces which are logarithmic with respect to both numbers, e.g., there are 20 terraces which are both 2-logarithmic and 7-logarithmic with respect to $p = 11$.

If we now consider $p = 13$, there are 54 terraces which are both 2-logarithmic and 7-logarithmic, and the same number which are both 6-logarithmic and 11-logarithmic. In cases where the two primitive roots are not inverses modulo 13, there are none which are logarithmic with respect to both.

Example 4.4.2 A 2-logarithmic and 7-logarithmic terrace for $p = 13$ is given by

$$10\ 3\ 11\ 8\ 2\ 7\ 9\ 12\ 1\ 5\ 4\ 6.$$

Taking it to be 2-logarithmic gives the exponent terrace

$$10\ 8\ 7\ 9\ 4\ 11\ 5\ 1\ 2\ 6\ 3\ 12,$$

while taking it to be 7-logarithmic gives the exponent terrace

$$4\ 5\ 2\ 3\ 10\ 6\ 8\ 1\ 7\ 11\ 9\ 12.$$

Example 4.4.3 A 3-logarithmic and 11-logarithmic terrace for $p = 17$ is given by

$$1\ 2\ 5\ 3\ 13\ 4\ 9\ 14\ 10\ 8\ 11\ 12\ 16\ 6\ 15\ 7.$$

Note If we have a logarithmic terrace $\mathbf{a}$ for a given prime p, then we will refer to $\min\{|a_1 - a_{p-1}|,\ p - 1 - |a_1 - a_{p-1}|\}$ as the *end difference.* It turns out that, if $p \leq 13$, then all terraces in $\mathbb{Z}_{p-1}$ which are simultaneously logarithmic for a given pair of primitive roots have the same end difference.

In the case of $p = 7$, there are no logarithmic terraces which are simultaneously logarithmic with respect to two primitive roots. In the case of $p = 11$, the end difference in a terrace which is simultaneously logarithmic with respect to $\{2, 6\}$ is 3, with respect to

$\{2,7\}$, $\{6,7\}$, $\{6,8\}$ or $\{2,8\}$ is 5, and with respect to $\{7,8\}$ is 1.

In the case of $p = 13$, the end difference in a terrace which is simultaneously logarithmic with respect to both $\{2,7\}$ or $\{6,11\}$ is 4. For $p = 13$, there are no terraces which are simultaneously logarithmic with respect to a pair of non-inverses.

In the case of $p = 17$ however, it is possible to find terraces which are logarithmic with respect to the same two fixed primitive roots, but where the end differences are not constant.

Example 4.4.4 The following are examples of terraces for $p = 17$ which are simultaneously logarithmic for both 3 and 7, but where the end differences are different.

$$1\ 2\ 11\ 7\ 14\ 16\ 12\ 9\ 15\ 10\ 4\ 9\ 6\ 8\ 13\ 5,$$

$$8\ 13\ 11\ 15\ 9\ 12\ 5\ 2\ 7\ 16\ 1\ 3\ 4\ 10\ 6\ 14.$$

Theorem 1.7.1 told us that the p-complement of an exponent terrace is also an exponent terrace. The idea of complement terraces also comes into play when dealing with terraces which are simultaneously logarithmic for two primitive roots. If $\mathbf{a}$ is an exponent terrace, the p-complement is found by replacing a_i by $p - a_i$. In the theorem which follows, we will make use of what we will call the $(p-1)$-complement. Here, $\mathbf{a}$ is a logarithmic terrace and the $(p-1)$-complement will be found by replacing a_i by $p-1-a_i$ (except when $a_i = p-1$, in which case a_i is left unchanged).

In general, the $(p-1)$-complement of an x-logarithmic terrace is not also x-logarithmic. For example, the 3-logarithmic terrace of Example 4.3.1 has $(p-1)$-complement

$$4\ 3\ 6\ 2\ 1\ 5$$

which is not 3-logarithmic. Neither is the p-complement

$$5\ 4\ 1\ 3\ 2\ 6$$

which uses what might be considered the better definition of complement.

Theorem 4.4.1 *Let x and y be primitive roots of a fixed prime p, where $xy \equiv 1 \pmod p$. An x-logarithmic terrace, $\mathbf{a}$, is also a y-logarithmic terrace if and only if its $(p-1)$-complement, $\mathbf{b}$, is also an x-logarithmic terrace. The ith elements in the exponent terraces* *of each satisfy $c_i d_i \equiv 1 \pmod p$, where* **c** *is the exponent terrace which corresponds to* **a** *and* **d** *is that which corresponds to* **b**. *The exponent terrace of* **a** *for the primitive root y is also given by* **d**.

Example 4.4.5 The following is such an example for $p = 11$, $x = 7$, $y = 8$.

a	2	4	7	1	8	6	5	10	9	3
b	8	6	3	9	2	4	5	10	1	7
c	5	3	6	7	9	4	10	1	8	2
d	9	4	2	8	5	3	10	1	7	6

Proof

Let x and y be primitive roots such that $y \equiv x^{-1} \pmod p$. Then

$$y^{a_i} \equiv x^{-a_i} \equiv x^{p-1-a_i} \pmod p.$$

So, the $(p-1)$-complement of **a** is x-logarithmic $\Leftrightarrow$ **a** is y-logarithmic.

So if **a** is x-logarithmic and y-logarithmic then the $(p-1)$-complement of **a** is also logarithmic with respect to both x and y.

Further, if $c_i \equiv x^{a_i}$ and $d_i \equiv x^{p-1-a_i}$, then

$$c_i d_i \equiv x^{a_i} x^{p-1-a_i} \equiv x^{p-1} \equiv 1 \pmod p.$$

$\square$

Recall that if **a** is an x-logarithmic terrace for $\mathbb{Z}_{p-1}$, then so is $\mathbf{a} + \frac{p-1}{2}$. Thus, the following result is immediate.

Theorem 4.4.2 *Let x and y be primitive roots of a fixed prime p such that $xy \equiv 1 \pmod p$. If* **a** *is a logarithmic terrace with respect to both x and y, then so is $\mathbf{a} + \frac{p-1}{2} \pmod{p-1}$.*

Theorem 4.4.1 also allows us to think about terraces which are simultaneously logarithmic for two primitive roots in a slightly different way. For example, the terraces for $p = 11$ which are simultaneously logarithmic for both 2 and 8 can also be thought of as the $(p-1)$-complements of 6-logarithmic terraces which are also 8-logarithmic or as the $(p-1)$-complements of 7-logarithmic terraces which are also 2-logarithmic.

Note If x, y are not inverse of one another, then the $(p-1)$-complement of a terrace that is both x-logarithmic and y-logarithmic need not be x-logarithmic and y-logarithmic.

Example 4.4.6 An example of a 2-logarithmic and 7-logarithmic for $p = 11$ is given by

$$4\ 2\ 5\ 6\ 1\ 7\ 8\ 10\ 3\ 9.$$

Its $(p-1)$-complement

$$6\ 8\ 5\ 4\ 9\ 3\ 2\ 10\ 7\ 1$$

is neither. Indeed for $p = 11$ there is no such example for any pair of x, y which are not inverses.

Theorem 4.4.3 *If* $\mathbf{a}$ *is an* x*-logarithmic terrace for* p*, where* $p \equiv 1 \pmod 4$*, then the terrace,* $\mathbf{c}$*, formed by adding* $\frac{p-1}{2}$ *to all odd or all even elements in* $\mathbf{a}$ *is* $(p-x)$*-logarithmic.*

Proof

From Theorem 4.2.1, we know that $\mathbf{c}$ is a terrace. Now we want to show that it is $(p-x)$-logarithmic in both cases. It should be remembered that when $p \equiv 1 \pmod 4$, the negative of a primitive root is also a primitive root.

We first show that adding $\frac{p-1}{2}$ to all of the odd elements of $\mathbf{a}$ gives a $(p-x)$-logarithmic terrace since the resulting exponent terrace for $\mathbf{c}$ is the same as that for $\mathbf{a}$.

If we first consider the even elements from $\mathbf{a}$, then

$$x^{2i} \equiv (-(p-x))^{2i} \equiv (p-x)^{2i} \pmod p.$$

If we now consider the odd elements from $\mathbf{a}$ (with $\frac{p-1}{2}$ added), we see that

$$\begin{aligned} x^{2i+1} &\equiv (-(p-x))^{2i+1} \equiv -(p-x)^{2i+1} \\ &\equiv (p-x)^{\frac{p-1}{2}}.(p-x)^{2i+1} \\ &\equiv (p-x)^{2i+1+\frac{p-1}{2}} \pmod p. \end{aligned}$$

We next show that adding $\frac{p-1}{2}$ to all of the even elements of $\mathbf{a}$ gives a $(p-x)$-logarithmic terrace since the resulting exponent terrace for $\mathbf{c}$ is the p-complement of that for $\mathbf{a}$.

If we first consider the even elements from $\mathbf{a}$ (with $\frac{p-1}{2}$ added), then

$$\begin{aligned}(p-x)^{2i+\frac{p-1}{2}} &\equiv -(p-x)^{2i}\\ &\equiv -x^{2i} \pmod p.\end{aligned}$$

If we now consider the odd elements from **a**, we see that

$$(p-x)^{2i+1} \equiv -x^{2i+1} \pmod p.$$

□

Example 4.4.7 An example of a 2-logarithmic terrace in $\mathbb{Z}_{12}$ is given by

$$1\ 3\ 6\ 7\ 2\ 12\ 8\ 11\ 10\ 4\ 9\ 5.$$

Adding 6 to all odd elements gives

$$7\ 9\ 6\ 1\ 2\ 12\ 8\ 5\ 10\ 4\ 3\ 11,$$

which it can be seen is 11-logarithmic. Adding 6 to all even elements gives

$$1\ 3\ 12\ 7\ 8\ 6\ 2\ 11\ 4\ 10\ 9\ 5,$$

which is also 11-logarithmic.

We now consider p-complements.

Suppose that **a** is an x-logarithmic terrace in $\mathbb{Z}_{p-1}$. Then its exponent terrace is

$$x^{a_1}\ \ldots\ x^{a_{p-1}},$$

and its p-complement is given by

$$p-a_1\ \ldots\ p-a_{p-1}.$$

Now consider

$$x^{p-a_1}\ \ldots\ x^{p-a_{p-1}},$$

$$\text{i.e. } x^{1-a_1}\ \ldots\ x^{1-a_{p-1}}, \text{ since } x^{p-1} \equiv 1 \pmod p,$$

$$\text{i.e. } y^{a_1-1}\ \ldots\ y^{a_{p-1}-1}, \text{ where } xy \equiv 1 \pmod p.$$

We have therefore proved the following.

Theorem 4.4.4 *Let x and y be primitive roots of a fixed prime p such that $xy \equiv 1 \pmod{p}$. The p-complement of an x-logarithmic terrace, $\mathbf{a}$, is also x-logarithmic if and only if $(\mathbf{a}-1)$ is y-logarithmic.*

Example 4.4.8 The following is 2-logarithmic for $p = 13$.

$$\mathbf{a} = 11 \;\; 10 \;\; 4 \;\; 9 \;\; 5 \;\; 2 \;\; 12 \;\; 8 \;\; 1 \;\; 3 \;\; 6 \;\; 7.$$

Its exponent terrace is given by

$$7 \;\; 10 \;\; 3 \;\; 5 \;\; 6 \;\; 4 \;\; 1 \;\; 9 \;\; 2 \;\; 8 \;\; 12 \;\; 11.$$

It can also be seen that

$$\mathbf{a} - 1 = 10 \;\; 9 \;\; 3 \;\; 8 \;\; 4 \;\; 1 \;\; 11 \;\; 7 \;\; 12 \;\; 2 \;\; 5 \;\; 6,$$

is 7-logarithmic with exponent terrace

$$4 \;\; 8 \;\; 5 \;\; 3 \;\; 9 \;\; 7 \;\; 2 \;\; 6 \;\; 1 \;\; 10 \;\; 11 \;\; 12.$$

So the p-complement of $\mathbf{a}$ is also 2-logarithmic.

It can be seen that the product of corresponding terms in the exponent terraces are all 2 (modulo 13). This is due to the fact that $x^{a_1}y^{a_1-1} = x^{a_1}x^{p-a_1} = x^p \equiv x \pmod{p}$.

Notes

1. In general, if $\mathbf{a}$ is a logarithmic terrace, $\mathbf{a} - 1$ is not.

2. Theorems 4.4.3 and 4.4.4 also help us to see that when $p \equiv 1 \pmod{4}$, there is a one to one correspondence between x-logarithmic terraces whose p-complements are also x-logarithmic, and $(p - x)$-logarithmic terraces whose p-complements are also $(p - x)$-logarithmic. For example when $p = 13$, there are 64 terraces which are 11-logarithmic and whose p-complements are also 11-logarithmic, and the same number which are 2-logarithmic and whose p-complements are also 2-logarithmic.

Consider Example 4.4.8 above which is 2-logarithmic, as is its p-complement. As we have seen, by Theorem 4.4.4,

$$\mathbf{a}-1 = 10\ 9\ 3\ 8\ 4\ 1\ 11\ 7\ 12\ 2\ 5\ 6$$

is 7-logarithmic. From **a** we obtain, by use of Theorem 4.4.3, the 11-logarithmic terrace

$$\mathbf{c} = 5\ 10\ 4\ 3\ 11\ 2\ 12\ 8\ 7\ 9\ 6\ 1,$$

and similarly from $\mathbf{a}-1$ we obtain the 6-logarithmic terrace

$$4\ 9\ 3\ 2\ 10\ 1\ 11\ 7\ 6\ 8\ 5\ 12.$$

Since this is $\mathbf{c}-1$, it follows from Theorem 4.4.4 that the p-complement of **c** is 11-logarithmic. This illustrates the one to one correspondence described above.

In Example 4.4.7 above, the 2-logarithmic terrace given has a p-complement which is another 2-logarithmic terrace,

$$12\ 10\ 7\ 6\ 11\ 1\ 5\ 2\ 3\ 9\ 4\ 8.$$

Adding $\frac{p-1}{2}$ to the odd or even elements of this terrace also gives two 11-logarithmic terraces.

Note It can be seen that adding $\frac{p-1}{2}$ (mod $p-1$) to all odd elements of a terrace and then taking the p-complement is the same as first taking the p-complement and then adding $\frac{p-1}{2}$ (mod $p-1$) to all even elements. Looking back at the original terrace given in Example 4.2.1 it can be seen that both of these options give

$$9\ 4\ 10\ 7\ 6\ 11\ 8\ 12\ 2\ 3\ 5\ 1.$$

Theorem 4.4.5 *Let x, y, u and v be primitive roots of a fixed prime p. If $xy \equiv 1 \pmod p$ and $uv \equiv 1 \pmod p$, then the number of terraces which are both x-logarithmic and y-logarithmic is the same as the number which are both u-logarithmic and v-logarithmic. The x-logarithmic and y-logarithmic terraces give rise to the same set of exponent terraces as the u-logarithmic and v-logarithmic terraces.*

Proof

Assume we have a terrace **a** which is both x-logarithmic and y-logarithmic. Since u and v are primitive roots of p, x and y can be expressed as powers of both (modulo p). So we have

$$x \equiv u^m \pmod p \text{ and } x \equiv v^n \pmod p.$$

Since $xy \equiv 1 \pmod p$ and $uv \equiv 1 \pmod p$, we can see that

$$y \equiv x^{-1} \equiv u^{-m} \equiv v^m \ (\text{mod} p),$$

as well as

$$y \equiv x^{-1} \equiv v^{-n} \equiv u^n \ (\text{mod} p).$$

So it can be seen that $m \equiv -n \pmod{p-1}$.

The above shows that multiplying **a** by m will give us a terrace which is both u-logarithmic and v-logarithmic, as will multiplying by n. Since $m \equiv -n \pmod{p-1}$, and since we already know that the $(p-1)$-complement of a terrace which is x-logarithmic and y-logarithmic is also x-logarithmic and y-logarithmic, this confirms that a terrace which is logarithmic with respect to x and y can be multiplied by an integer to give us a terrace which (along with its $(p-1)$-complement) is logarithmic with respect to u and v.

This one to one correspondence between terraces which are simultaneously logarithmic for two primitive roots which are inverses modulo p, in combination with Theorem 1.7.2, tells us that the exponent terraces for any two such simultaneously logarithmic terraces will be the same.

□

Definition 4.4.1 Let S denote the set of unordered pairs of primitive roots of p. Let $(u, v) \sim (x, y)$ if and only if there exists an α, with g.c.d.$(\alpha, p-1) = 1$, such that $u \equiv x^\alpha \pmod{p-1}$, $v \equiv y^\alpha \pmod{p-1}$ or $u \equiv y^\alpha \pmod{p-1}$, $v \equiv x^\alpha \pmod{p-1}$.

Lemma 4.4.6 $\sim$ *is an equivalence relation.*

Proof

(i) $(u, v) \sim (u, v)$ (take $\alpha = 1$).

(ii) Suppose $(u, v) \sim (x, y)$. First suppose there exists an α, with g.c.d.$(\alpha, p-1) = 1 \pmod{p-1}$ such that $u \equiv x^\alpha \pmod{p-1}$, $v \equiv y^\alpha \pmod{p-1}$.

Define β by $\alpha\beta \equiv 1 \pmod{p-1}$. Then $u^\beta \equiv x \pmod{p-1}$, $v^\beta \equiv y \pmod{p-1}$ so that $(x, y) \sim (u, v)$. If we have $u \equiv y^\alpha \pmod{p-1}$, $v \equiv x^\alpha \pmod{p-1}$ then $u^\beta \equiv y \pmod{p-1}$, $v^\beta \equiv x \pmod{p-1}$ so $(x, y) \sim (u, v)$.

(iii) Suppose $(u,v) \sim (x,y)$ and $(x,y) \sim (w,z)$ and that there exists α, β such that $u \equiv x^{\alpha} \pmod{p-1}$, $v \equiv y^{\alpha} \pmod{p-1}$, $x \equiv w^{\beta} \pmod{p-1}$, $y \equiv z^{\beta} \pmod{p-1}$.

Then, $u \equiv w^{\alpha\beta} \pmod{p-1}$, $v \equiv z^{\alpha\beta} \pmod{p-1}$ where g.c.d.$(\alpha\beta, p-1) = 1$. So $(u,v) \sim (w,z)$.

Next we will suppose that $u \equiv x^{\alpha} \pmod{p-1}$, $v \equiv y^{\alpha} \pmod{p-1}$, $x \equiv z^{\beta} \pmod{p-1}$, $y \equiv w^{\beta} \pmod{p-1}$. Then $u \equiv z^{\alpha\beta} \pmod{p-1}$, $v \equiv w^{\alpha\beta} \pmod{p-1}$ and so $(u,v) \sim (w,z)$.

Suppose $u \equiv y^{\alpha} \pmod{p-1}$, $v \equiv x^{\alpha} \pmod{p-1}$, $x \equiv w^{\beta} \pmod{p-1}$, $y \equiv z^{\beta} \pmod{p-1}$. Then $u \equiv z^{\alpha\beta} \pmod{p-1}$, $v \equiv w^{\alpha\beta} \pmod{p-1}$ and so $(u,v) \sim (w,z)$.

□

Example 4.4.9 For $p = 11$, the primitive roots are 2, 6, 7, 8. The equivalence classes are

(i) $\{(2,6),(7,8)\}$,

(ii) $\{(2,7),(2,8),(6,7),(6,8)\}$.

Note: As shown in the proof of Theorem 4.4.5, inverse pairs of primitive roots form one of the equivalence classes.

Theorem 4.4.7 *Let x, y, u, v be primitive roots of p. If $(x,y) \sim (u,v)$ then for each terrace which is logarithmic for both x and y, there is a multiple of this terrace which is a logarithmic terrace for both u and v.*

Proof

If $x = u^r$, $y = v^r$ and $(a_1, a_2, \ldots, a_{p-1})$ is logarithmic for both x and y, then $(ra_1, ra_2, \ldots, ra_{p-1})$ is a logarithmic terrace for both u and v.

□

Corollary 4.4.8 *For each equivalent pair of primitive roots, there are the same number of terraces which are simultaneously logarithmic.*

The above tells us that if we have a terrace corresponding to one pair from each equivalence class, then we can find a terrace which is simultaneously logarithmic for any equivalent pairs of primitive roots.

In the case of $p = 11$, there are two equivalence classes (as seen in Example 4.4.9 above). Example 4.4.1 in association with the following terrace which is logarithmic with respect to both 2 and 7, shows that we can find a terrace which is simultaneously logarithmic with respect to any pair of primitive roots for $p = 11$.

Example 4.4.10 A 2-logarithmic and 7-logarithmic terrace for $p = 11$ is given by

$$4\ 2\ 5\ 6\ 1\ 7\ 8\ 10\ 3\ 9.$$

Since $2 \equiv 8^7$ and $7 \equiv 2^7 \pmod{11}$, multiplying by 7 (mod 10) gives the terrace

$$8\ 4\ 5\ 2\ 7\ 9\ 6\ 10\ 1\ 3$$

which is both 2-logarithmic and 8-logarithmic.

In the case of $p = 13$, there are three equivalence classes. These are given by

(i) $\{(2,7),(6,11)\}$,
(ii) $\{(2,6),(7,11)\}$,
(iii) $\{(2,11),(6,7)\}$.

Example 4.4.2 is one example of a terrace which is logarithmic with respect to a pair of primitive roots which occurs in the equivalence class that contains the inverse pairs (see (i) above). There are no such simultaneously logarithmic terraces for non-inverse pairs when $p = 13$.

In the case of $p = 17$, there are five equivalence classes which are as follows, with the first class consisting of inverse pairs.

(i) $\{(3,6),(5,7),(10,12),(11,14)\}$,
(ii) $\{(3,5),(3,12),(5,14),(6,7),(6,10),(7,11),(10,11),(12,14)\}$,
(iii) $\{(3,7),(3,10),(5,6),(5,11),(6,12),(7,14),(10,14),(11,12)\}$,
(iv) $\{(3,11),(5,10),(6,14),(7,12)\}$,
(v) $\{(3,14),(5,12),(6,11),(7,10)\}$.

Example 4.4.3 in conjunction with the following four examples shows that for each of these pairs a terrace which is simultaneously logarithmic does exist.

Example 4.4.11 A 3-logarithmic and 12-logarithmic terrace for $p = 17$ is given by

$$3\ 1\ 5\ 14\ 10\ 4\ 13\ 8\ 2\ 16\ 11\ 12\ 15\ 7\ 6\ 9.$$

Example 4.4.12 A 3-logarithmic and 7-logarithmic terrace for $p = 17$ is given by

$$1\ 2\ 11\ 7\ 14\ 16\ 12\ 9\ 15\ 10\ 4\ 3\ 6\ 8\ 13\ 5.$$

Example 4.4.13 A 3-logarithmic and 14-logarithmic terrace for $p = 17$ is given by

$$1\ 2\ 11\ 3\ 8\ 10\ 13\ 6\ 9\ 5\ 15\ 16\ 4\ 14\ 12\ 7.$$

Example 4.4.14 A 3-logarithmic and 6-logarithmic terrace for $p = 17$ is given by

$$4\ 2\ 5\ 12\ 11\ 16\ 15\ 8\ 14\ 3\ 1\ 9\ 13\ 7\ 10\ 6.$$

Note that the classes (i), (iv) and (v) are half of the size of classes (ii) and (iii). We now explain this phenomenon.

In (i), $(5,7) \sim (3,6)$ since $5 \equiv 3^5$ and $7 \equiv 6^5$, but also because $5 \equiv 6^{11}$ and $7 \equiv 3^{11}$. A terrace that is simultaneously 5-logarithmic and 7-logarithmic can be converted into a terrace that is simultaneously 3-logarithmic and 6-logarithmic by multiplying by either 5 or 11. Such a situation can occur only when there are primitive roots x, y, u, v and integers α, β such that $u \equiv x^\alpha$, $v \equiv y^\alpha$, $u \equiv y^\beta$, $v \equiv x^\beta$, i.e. where $x \equiv y^c$ and $y \equiv x^c$ (where $c \equiv \frac{\alpha}{\beta} \pmod{p-1}$). But in such cases $y \equiv x^c \equiv y^{c^2} \pmod{p}$, so that $c^2 \equiv 1 \pmod{p-1}$.

The following theorem can be found in [25, Theorem 5-2].

Theorem 4.4.9 *If $(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ is solvable, it has exactly $2^{\sigma+\tau}$ solutions, where σ is the number of distinct odd prime divisors of m and τ is 0, 1, or 2 according as $4 \nmid m$, $2^2 \| m$ ($2^2 | m$ but 2^3 doesn't), or $8 | m$.*

Example 4.4.15 Take $p = 17$, $m = p - 1 = 16$, $a = 1$. So we are interested in the solutions to $x^2 \equiv 1 \pmod{16}$. Here, $\sigma = 0$ and $\tau = 2$ so there are $2^2 = 4$ solutions, namely 1, 7, 9, 15. Ignoring 1, we see that there are therefore three classes which are half the size of the others.

(i) The class of inverse pairs. Here $x \equiv y^{15}$ for each pair, so $c = 15$.

(ii) $3 \equiv 11^7$ and $11 \equiv 3^7$ corresponding to $c = 7$.

(iii) $3 \equiv 14^9$ and $14 \equiv 3^9$ corresponding to $c = 9$.

Example 4.4.16 $p = 19$. Here, the congruence $x^2 \equiv 1 \pmod{18}$ has only two solutions since $\sigma = 1$ and $\tau = 0$. The solution other than 1 is 17, corresponding to the class of inverse pairs. There are six primitive roots of 19, so there are $\binom{6}{2} = 15$ pairs. One class consists of three pairs, and two classes consist of six pairs. The classes are

(i) $\{(2,10),\ (3,13),\ (14,15)\}$,

(ii) $\{(2,3),\ (2,14),\ (3,14),\ (10,13),\ (10,15),\ (13,15)\}$,

(iii) $\{(2,13),\ (2,15),\ (3,10),\ (3,14),\ (3,15),\ (10,14)\}$.

4.5 Rejoinable and Pseudo-rejoinable Terraces

We define a logarithmic terrace to be *rejoinable* if it can be partitioned into two segments such that, when the segments are interchanged, another logarithmic terrace is obtained. Equivalently we could say that a logarithmic terrace is rejoinable if it can be split into two segments such that, when each segment is reversed, another logarithmic terrace is obtained. Accordingly, we define a logarithmic terrace to be *pseudo-rejoinable* if it can be partitioned into two segments such that, when just one of them is reversed, another logarithmic terrace is obtained.

In representations of rejoinable logarithmic terraces, we use a vertical bar | (or "fence") to indicate the point of section. Likewise, in representations of pseudo-rejoinable logarithmic terraces, we use a vertical bar preceded or followed by a horizontal arrow pointing to the segment to be reversed. We use vertical bars and arrows likewise in the exponent terraces corresponding to rejoinable and pseudo-rejoinable logarithmic terraces.

Example 4.5.1 A 2-logarithmic terrace for $p = 11$ which is both rejoinable and pseudo-rejoinable is given by

$$4\ 7\ 9\ 8 \leftarrow |\ 6\ 2\ 3\ |\ 10\ 5\ 1.$$

The corresponding exponent terrace is given by

$$5\ 7\ 6\ 3 \leftarrow |\ 9\ 4\ 8\ |\ 1\ 10\ 2.$$

Theorem 4.5.1 *If x and y are primitive roots for a given prime p, there is a one to one correspondence between rejoinable terraces for x and those for y.*

Proof

Let $\mathbf{a}$ be a rejoinable terrace with respect to primitive root x of p. Since it is rejoinable,

$$a_n - a_{n+1} \equiv \pm(a_1 - a_{p-1}) \pmod{p-1}, \text{ for some } n,\ 1 \leq n \leq p-2.$$

By Theorem 1.7.2, the exponent terrace corresponding to this terrace is also the exponent terrace for a y-logarithmic terrace, $\mathbf{c}$, where y is any other primitive root of p, and where, if $x \equiv y^d \pmod{p}$, $c_i \equiv da_i \pmod{p-1}$. It follows that

$$d(a_n - a_{n+1}) \equiv \pm d(a_1 - a_{p-1}) \pmod{p-1},$$
$$\text{i.e. } c_n - c_{n+1} \equiv \pm(c_1 - c_{p-1}) \pmod{p-1}.$$

and $\mathbf{c}$ is rejoinable in the same place(s).

□

Example 4.5.2 A 3-logarithmic rejoinable terrace for $p = 7$ is given by

1 3 6 5 | 4 2.

$3 \equiv 5^5 \pmod 7$ and so by Theorem 1.7.2 we know that multiplying the above terrace by 5 and working modulo 6 will give us a 5-logarithmic terrace:

5 3 6 1 | 2 4.

The differences are all multiplied by a factor of 5, and it can be seen that this terrace is also rejoinable (in the same place as the original 3-logarithmic terrace).

Corollary 4.5.2 *There is a one to one correspondence between pseudo-rejoinable terraces for different primitive roots.*

The following example shows that it is possible for an x-logarithmic terrace to be rejoinable in two different places.

Example 4.5.3 The following 2-logarithmic terrace for $p = 11$ can be rejoined at either of the places indicated.

2-logarithmic	1 9 3 | 10 5 | 8 7 6 2 4
exponent	2 6 8 | 1 10 | 3 7 9 4 5

It is also possible for a terrace to be simultaneously rejoinable with respect to two different primitive roots, although in the cases of $p = 7$ and $p = 13$, there are no such examples.

In the case of $p = 11$, there are such examples where x, y are the primitive roots and $xy \equiv 1 \pmod{p}$. We do not have any examples for larger primes, but there is no reason to suppose that they do not exist.

Example 4.5.4 A 2-logarithmic and 6-logarithmic terrace which is rejoinable for both primitive roots 2 and 6 is given by

$$1\ 2\ 6\ 8 \overset{2}{|}\ 5\ 10 \overset{6}{|}\ 7\ 9\ 3\ 4.$$

Example 4.5.5 A 7-logarithmic and 8-logarithmic terrace which is rejoinable for both primitive roots 7 and 8 is given by

$$3\ 6\ 8\ 4 \overset{7}{|}\ 5\ 10 \overset{8}{|}\ 1\ 7\ 9\ 2.$$

Looking more closely at the above examples, it can be seen that 2 and 6 are inverses modulo 11, as are 7 and 8. It can also be seen that if we regard Example 4.5.4 as being 2-logarithmic and Example 4.5.5 as being 7 logarithmic, then they have the same exponent terrace. The same is true if we regard Example 4.5.4 as being 6-logarithmic and Example 4.5.5 as being 8-logarithmic. In fact, since $2 \equiv 7^3 \pmod{11}$, $6 \equiv 8^3 \pmod{11}$, $2 \equiv 8^7 \pmod{11}$ and $6 \equiv 7^7 \pmod{11}$, multiplying the terrace in Example 4.5.5 by either 3 or 7 (working modulo 10) gives a terrace which is rejoinable with respect to both 7 and 8. Multiplying by 3 gives the terrace seen above in Example 4.5.5.

Theorem 4.5.3 *There is a one to one correspondence between terraces which are simultaneously rejoinable for two primitive roots x and y, when $xy \equiv 1 \pmod{p}$, and those which are simultaneously rejoinable for primitive roots u, v where $uv \equiv 1 \pmod{p}$.*

Proof

Let $\mathbf{a}$ be a rejoinable terrace with respect to x and y. If we follow the same argument as in Theorem 4.5.1, replacing y with u, then if $x \equiv u^d$ and $c_i \equiv da_i \pmod{p-1}$ it can be seen that $\mathbf{c}$ is rejoinable with respect to u. $\mathbf{a}$, when regarded as being an x-logarithmic terrace, has the same exponent terrace as $\mathbf{c}$ when it is regarded as being u-logarithmic. Applying the same argument to y and v where $y \equiv v^d \pmod{p-1}$, it can be seen that $\mathbf{c}$ is also rejoinable with respect to v. **a**, when regarded as being a y-logarithmic terrace, has the same exponent terrace as **c** when it is regarded as being v-logarithmic. So **c** is both u-logarithmic and v-logarithmic.

□

As a special case of the above procedure, suppose that a terrace is both x-logarithmic and y-logarithmic where $xy \equiv 1 \pmod p$, and is rejoinable for both x and y. Taking $u = y$ and $v = x$ we have $x \equiv y^{p-2}$ and $y \equiv x^{p-2} \pmod p$, so multiplying by $p-2 \pmod{p-1}$, i.e. taking the $(p-1)$-complement, gives another terrace which is both x-logarithmic and y-logarithmic. By Theorem 4.5.1, this is rejoinable for x at the same place as the original terrace was rejoinable for y, and vice versa. So we immediately have the following theorem.

Theorem 4.5.4 *For prime p, let **a** be a terrace which is both logarithmic and rejoinable with respect to two primitive roots, x and y, where $xy \equiv 1 \pmod p$. The $(p-1)$-complement of such a terrace, **b**, is also rejoinable with respect to x and y, with the fences occurring in the same positions, but with the primitive roots with respect to which the terrace is rejoinable at these positions being switched over.*

Example 4.5.6 Recall the 2-logarithmic and 6-logarithmic terrace which is rejoinable for both primitive roots 2 and 6 from Example 4.5.4.

$$1\ 2\ 6\ 8 \overset{2}{|} 5\ 10 \overset{6}{|} 7\ 9\ 3\ 4.$$

The $(p-1)$-complement of this terrace is

$$9\ 8\ 4\ 2 \overset{6}{|} 5\ 10 \overset{2}{|} 3\ 1\ 7\ 6,$$

and it can be seen that this is also rejoinable with respect to 2 and 6, with the fences in the same position but with the primitive roots with respect to which it is rejoinable at these positions swapped over.

Chapter 5

Training Schedules

5.1 Introduction

Consider the following array

$$\begin{array}{cccccccccc}
1 & 2 & 5 & 3 & 4 & 5 & 1 & 4 & 2 & 3 \\
2 & 3 & 1 & 4 & 5 & 1 & 2 & 5 & 3 & 4 \\
3 & 4 & 2 & 5 & 1 & 2 & 3 & 1 & 4 & 5 \\
4 & 5 & 3 & 1 & 2 & 3 & 4 & 2 & 5 & 1 \\
5 & 1 & 4 & 2 & 3 & 4 & 5 & 3 & 1 & 2 \\
1 & 3 & 4 & 5 & 2 & 4 & 1 & 2 & 3 & 5 \\
2 & 4 & 5 & 1 & 3 & 5 & 2 & 3 & 4 & 1 \\
3 & 5 & 1 & 2 & 4 & 1 & 3 & 4 & 5 & 2 \\
4 & 1 & 2 & 3 & 5 & 2 & 4 & 5 & 1 & 3 \\
5 & 2 & 3 & 4 & 1 & 3 & 5 & 1 & 2 & 4 \\
1 & 4 & 3 & 2 & 5 & 3 & 1 & 5 & 4 & 2 \\
2 & 5 & 4 & 3 & 1 & 4 & 2 & 1 & 5 & 3 \\
3 & 1 & 5 & 4 & 2 & 5 & 3 & 2 & 1 & 4 \\
4 & 2 & 1 & 5 & 3 & 1 & 4 & 3 & 2 & 5 \\
5 & 3 & 2 & 1 & 4 & 2 & 5 & 4 & 3 & 1 \\
1 & 5 & 2 & 4 & 3 & 2 & 1 & 3 & 5 & 4 \\
2 & 1 & 3 & 5 & 4 & 3 & 2 & 4 & 1 & 5 \\
3 & 2 & 4 & 1 & 5 & 4 & 3 & 5 & 2 & 1 \\
4 & 3 & 5 & 2 & 1 & 5 & 4 & 1 & 3 & 2 \\
5 & 4 & 1 & 3 & 2 & 1 & 5 & 2 & 4 & 3
\end{array} \tag{5.1.1}$$

It can be seen that each row of this array consists of a permutation of $1, \ldots, 5$ followed by another. We will consider each permutation to be a *block*. A closer look shows that the array is made up of eight 5×5 Latin squares. Each row also contains nine ordered pairs of adjacent distinct numbers. The first row, for example, has the distinct pairs $\{1,2\}, \{2,5\}, \{5,3\}, \ldots, \{2,3\}$. It should further be noted that each of the 20 possible ordered pairs feature exactly once in any two adjacent columns and that within each row, the jth entry in the second block always differs from the jth entry in the first block. This array is a solution in the case $n = 5$ to the problem concerning the construction of training schedules for $n(n-1)$ athletes which are to be balanced in various ways for carryover effects. A repeated carryover effect arises wherever X follows Y more than once. Suppose that there are $n(n-1)$ athletes and n tasks, and that each athlete has to carry out the n tasks in some order and then repeat them in a different order in $2n$ periods of time. In the above array, this is done in such a way that

i. no carryover occurs twice for any athlete;

ii. in any two consecutive periods each carryover occurs exactly once;

iii. for any $j \leq n$, each athlete has different tasks in the jth and $(n+j)$th periods.

If we look at the left half of (5.1.1), it can be seen that it is clearly *cyclic* in the sense that row $5i+j+1$ is obtained from row $5i+1$ by adding $j \pmod 5$ to each number, $0 \leq i < 4$, $0 \leq j \leq 4$. So the design is based on the Williams terrace of Section 1.9, and is built cyclically from rows 1, 6, 11 and 16:

$$\begin{array}{ccccc} 1 & 2 & 5 & 3 & 4 \\ 1 & 3 & 4 & 5 & 2 \\ 1 & 4 & 3 & 2 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{array} \qquad (5.1.2)$$

These rows have differences

$$\begin{array}{cccc} 1 & 3 & 3 & 1 \\ 2 & 1 & 1 & 2 \\ 3 & 4 & 4 & 3 \\ 4 & 2 & 2 & 4 \end{array} \qquad (5.1.3)$$

If $n = p = 2m+1$, then in general the $n-1$ lines of differences are established through multiplication of the original line of differences by a ($a = 1, 2, \ldots, 2m$). Since p is a prime, a can be anything less than p. It can then be seen that the left half of the schedules for our $n(n-1)$ athletes are formed using the $n-1$ lines of differences, with the cyclic property mentioned above meaning that each line allows for the construction of a block for n athletes (which is an $n \times n$ Latin square).

The differences in (5.1.2) are also the differences between adjacent pairs of numbers on the right half of (5.1.1), with a column of differences down the middle so that the first entry on the right half can be obtained from the last entry on the left half. So the differences used are as follows:

$$\begin{array}{cccc|c|cccc} 1 & 3 & 3 & 1 & 1 & 1 & 3 & 3 & 1 \\ 2 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 2 \\ 3 & 4 & 4 & 3 & 3 & 3 & 4 & 4 & 3 \\ 4 & 2 & 2 & 4 & 4 & 4 & 2 & 2 & 4 \end{array}$$

In practical terms, this means that once we have the first row of our array, it is possible to obtain all other rows from it. If we look at the differences in row 1, we then multiply these by 2, 3 and 4 (working modulo 5 each time) in order to construct rows 6, 11 and 16. The other rows can then be obtained by making use of the cyclic structure mentioned above.

From this point onwards, instead of writing out the schedule for each player of the $n(n-1)$ players in full, we will focus on the schedule of the first player since the schedules for the others can be obtained from it. In addition, each permutation of the n activities for this player will be regarded as a block and represented by a row in a Latin rectangle. For example, (5.1.1) would be represented by

$$\begin{array}{ccccc} 1 & 2 & 5 & 3 & 4 \\ 5 & 1 & 4 & 2 & 3 \end{array}$$

In [11] it is shown how to construct such a schedule (with each activity being carried out twice) when n is an odd prime or $n = 9$, 15 or 25. In this chapter, we will be trying to generalise this work so that each of our $n(n-1)$ athletes can carry out all n tasks as many times as possible, rather than just twice. The following conditions must still be satisfied:

- **i.** no carryover occurs twice for any athlete;
- **ii.** in any two consecutive periods each carryover occurs exactly once;
- **iii.** for any $j \leq n$, each athlete has different tasks in the $kn+j$th periods, $0 \leq k \leq b-1$, where b is the number of blocks.

In addition to being interested in the carryovers within each block, we are also interested in the carryovers between blocks which are obtained by looking at the last element of a block and the first element of the subsequent one. So the maximum number of times that each of the tasks could be carried out by an athlete is theoretically $n-1$. This is the case since if we are working with n tasks, there are $n(n-1)$ possible carryovers. If each activity is carried out $(n-1)$ times, that would result in $n(n-1)-1$ carryovers within each row. Since this is clearly less than the number of possible carryovers, they could all be distinct. In the case where $n=3$ for example, it can be seen that each activity can be carried out twice without any repeated carryovers.

Example 5.1.1 A schedule for 6 players (when $n=3$) is given by

$$\begin{array}{c}(123)(213)\\(231)(321)\\(312)(132)\\(213)(123)\\(321)(231)\\(132)(312)\end{array}$$

It can be seen that this example does not satisfy the third of the conditions mentioned above however, since the third element in each block is the same within each row.

In this chapter, we will be looking at how an activity can be carried out as many times as possible while focussing on how terraces can assist us in this task. It is possible for an activity to be carried out a number of times and still satisfy all of the relevant conditions without the use of terraces however. In the case where $n=5$, it turns out that each activity can be carried out a maximum of three times. Without loss of generality, if we assume that the first block for the first player is given by

$$1\quad 2\quad 3\quad 4\quad 5$$

then there are four different ways in which the activities can be carried out three times so that the required conditions are satisfied. The schedule for the first player in each of these cases is as follows:

$$\left.\begin{array}{ccccc}1&2&3&4&5\\2&4&1&5&3\\5&1&4&3&2\end{array}\right\}(1)$$

$$\left.\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \\ 5 & 3 & 2 & 1 & 4 \end{array}\right\} (2)$$

$$\left.\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \\ 2 & 5 & 4 & 1 & 3 \end{array}\right\} (3)$$

$$\left.\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \\ 3 & 1 & 5 & 2 & 4 \end{array}\right\} (4)$$

5.2 Repeats using the Williams Terrace

We are now going to focus specifically on the case where n is a prime, $p = 2m + 1$. Using the Williams terrace to give us the necessary differences, each activity can be carried out at least $(p-3)/2$ times, although how we build the schedule depends on the value of $p \pmod 4$.

If the first element of a block is taken to be X, then the last element in that block will be $X + a(m + 1)$ if we have used the Williams terrace. Looking back at the first row of (5.1.2) where $p = 5$ and $a = 1$, it can be seen that the difference between the first and last elements is $a(m + 1) = 3$, while the difference between the first and last elements in the second row where $a = 2$ is also $a(m+1) = 6 \equiv 1 \pmod 5$. Recalling that $a = 1, 2, \ldots, 2m$, it can be seen that this holds for the other rows.

In general, if we are working with the Williams terrace and i is even, the ith entry in the $(k+1)$th block, where b is the number of blocks, $0 \leq k \leq b-1$, d is the difference between blocks and X is the first element of the first block, is

$$X + ka(m + 1 + d) + \tfrac{ia}{2} \pmod{2m + 1},$$

while the $(2m + 1 - i)$th entry in such a block is

$$X + ka(m + 1 + d) - \tfrac{(2m-i)a}{2} \pmod{2m + 1}.$$

If i is odd, then the ith entry in the $(k + 1)$th block is

$$X + ka(m + 1 + d) - \tfrac{(i-1)a}{2} \pmod{2m + 1},$$

while the $(2m+1-i)$th entry in such a block is

$$X + ka(m+1+d) + \tfrac{(2m+1-i)a}{2} \pmod{2m+1}.$$

Focussing on the first row in our efforts to have each activity be carried out as many times as possible (using the first row of differences in (5.1.2)), it can be seen that the differences within each block are always odd. In order to maximise the number of repeats while avoiding a repeated carryover, it is therefore necessary to have an even difference between the blocks.

In the case where $p \equiv 3 \pmod 4$, clearly m must be odd since $p = 2m+1$. It is possible to carry out each activity $\frac{p-1}{2}$ times using the Williams terrace by adding $\frac{p+1}{2}$ between blocks when $a = 1$. Note that $\frac{p+1}{2} = m+1$ will always be even in such cases.

Block 1	X	$\ldots$	$X + a(m+1)$
Block k+1	$X + 2ka(m+1)$	$\ldots$	$X + a(2k+1)(m+1)$

We require the first element from each block within a row to be different as it would then follow that since the differences are the same within each block, the elements in a particular position within each block are different. So in order to ensure that the first element in the $(k+1)$th and $(l+1)$th blocks are different, we require

$$X + 2ka(m+1) \not\equiv X + 2la(m+1) \pmod{2m+1}.$$

In other words, we don't want

$$2a(k-l)(m+1) \equiv 0 \pmod{2m+1},$$
$$\text{i.e. } (k-l)(m+1) \equiv 0 \pmod{2m+1}.$$

For $0 \leq k, l \leq \frac{p-3}{2}$, indeed for any $k, l < p$, this will not happen since $p = 2m+1$ is prime and p does not divide $k - l$ or $m + 1$.

Since entries in the same position of each of the blocks are different, a repeated carryover cannot occur at the same position in two blocks.

Since the distribution of differences is symmetric, it is also possible that a repeated carryover could occur in a different position, and so this has to be considered. This could only happen if the ith entry in the first half of a block is equal to the $(2m+1-i)$th entry in the second half of a block. In checking that we do not have any repeated carryovers, we will need to take into account whether i is odd or even (with i being the position of an element in the first block prior to adding a particular difference for the first time).

If i is even, we have a repeated carryover if

$$\begin{aligned} X + 2ka(m+1) + \tfrac{ia}{2} &\equiv X + 2la(m+1) - \tfrac{(2m-i)a}{2} \pmod{2m+1}, \\ \text{i.e. } 2a(k-l)(m+1) &\equiv -ma \pmod{2m+1}, \\ \text{i.e. } 2(k-l)(m+1) &\equiv -m \pmod{2m+1}, \\ \text{i.e. } 2(k-l)(m+1) &\equiv (m+1) \pmod{2m+1}, \\ \text{i.e. } 2(k-l) &\equiv 1 \pmod{2m+1}, \\ \text{i.e. } k-l &\equiv m+1 \pmod{2m+1}. \end{aligned}$$

This will not happen when $k, l \leq \frac{p-3}{2} = \frac{2m-2}{2} = m-1$. So we can have $m = \frac{p-1}{2}$ blocks.

In the case where i is odd, we can have a repeated carryover if

$$\begin{aligned} X + 2ka(m+1) - \tfrac{(i-1)a}{2} &\equiv X + 2la(m+1) + \tfrac{(2m+1-i)a}{2} \pmod{2m+1}, \\ \text{i.e. } 2a(k-l)(m+1) &\equiv ma \pmod{2m+1}, \\ \text{i.e. } 2(k-l)(m+1) &\equiv m \pmod{2m+1}, \\ \text{i.e. } 2(k-l)(m+1) &\equiv -(m+1) \pmod{2m+1}, \\ \text{i.e. } 2(k-l) &\equiv -1 \pmod{2m+1}, \\ \text{i.e. } k-l &\equiv m \pmod{2m+1}, \end{aligned}$$

It can be seen that this will not happen when $k, l \leq m-1$. As a result, each activity can be carried out $\frac{p-1}{2}$ times with all of the conditions being satisfied.

Example 5.2.1 When $p = 7$, each activity can be carried out three times and still satisfy the desired conditions if we add 4 between blocks in the first row:

1	2	7	3	6	4	5
2	3	1	4	7	5	6
3	4	2	5	1	6	7

Were we to continue for another block, we would get

4	5	3	6	2	7	1

and it can be seen that 45, 36 and 27 are repeated carryovers.

Example 5.2.2 When $p = 11$, each activity can be carried out five times and still satisfy the desired conditions if we add 6 between blocks in the first row:

1	2	11	3	10	4	9	5	8	6	7
2	3	1	4	11	5	10	6	9	7	8
3	4	2	5	1	6	11	7	10	8	9
4	5	3	6	2	7	1	8	11	9	10
5	6	4	7	3	8	2	9	1	10	11

Adding $\frac{p+1}{2}$ between blocks when $p \equiv 1 \pmod 4$ would not give a similar result since in such cases it would have an odd value. This would result in a repeated carryover appearing at an earlier stage.

We are going to consider the cases where $p \equiv 1 \pmod 4$ with respect to their values modulo 12. Since p is prime, we are interested in the cases where $p \equiv 1 \pmod{12}$ and $p \equiv 5 \pmod{12}$.

If $p \equiv 1 \pmod{12}$, then we shall show that adding either $\frac{p-1}{6}$ or $p - 1 - \frac{p-1}{6} = \frac{5p-5}{6}$ in between the blocks given by the Williams terrace will ensure that each activity can be carried out $\frac{p-3}{2}$ times but not $\frac{p-1}{2}$. For such primes, $\frac{p-1}{6}$ and $\frac{5p-5}{6}$ would have the even values we desire. First of all, we will consider the case where we add $\frac{p-1}{6} = \frac{m}{3}$.

Block 1	X	...	$X + a(m+1)$
Block k+1	$X + ka(m+1+\frac{m}{3})$	...	$X + ka(m+1+\frac{m}{3}) + a(m+1)$

We again require the first element in each block within a row to be different, so we need,

$$X + ka(m+1+\tfrac{m}{3}) \not\equiv X + la(m+1+\tfrac{m}{3}) \pmod{2m+1}.$$

In other words, we don't want

$$a(k-l)(m+1+\tfrac{m}{3}) \equiv 0 \pmod{2m+1},$$
$$\text{i.e. } m+1+\tfrac{m}{3} \equiv 0 \pmod{2m+1},$$
$$\text{i.e. } 3(m+1) \equiv -m \equiv m+1 \pmod{2m+1}.$$

This doesn't happen since $3 \not\equiv 1 \pmod p$.

So we will not have the same element appearing in the same position of any of the $\frac{p-3}{2}$ blocks, and so we will not have a repeated carryover appearing in the same position. Since the distribution of differences is symmetric, we again need to check that the ith entry in the first half of a block is not equal to the $(2m+1-i)$th entry in the second half of a block.

So if i is even, we have a repeated carryover if

$$X + ka(m+1+\tfrac{m}{3}) + \tfrac{ia}{2} \equiv X + la(m+1+\tfrac{m}{3}) - \tfrac{(2m-i)a}{2} \pmod{2m+1},$$
$$\text{i.e. } a(k-l)(m+1+\tfrac{m}{3}) \equiv -ma \pmod{2m+1},$$
$$\text{i.e. } (k-l)(m+1+\tfrac{m}{3}) \equiv -m \pmod{2m+1},$$
$$\text{i.e. } (k-l)(3m+3+m) \equiv -3m \pmod{2m+1},$$
$$\text{i.e. } (k-l) \equiv -3m \pmod{2m+1},$$
$$\text{i.e. } (k-l) \equiv m+2 \pmod{2m+1}.$$

It can be seen that $k-l$ will not have such a value for the first $\frac{p-3}{2}$ blocks since $0 \leq k \leq \frac{p-5}{2} = m-2$.

Now we have to consider the case where i is odd. In this case, we would have a repeated carryover if

$$X + ka(m+1+\tfrac{m}{3}) - \tfrac{(i-1)a}{2} \equiv X + la(m+1+\tfrac{m}{3}) + \tfrac{(2m+1-i)a}{2} \pmod{2m+1},$$
$$\text{i.e. } a(k-l)(m+1+\tfrac{m}{3}) \equiv ma \pmod{2m+1},$$
$$\text{i.e. } (k-l)(3m+3+m) \equiv 3m \pmod{2m+1},$$
$$\text{i.e. } k-l \equiv m-1 \pmod{2m+1}.$$

So as above, we can have $\frac{p-3}{2}$ blocks.

Example 5.2.3 When $p = 13$, each activity can be carried out five times and still satisfy the desired conditions if we add 2 between blocks in the first row:

1	2	13	3	12	4	11	5	10	6	9	7	8
10	11	9	12	8	13	7	1	6	2	5	3	4
6	7	5	8	4	9	3	10	2	11	1	12	13
2	3	1	4	13	5	12	6	11	7	10	8	9
11	12	10	13	9	1	8	2	7	3	6	4	5

The cases where we add $\frac{5p-5}{6}$ are dealt with similarly.

Example 5.2.4 This time, $p = 13$ and we add 10 between blocks in the first row:

1	2	13	3	12	4	11	5	10	6	9	7	8
5	6	4	7	3	8	2	9	1	10	13	11	12
9	10	8	11	7	12	6	13	5	1	4	2	3
13	1	12	2	11	3	10	4	9	5	8	6	7
4	5	3	6	2	7	1	8	13	9	12	10	11

If $p \equiv 5 \pmod{12}$, then adding either $\frac{p-5}{6}$ or $p - 1 - \frac{p-5}{6} = \frac{5p-1}{6}$ in between the blocks given by the Williams terrace will also give $\frac{p-3}{2}$ blocks. For such primes, $\frac{p-5}{6}$ or $\frac{5p-1}{6}$ would again have the even values we desire. First of all, we will consider the case where we add $\frac{p-5}{6} = \frac{m-2}{3}$.

Block 1	X	...	$X + a(m+1)$
Block k+1	$X + ka(m+1+\frac{m-2}{3})$	...	$X + ka(m+1+\frac{m-2}{3}) + a(m+1)$

Again, we require the first element in each block within a row to be different. So we require,

$$X + ka(m+1+\tfrac{m-2}{3}) \not\equiv X + la(m+1+\tfrac{m-2}{3}) \pmod{2m+1}.$$

In other words, we don't want

$$\begin{aligned} a(k-l)(m+1+\tfrac{m-2}{3}) &\equiv 0 \pmod{2m+1}, \\ \text{i.e. } m+1+\tfrac{m-2}{3} &\equiv 0 \pmod{2m+1}, \\ \text{i.e. } 3(m+1) \equiv -m+2 &\equiv m+3 \pmod{2m+1}, \\ \text{i.e. } 2m &\equiv 0 \pmod{2m+1}. \end{aligned}$$

We now need to check to make sure that we will not have any repeated carryovers, and again we need to take into account whether i is odd or even.

If i is even, we have a repeated carryover if

$$\begin{aligned} X + ka(m+1+\tfrac{m-2}{3}) + \tfrac{ia}{2} &\equiv X + la(m+1+\tfrac{m-2}{3}) - \tfrac{(2m-i)a}{2} \pmod{2m+1}, \\ \text{i.e. } a(k-l)(m+1+\tfrac{m-2}{3}) &\equiv -ma \pmod{2m+1}, \\ \text{i.e. } (k-l)(3m+3+m-2) &\equiv -3m \pmod{2m+1}, \\ \text{i.e. } (k-l) &\equiv 3m \pmod{2m+1}, \\ \text{i.e. } k-l &\equiv m-1 \pmod{2m+1}. \end{aligned}$$

In the case where i is odd, we can have a repeated carryover if

$$X + ka(m+1+\tfrac{m-2}{3}) - \tfrac{(i-1)a}{2} \equiv X + la(m+1+\tfrac{m-2}{3}) + \tfrac{(2m+1-i)a}{2} \pmod{2m+1},$$
$$\text{i.e. } (k-l)(m+1+\tfrac{m-2}{3}) \equiv ma \pmod{2m+1},$$
$$\text{i.e. } (k-l)(3m+3+m-2) \equiv 3m \pmod{2m+1},$$
$$\text{i.e. } (k-l) \equiv -3m \pmod{2m+1},$$
$$\text{i.e. } k-l \equiv m+2 \pmod{2m+1}.$$

So again we see that in both cases, we can have $\frac{p-3}{2}$ blocks, and the process is similar when we add $\frac{5p-1}{6}$.

Example 5.2.5 In the case where $p = 17$, adding either 2 or 14 between blocks means that each activity can be carried out seven times with all of the desired conditions being satisfied.

Thus if $p \equiv 1 \pmod 4$, the use of the Williams terrace allows fewer blocks than for $p \equiv 3 \pmod 4$. This unsatisfactory state of affairs can be overcome by using a different terrace.

5.3 Owens Terrace

Once again we wish to maximise the number of times that an activity can be carried out without repeating a carryover. Since -1 is the only element of $\mathbb{Z}_n$ which doesn't appear in the 2-sequencing, if we use it as the difference between blocks in our first row, it will not result in a repeated carryover. Again, the $n-1$ lines of differences we want are established through multiplication of the original line of differences by a ($a = 1, 2, \ldots, 2m$).

In Section 1.10, we looked at the general construction of an Owens terrace. Now we will consider what happens when we desire multiple blocks.

In general, if we are working with the Owens terrace where b is the number of blocks, $0 \le k \le b-1$, d is the difference between blocks and X is the first element of the first block, then when i is even, the ith entry in the $(k+1)$th block is

$$X + a(i-1) + k(d+2) \pmod{2m+1},$$

when $p \equiv 1 \pmod 4$ and $i \leq \frac{p-1}{2}$ or when $p \equiv 3 \pmod 4$ and $i \leq \frac{p+1}{2}$. In the cases where $p \equiv 1 \pmod 4$ and $i \geq \frac{p+3}{2}$ or $p \equiv 3 \pmod 4$ and $i \geq \frac{p+5}{2}$, the ith entry in a block (where i is even) is

$$X + ai + k(d+2) \pmod{2m+1}.$$

When i is odd, the ith entry in the $(k+1)$th block is

$$X - a(i-1) + k(d+2) \pmod{2m+1},$$

when $p \equiv 1 \pmod 4$ and $i \leq \frac{p+1}{2}$ or when $p \equiv 3 \pmod 4$ and $i \leq \frac{p-1}{2}$. In the cases where $p \equiv 1 \pmod 4$ and $i \geq \frac{p+5}{2}$ or $p \equiv 3 \pmod 4$ and $i \geq \frac{p+3}{2}$, the ith entry in a block (where i is odd) is

$$X - a(i-2) + k(d+2) \pmod{2m+1}.$$

5.4 Repeats using the Owens Terrace

Using the Owens terrace in place of the Williams terrace, we can carry out each activity $\frac{p-1}{2}$ times for both $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. In this case, a is subtracted between blocks given by the Owens terrace and since $-a$ doesn't appear in the 2-sequencing for any given row we are again able to maximise the number of blocks before repeated carryovers come into play. The fact that the Owens terrace is very close to being directed helps us when it comes to checking for repeated carryovers. Once we have checked that the same element does not occur more than once in any position within a block, we then just have to compare the elements which come before the one difference which is repeated. So we want to compare the first element of each block, with the $\frac{p+1}{2}$th element of each block. Since the 2-sequencing includes every element of $\mathbb{Z}_n$ exactly once, except that $-a$ is missing and $+a$ appears twice, it should be clear that the difference between the first and last elements in any block is $2a$, with the others cancelling each other out.

Block 1	X	...	$X+2a$
Block k+1	$X+ka$	...	$X+(k+2)a$

Here, to ensure that condition (iii) is satisfied, we require

$$X + ka \not\equiv X + la \pmod{2m+1},$$
$$\text{i.e. } (k-l)a \not\equiv 0 \pmod{2m+1},$$

and this is clearly true.

In the case where $p \equiv 1 \pmod 4$, the difference between the two elements we're interested in is $\frac{p+1}{2}a = (m+1)a$. So in order to avoid a repeated carryover, we want

$$X + ka \not\equiv X + (m+1)a + la \pmod{2m+1}.$$

In other words, we don't want

$$a(k - l - m - 1) \equiv 0 \pmod{2m+1},$$
$$\text{i.e. } k - l \equiv m + 1 \pmod{2m+1}.$$

We want $k, l < m$ and so we can have $\frac{p-1}{2}$ blocks.

Example 5.4.1 When $p = 13$, each activity can be carried out six times and still satisfy the desired conditions if we subtract 1 between blocks in the first row:

1	2	12	4	10	6	8	9	7	11	5	13	3
2	3	13	5	11	7	9	10	8	12	6	1	4
3	4	1	6	12	8	10	11	9	13	7	2	5
4	5	2	7	13	9	11	12	10	1	8	3	6
5	6	3	8	1	10	12	13	11	2	9	4	7
6	7	4	9	2	11	13	1	12	3	10	5	8

In the case where $p \equiv 3 \pmod 4$, the difference between the two elements we're interested in is $\frac{p-1}{2}a = ma$. So in order to avoid a repeated carryover, we want

$$X + ka \not\equiv X + a(l + m) \pmod{2m+1}.$$

In other words, we don't want

$$a(k - l - m) \equiv 0 \pmod{2m+1},$$
$$\text{i.e. } k - l \equiv m \pmod{2m+1}.$$

So again, we can have $\frac{p-1}{2}$ blocks.

The use of these terraces gives us a straightforward method for obtaining a schedule where each athlete can carry out particular activities a certain number of times. This method does not necessarily provide us with the maximum number of blocks, but it is an efficient way to get halfway towards the theoretical maximum number of times an activity can be repeated (or just under in some cases). In the case where $p = 7$ for example, each activity can be carried out a maximum of three times using the two terraces we've looked at in detail here. Using the Williams terrace three times and then ad hoc methods, it can be seen that it is possible to carry out each activity at least four times in such a way that our conditions are satisfied.

Example 5.4.2 Here we extend Example 5.2.1 in such a way that each activity can be carried out four times:

1	2	7	3	6	4	5
2	3	1	4	7	5	6
3	4	2	5	1	6	7
4	6	5	7	2	1	3

In this chapter, we have seen that for a prime number of activities, p, terraces can be used in such a way that $p(p-1)$ athletes can carry out the activities $\frac{p-1}{2}$ times and their schedules will satisfy the following conditions:

i. no carryover occurs twice for any athlete;

ii. in any two consecutive periods each carryover occurs exactly once;

iii. for any $j \leq n$, each athlete has different tasks in the $kn+j$th periods, $0 \leq k \leq b-1$, where b is the number of blocks.

It is currently not known if a general method exists which would allow the training schedules to be extended beyond this point and closer to the theoretical limit with regards to the number of times that each activity can be carried out by the athletes while satisfying the desired conditions. In the case where $p = 5$, we know that each activity can be carried out a maximum of three times while satisfying all of the given conditions. So the theoretical limit whereby each activity can be carried out four times is not possible in this case. It would be very interesting to know the 'best possible' result for each prime.

Appendix A

Programming Examples

Computational assistance has been of great value when it came to proving many of the results in this thesis.

A.1 Whist Tournaments

In Chapters 2 and 3 for example, having found a bound above which it could be said that a certain kind of whist tournament would always exist for the appropriate primes, it was necessary to show that such tournaments exist for the appropriate values below that bound (or for as many of them as possible). To do so, we wanted to find values which satisfied the relevant conditions in each case. It was at this stage that the Magma computational algebra system was of use. The following is an example programme of this type (for anyone familiar with Magma or the commands it makes use of), and can be used to find appropriate values of x below the bound of 3249 which was established in the proof of the existence of $\mathbb{Z}$-cyclic OTWh(p) for all primes $p \equiv 5 \pmod 8$, $p \geq 29$. The values generated by this programme are given in Section 2.3.

```
ChangeDirectory("h:");

for prime in [0..3249] do

if IsPrime(prime) then

if (prime mod 8) eq 5 then
```

```
G:=ResidueClassRing(prime);

for x in G do

criterion_1:=false; criterion_2:=false; criterion_3:=false;
criterion_4:=false; criterion_5:=false;

if IsSquare(x) then criterion_1:=true; end if;

if IsSquare(x^2 + x + 1) then criterion_2:=true; end if;

if IsSquare(x^2 - x + 1) then criterion_3:=true; end if;

if IsSquare((x^2 + x + 1)*(x^2 - x + 1)*((x^2-1)^2)) then
criterion_4:=true; end if;

if IsPower((x^2 + x + 1)*(x^2 - x + 1)*((x^2-1)^2),4) then
criterion_5:=true; end if;

if criterion_1 eq false and criterion_2 eq true and criterion_3 eq
true and criterion_4 eq true and criterion_5 eq false then
SetOutputFile("values.txt"); print "For prime:"," ",prime," , ",
x, "satisfies the conditions"; UnsetOutputFile(); break; else if x
eq (prime-1) then SetOutputFile("values.txt"); print "No such x
for prime: ", prime; UnsetOutputFile(); end if;

end if; end for; end if; end if; end for;
```

A.2 Terraces

The Magma computational algebra system was also of use in Chapter 4 when it came to the search for terraces, logarithmic terraces, exponent terraces and rejoinable terraces. The following is an example in the form of a programme which gives all of the 2-logarithmic and exponent terraces for $p = 11$ (again for anyone familiar with Magma or its commands). It is structured to look at all possible arrangements of the elements of $\mathbb{Z}_{10}$ and first of all determine whether or not each one is a terrace. If not, it moves to the next possibility. If it is a terrace, the programme then investigates whether or not the terrace is logarithmic (in this case 2-logarithmic). If it is, the terrace is printed out along with the corresponding exponent terrace. This programme can be used to obtain a list of all 1,184 2-logarithmic and exponent terraces for $p = 11$, whose existence was mentioned in Section 4.3.

```
ChangeDirectory("h:");

p:=11; z:=2; gr:=0;

for i in [1..10] do for j in [1..9] do for k in [1..8] do for l in
[1..7] do for m in [1..6] do for n in [1..5] do for ij in [1..4]
do for jk in [1..3] do for kl in [1..2] do for lm in [1..1] do

gg:=[1,2,3,4,5,6,7,8,9,10];

b:=gg[i]; c:=Exclude(gg,b); d:=c[j]; e:=Exclude(c,d); f:=e[k];
g:=Exclude(e,f); h:=g[l]; pp:=Exclude(g,h); q:=pp[m];
r:=Exclude(pp,q); s:=r[n]; mn:=Exclude(r,s); no:=mn[ij];
cg:=Exclude(mn,no); pq:=cg[jk]; rs:=Exclude(cg,pq); st:=rs[kl];
uv:=Exclude(rs,st); vw:=uv[lm];

a:=[b,d,f,h,q,s,no,pq,st,vw];

aa:=[(a[cd+1]-a[cd]) mod (p-1):cd in [1..(p-2)]];

aaa:=SequenceToMultiset(aa);

xy:=0; for de in [1..(p-2)] do if 2*aa[de] mod (p-1) eq 0 and
Multiplicity(aaa,aa[de]) eq 1 or 2*aa[de] mod (p-1) ne 0 and
Multiplicity(aaa,aa[de]) + Multiplicity(aaa,-aa[de] mod (p-1)) eq
2 then xy:=xy+1; end if; end for; if xy eq (p-2) then dd:=[z^a[cc]
```

```
mod p:cc in[1..(p-1)]];

ddd:=[(dd[ef+1]-dd[ef]) mod (p-1):ef in [1..(p-2)]];
dddd:=SequenceToMultiset(ddd); yz:=0; for fm in [1..(p-2)] do if
2*ddd[fm] mod (p-1) eq 0 and Multiplicity(dddd,ddd[fm]) eq 1 or
2*ddd[fm] mod (p-1) ne 0 and Multiplicity(dddd,ddd[fm]) +
Multiplicity(dddd,-ddd[fm] mod (p-1)) eq 2 then yz:=yz+1; end if;
end for; if yz eq (p-2) then gr:=gr+1; SetOutputFile("p=11, pr=2,
log,exp terraces.txt"); print "log",gr,"=",a,"exp",gr,"=",dd;
UnsetOutputFile(); end if; end if;

end for; end for; end for; end for; end for; end for; end for; end
for; end for; end for;
```

Bibliography

[1] R. J. R. Abel, S. Costa, and N. J. Finizio. Directed-ordered whist tournaments and $(v, 5, 1)$ existence families - existence results and some new classes of $\mathbb{Z}$-cyclic solutions. Discrete Appl. Math. 143 (2004), 43-53.

[2] R. J. R. Abel, N. J. Finizio, M. Greig, and S. J. Lewis. $(2, 6)$ $GWhD(v)$ - Existence results and some $\mathbb{Z}$-cyclic solutions. Congr. Numer. 144 (2000), 5-39.

[3] R. J. R. Abel, N. J. Finizio, M. Greig, and S. J. Lewis. Generalized whist tournament designs. Discrete Math. 268 (2003), 1-19.

[4] I. Anderson. A hundred years of whist tournaments. J. Combin. Math. Combin. Comput. 19 (1995), 129-150.

[5] I. Anderson. Combinatorial Designs and Tournaments. Oxford Science Publications, Clarendon Press, Oxford, 1997.

[6] I. Anderson, S. D. Cohen, and N. J. Finizio. An existence theorem for cyclic triplewhist tournaments. Discrete Math. 138 (1995), 31-41.

[7] I. Anderson and L. H. M. Ellison. $\mathbb{Z}$-cyclic ordered triplewhist tournaments on p elements, where $p \equiv 5 \pmod 8$. Discrete Math. 293 (2005a), 11-17.

[8] I. Anderson and L. H. M. Ellison. $\mathbb{Z}$-cyclic ordered triplewhist and directed triplewhist tournaments on p elements, where $p \equiv 9 \pmod{16}$ is prime. J. Combin. Math. Combin. Comput. 53 (2005b), 39-48.

[9] I. Anderson and L. H. M. Ellison. $\mathbb{Z}$-cyclic directed moore $(2, 6)$ generalised whist tournament designs on p elements, where $p \equiv 7 \pmod{12}$. Ars Combin., to appear.

[10] I. Anderson and C. Ferguson. Carryover Designs For Fitness Training Including Rugby Training Schedules. University of Glasgow, Department of Mathematics Preprint Series (2002).

[11] I. Anderson and C. Ferguson. Training Schedules Balanced for Carryover Effects Bulletin of the ICA 40 (2004), 5-12.

[12] I. Anderson and N. J. Finizio. Triplewhist tournaments that are also Mendelsohn designs. J. Combin. Des. 5 (1997), 397-406.

[13] I. Anderson and N. J. Finizio. On the construction of directed triplewhist tournaments. J. Combin. Math. Combin. Comput. 35 (2000), 107-115.

[14] I. Anderson, N. J. Finizio and P. A. Leonard. New product theorems for $\mathbb{Z}$-cyclic whist tournaments. J. Combin. Theory Ser. A 88 (1999), 162-166.

[15] I. Anderson and D. A. Preece. Locally balanced change-over designs. Utilitas Math. 62 (2002), 33-59.

[16] I. Anderson and D. A. Preece. Logarithmic terraces. Bull. ICA, to appear.

[17] R. A. Bailey. Quasi-complete Latin squares: construction and randomisation. J. Roy. Statist. Soc. Ser. B 19 (1984), 323-334.

[18] M. Buratti. Existence of $\mathbb{Z}$-cyclic triplewhist tournaments for a prime number of players. J. Combin. Theory Ser. A 90 (2000), 315-325.

[19] N. J. Finizio. Orbits of cyclic Wh(v) of $\mathbb{Z}_N$-type. Congr. Numer. 82 (1991), 15-28.

[20] N. J. Finizio and J. T. Lewis. A criterion for cyclic whist tournaments with the three person property. Utilitas Math. 52 (1997), 129-140.

[21] N. J. Finizio and S. J. Lewis. Some specializations of pitch tournament designs. Utilitas Math. 56 (1999), 33-52.

[22] R. F. Foster. Duplicate Whist. Brentano's, N.Y., 1894.

[23] G. Ge and C. W. H. Lam. Whist tournaments with the three person property. Discrete Appl. Math. 138 (2004), 265-276.

[24] H. -D. O. F. Gronau and R. C. Mullin. On super-simple 2-$(v, 4, \lambda)$ designs. J. Combin. Math. Combin. Comput. 11 (1992), 113-121.

[25] W. J. LeVeque. Topics in Number Theory, Volume 1 (Addison-Wesley, 1956).

[26] Y. S. Liaw. Some constructions of combinatorial designs. PhD Thesis, University of Glasgow, 1994.

[27] Y. S. Liaw. Construction of $\mathbb{Z}$-cyclic triplewhist tournaments. J. Combin. Des. 4 (1996), 219-233.

[28] R. Lidl and H. Niederreiter. 'Finite Fields.' Encyclopaedia of Mathematics Volume 20. Cambridge University Press, Cambridge, UK, 1983.

[29] Y. Lu and Z. Shengyuan. Existence of whist tournaments with the three-person property $3PWH(v)$. Discrete Appl. Math. 101 (2000), 207-219.

[30] J. T. Mitchell. Duplicate Whist. McClurg, Chicago, 1891; second edition 1897.

[31] E. H. Moore. Tactical memoranda I-III. Amer. J. Math. 18 (1896), 264-303.

[32] P. Prescott. Construction of sequentially counterbalanced designs formed from two Latin squares. Utilitas Math. 55 (1999), 135-152.

[33] P. Prescott. Construction of uniform-balanced cross-over designs for any odd number of treatments. Statistics in Medicine 18 (1999), 265-272.

[34] E. J. Williams. Experimental designs balanced for the estimation of residual effects of treatments. Australian Journal of Scientific Research Ser. A 2 (1949), 149-168.

[35] R. M. Wilson. An existence theory for pairwise balanced designs III. J. Combin. Theory Ser. A 18 (1975), 71-79.