FINITE LEFT NEOFIELDS AND THEIR USE AS A UNIFYING PRINCIPLE IN CONSTRUCTIONS FOR ORTHOGONAL LATIN SQUARES

A thesis submitted for the degree of Doctor of Philosophy

September 1991

David Bedford
Department of Mathematical and Computing Sciences
University of Surrey
Abstract

One of the outstanding problems in the study of latin squares is that of improving the known lower bounds for \( N(n) \), the maximum number of latin squares of order \( n \) in a mutually orthogonal set. After describing the methods of construction which attain the best known lower bounds for \( N(n) \), \( n \leq 32 \) and showing how most of these are interrelated we provide a general method of construction for sets of mutually orthogonal latin squares (m.o.l.s.) from left neofields. We then give detailed information about the structure of all isomorphically distinct left neofields of order less than ten and about the m.o.l.s. which they produce, and summarised information for orders up to fourteen. We further show that many of the previously known constructions of m.o.l.s. effectively employ the construction which we describe, in particular the recent constructions of three m.o.l.s. of order fourteen and four of order twenty.

In the course of this investigation it is noted that the number of complete mappings of both of the non-cyclic abelian groups of order eight is the same. Furthermore, it is found that both of the non-abelian groups of order eight possess the same number of complete and near complete mappings. We explain and justify why this is the case.

In our study of left neofields we discuss the properties of sequenceability and R-sequenceability of groups. At the end of the thesis, we discuss a related question, raised by R. L. Graham, as to which groups are \( r \)-set-sequenceable. This is solved for abelian groups except that, for \( r = n - 1 \), the question is reduced to that of asking which abelian groups are R-sequenceable.
Acknowledgements

First and foremost I am deeply indebted to my supervisor Dr. A. D. Keedwell. As an undergraduate my interest in mathematics was first stimulated by Dr. Keedwell’s lectures and he has since proved to be an invaluable source of advice and encouragement both in guiding my research and during the writing of this thesis.

Secondly, I acknowledge the Science and Engineering Research Council for their financial support during the first two years of my research.

Thirdly, I wish to thank my colleagues in the Department of Mathematics at the University of Essex for their support during the final year of my research.

Finally, I thank my wife Ceri for her patience and encouragement over the past three years and my daughter Siân without whom this thesis would have been written earlier but with whom life has been much more fun.
## Contents

**Chapter 1  Basic Definitions**  page 1

1.0.  Introduction  1

1.1.  Latin squares  3

1.2.  Orthogonal latin squares  8

1.3.  Complete and near complete mappings of groups  11

**Chapter 2  Applications of Orthogonal Latin Squares**  16

2.0.  Introduction  16

2.1.  Euler's 36 officers problem  16

2.2.  Orthogonal latin squares as experimental designs  18

2.3.  Finite projective planes  19

2.4.  Construction of error detecting and correcting codes  22

2.5.  Orthogonal latin square graphs  23

**Chapter 3  Indirect Construction of M.O.L.S.**  26

3.0.  Introduction  26

3.1.  Direct product of quasigroups  26

3.2.  Parker's method  27

3.3.  Yamamoto's generating principle  29

3.4.  Yamamoto's method  32
3.5. Hedayat and Seiden’s method 42
3.6. Wang’s method 44

Chapter 4 Direct Constructions of M.O.L.S. From Groups 49
4.0. Introduction 49
4.1. Mann’s automorphism method 49
4.2. The orthomorphism method 52

Chapter 5 Finite Left Neofields 57
5.0. Introduction 57
5.1. Basic definitions 57
5.2. Generalised orthomorphisms, near orthomorphisms and left neofields 58
5.3. Isomorphisms of left neofields 65
5.4. Some properties of left neofields which are preserved under isomorphism 68
5.5. Main classes of addition tables 71

Chapter 6 Construction of M.O.L.S. Using Left Neofields 74
6.0. Introduction 74
6.1. Left neofields with orthogonal addition tables 74
6.2. Results 82
6.3. Observations 90
Chapter 1 Basic Definitions

1.0. Introduction

One of the outstanding problems in the study of latin squares is that of improving the known lower bounds for $N(n)$, the maximum number of latin squares of order $n$ in a mutually orthogonal set. The main purpose of this thesis is to describe the constructions used in obtaining the best known lower bounds for $N(n)$, $n \leq 32$ and to show that many of these constructions are closely related. In particular, constructions which attain the best known lower bounds for $N(n)$ for many of these orders are interpreted in terms of a new construction which involves the concept of a left neofield (an algebraic structure which is a generalisation of a finite field).

When there do not exist orthogonal latin squares for a particular order $n$ we will find it convenient to write $N(n) = 1$. Below is a list of the best known lower bounds of $N(n)$ for $n \leq 32$. [For the cases $n = 6$ and $p'$, $p$ prime, the bounds are known to hold with equality.]

<table>
<thead>
<tr>
<th>$n$</th>
<th>$N(n)$</th>
<th>$n$</th>
<th>$N(n)$</th>
<th>$n$</th>
<th>$N(n)$</th>
<th>$n$</th>
<th>$N(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\infty$</td>
<td>9</td>
<td>8</td>
<td>17</td>
<td>16</td>
<td>25</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>10</td>
<td>2</td>
<td>18</td>
<td>3</td>
<td>26</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>11</td>
<td>10</td>
<td>19</td>
<td>18</td>
<td>27</td>
<td>26</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>12</td>
<td>5</td>
<td>20</td>
<td>4</td>
<td>28</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>13</td>
<td>12</td>
<td>21</td>
<td>4</td>
<td>29</td>
<td>28</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>14</td>
<td>3</td>
<td>22</td>
<td>3</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>15</td>
<td>4</td>
<td>23</td>
<td>22</td>
<td>31</td>
<td>30</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>16</td>
<td>15</td>
<td>24</td>
<td>4</td>
<td>32</td>
<td>31</td>
</tr>
</tbody>
</table>

In the introduction to each Chapter we state which of the above bounds can be attained using constructions described in the chapter.

In Chapter 2 we give a brief overview of some of the numerous applications of m.o.l.s. in areas such as experimental design, projective geometry, coding theory...
and graph theory.

In Chapter 3 we describe several known constructions for sets of m.o.l.s. which all involve combining m.o.l.s. of smaller order together in some way. We then show that most of these so called indirect constructions can be treated as special cases of a generating principle for latin squares which was first introduced by Yamamoto.

In Chapter 4 we discuss how the Cayley tables of groups have been used to construct sets of m.o.l.s. directly.

In Chapter 5 we define the concept of a left neofield, present necessary and sufficient conditions for two left neofields to be isomorphic and prove that the number of distinct isomorphs of a left neofield based on a particular group \((G, \cdot)\) divides the order of aut \((G, \cdot)\). We also show how the addition table of a left neofield is affected by the main class transformations and in what sense these transformations preserve left neofield structure.

In Chapter 6 we give sufficient conditions for the addition tables of two left neofields to form a pair of orthogonal latin squares. In particular, we give sufficient conditions for the addition table of a left neofield to be orthogonal to a latin square formed by a certain rearrangement of its own rows and we also give sufficient conditions for the addition table of a left neofield to be self-orthogonal. Detailed information for all isomorphically distinct left neofields of order less than ten is presented along with extensive results concerning the orthogonality of addition tables. Examples of the largest sets of m.o.l.s. formed by the addition tables of left neofields based on all groups up to order eleven are presented (excluding those which may be obtained from the Desarguesian plane) as well as the total numbers of orthomorphisms and near orthomorphisms possessed by these groups. Motivated by observations made on these results, sufficient conditions for all isomorphs of a left neofield to coincide are given. We also note that the total
numbers of complete and near complete mappings of the pairs of groups $C_2 \times C_4$, $C_2 \times C_2 \times C_2$ and $O_4$, $D_4$ of order eight are equal. [In Chapter 9 we give a theoretical proof of why this is necessarily the case.]

In Chapter 7 we discuss how previously known results concerning property D neofields can be expressed in terms of left neofield theory. Some of these known results for property D neofields are then generalised to arbitrary left neofields.

In Chapter 8 we show how several recent constructions for m.o.l.s. effectively employ the use of a particular type of left neofield. Most notably the results $N(14) \geq 3$, $N(20) \geq 4$ and all known constructions for self-orthogonal latin squares of order ten have been obtained in this way.

Discussions of the sequenceability and R-sequenceability of groups in Chapter 5 lead us to consider a related question which was first raised by R. L. Graham. This question is almost completely solved for the case of abelian groups in Chapter 9. Only a question, which is equivalent to asking which abelian groups are R-sequenceable, remains unanswered.

In Chapter 10 we assess to what extent we have been successful in our attempt to show that many of the previously known constructions for m.o.l.s. are closely related.

1.1. Latin squares

**Definition 1.1.** A *Latin square* of order $n$ is an $n \times n$ array defined on a symbol set $S$ of size $n$ such that each member of $S$ occurs exactly once in each row and once in each column.
Example:

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

fig. 1.1.

We will often use \( S_1 = (1, 2, \ldots, n) \) or \( S_2 = (0, 1, \ldots, n-1) \) as our symbol set and say that a latin square is in standard form if the elements of its topmost row and left most column are in natural order. [Note that if the symbol set is \( S_2 \) we will often refer to the topmost row and left most column of a latin square as its zeroth row and zeroth column respectively.]

As we shall show in Theorem 1.1, the Cayley table of a group is always a latin square, the converse however is false. [In fact fig. 1.1 displays the smallest latin square which cannot be obtained as the Cayley table of a group.] It is still useful to consider a latin square as being the 'multiplication table' of some algebraic structure.

**Definition 1.2.** A quasigroup \((Q, \cdot)\) is a set \( Q \) and a binary operation \((\cdot)\) defined on \( Q \) such that, for any two elements \( a, b \in Q \), the equations \( a \cdot x = b \) and \( y \cdot a = b \) each have exactly one solution.

A quasigroup with an identity element is called a loop; an associative loop is simply a group. We will refer to the multiplication table of a quasigroup as its Cayley table.

**Theorem 1.1.** An \( n \times n \) array defined on a symbol set \( S \) is a latin square if and only if it forms the Cayley table of some quasigroup \((S, \cdot)\).

**Proof.** Let \( L \) be a latin square of order \( n \) defined on \( S \). We use \( L \) to define a
binary operation (\cdot) on S as follows. Firstly, we index the rows and columns of L using the elements of S (e.g. we could use the elements as they occur in the topmost row and left most column of L). Secondly, for any pair of elements \( x, y \) of S we define \( x \cdot y = z \), where \( z \) is the element of S which occurs in the \((x, y)\)th cell of L. Then \((S, \cdot)\) so formed is a quasigroup. To see this, let \( a, b \in S \), then the element \( b \) occurs exactly once in the \(a\)th row and once in the \(a\)th column of L, since L is a latin square. Thus the equations \( a \cdot x = b \) and \( y \cdot a = b \) each have a unique solution where \( x \in S \) is such that b occurs in the \((a, x)\)th cell of L and \( y \in S \) is such that b occurs in the \((y, a)\)th cell of L.

Conversely, let \((S, \cdot)\) be a quasigroup, then the Cayley table \( M \) of \((S, \cdot)\) forms a latin square. To see this, suppose that the element \( b \) occurs twice in any one row of \( M \). Then there exists an element \( a \) of S (namely the element which borders the row in question) such that the equation \( a \cdot x = b \) has two solutions. Thus no element of S occurs twice in any row of \( M \). Similarly for columns we have that if the element \( b \) of S occurs twice in any column of \( M \), then there exists \( a \in S \) such that the equation \( y \cdot a = b \) has two solutions. Thus each element of S occurs not more than once in each row and once in each column of \( M \) and, since \( M \) is an \(|S| \times |S| \) array, it must therefore be a latin square. \( \square \)

That the Cayley table of a group forms a latin square is a direct consequence of the above theorem and the fact that a group is a special type of quasigroup. That the latin square displayed in fig. 1.1 does not form the Cayley table of a group may be observed as follows. If we border the latin square of fig. 1.1 using the elements of its topmost and left most column, so as to define a binary operation (\cdot), then we obtain the following Cayley table of a loop.
Notice that we have $2 \cdot (3\cdot 4) = 4$ whereas $(2\cdot 3)\cdot 4 = 2$ and so the binary operation as defined is not associative. Clearly, if we permute the borders of the above square in any way then the resulting binary operation will still not be associative. Thus, the latin square of fig. 1.1 cannot be bordered so as to obtain the Cayley table of a group.

The Cayley table displayed in fig. 1.2 has the interesting property that its leading diagonal consists entirely of ones. We can also construct Cayley tables in which the leading diagonal consists of the elements in natural order. The corresponding quasigroups are given special names and these names are carried over to the latin squares formed by their Cayley tables.

**Definition 1.2.** A quasigroup $(Q, \cdot)$ is **unipotent** if $a \cdot a = b \cdot b$ for all $a, b \in S$.

**Definition 1.3.** A quasigroup $(Q, \cdot)$ is **idempotent** if $a \cdot a = a$ for all $a \in S$.

The latin square in fig. 1.2, for example, is unipotent.

Clearly, for any given latin square $L$, defined on a symbol set $S$, we can form further latin squares, defined on $S$, by simply rearranging the rows or columns of $L$ or by permuting the symbols in $L$. We will want to consider these latin squares as being essentially the same. The following concept will prove useful in this regard.

**Definition 1.4.** An orthogonal array $OA(n, r)$ of order $n$ and depth $r$ is an $r \times n^2$ matrix $M$ having $n$ different elements and with the property that each different
ordered pair of elements occurs exactly once as a column in any two rowed submatrix of \( M \).

Theorem 1.2. A latin square of order \( n \) both defines and is defined by an \( OA(n, 3) \).

Proof. Let \( L \) be a latin square of order \( n \) and define a \( 3 \times n^2 \) matrix \( M \) as follows. If \( k \) occurs in the \((i, j)\)th cell of \( L \), then \((i, j, k)\) is a column of \( L \). Since \( L \) has \( n^2 \) cells \( M \) is indeed a \( 3 \times n^2 \) matrix with entries from a symbol set of size \( n \). Clearly, each possible ordered pair \((i, j')\) occurs once in the two rowed submatrix formed by the first and second rows of \( M \) since these ordered pairs correspond to the cells of \( L \). Moreover, if the ordered pair \((i, k)\) or \((j, k)\) occurred twice in the two rowed submatrix formed by the first and third or the second and third rows of \( M \) respectively, then this would imply that the element \( k \) occurred twice in the \( i \)th row or \( j \)th column of \( L \) respectively, which contradicts the fact that \( L \) forms a latin square.

Conversely, given an \( OA(n, 3) \) we can construct an \( n \times n \) array \( L \) by placing \( k \) in the \((i, j)\)th cell of \( L \) if and only if \((i, j, k)\) is a column of the \( OA(n, 3) \). Using the definition of an \( OA(n, 3) \) we can easily see that each cell will only contain one element and each of the \( n \) elements will occur not more than once in each row and once in each column of \( L \), hence \( L \) is a latin square. \( \square \)

As in the proof of the above theorem, we will find it convenient to think of an \( OA(n, 3) \) as defining a latin square of order \( n \) in which the first two rows of the \( OA(n, 3) \) index the rows and columns of \( L \) respectively and the third row determines the corresponding cell entry. Now from any given \( OA(n, 3) \) we can see how to obtain further \( OA(n, 3) \)'s which may be considered to be in some way the same. Firstly we may apply an ordered triple \((\alpha, \beta, \gamma)\) of permutations to the symbols in the rows of the \( OA(n, 3) \). In terms of the corresponding latin square \( L \), the permutation \( \alpha \) results in a permutation of the rows of \( L \), whilst \( \beta \) permutes the columns and \( \gamma \) permutes the symbols. The ordered triple \((\alpha, \beta, \gamma)\) is called an
isotopism of $L$. The set of all latin squares which can be obtained from $L$ by such isotopisms is called the isotopism class of $L$. Clearly isotopism forms an equivalence relation on the set of latin squares and so we may say that two latin squares are isotopic if they belong to the same isotopism class.

There is another way of obtaining further $OA(n, 3)$'s from any given one and that is by permuting its rows in any one of the five possible (non-identity) ways. Transposing the first two rows will result in a latin square which is the transpose (in the matrix sense) of $L$. Transposing, say, the first and third rows amounts to interchanging the roles of rows and symbols in $L$ etc. The latin squares formed in this way are called adjugates or parastrophes. An isotopism class together with the parastrophes of all its members is called a main class.

1.2. Orthogonal latin squares

The following concept is of great importance in the study of latin squares.

**Definition 1.5.** Two latin squares of order $n$ are orthogonal if, when they are juxtaposed so as to form an array of ordered pairs $A$, each of the $n^2$ possible ordered pairs occurs in $A$ exactly once.

We say that two quasigroups $(G, \cdot)$ and $(G, \ast)$ are orthogonal if, for all $a, b \in G$, the pair of simultaneous equations $x \cdot y = a$ and $x \ast y = b$, has a unique solution in $G$. If two quasigroups are orthogonal, then their Cayley tables form a pair of orthogonal latin squares. In general, a set of $k$ latin squares, $A_1, A_2, \ldots, A_k$, is said to form a set of mutually orthogonal latin squares (m.o.l.s.) if the latin squares $A_i$ and $A_j$ are orthogonal whenever $i \neq j$. Such a set of $k$ m.o.l.s. is equivalent to the existence of an $OA(n, k+2)$, where $(i, j, x_1, x_2, \ldots, x_k)'$ is a column of the $OA(n, k+2)$ if and only if $x_i$ is the element in the $(i, j)$th cell of $A_i$. That this is indeed an orthogonal array follows on observing that, in the two rowed submatrix formed by any pair of its final $k$ rows, each possible ordered pair will
occur exactly once in virtue of the fact that the corresponding Latin squares are orthogonal.

A set of m.o.l.s. of order \( n \) can have at most \( n-1 \) members. To see this let \( (A_1, A_2, \ldots, A_k) \) be a set of m.o.l.s. of order \( n \) and, without loss of generality, let each be defined on \( S = \{1, 2, \ldots, n\} \). We can permute \( S \) in \( A_i \) without affecting either the fact that \( A_i \) forms a Latin square or its orthogonality to the other members of the set. For each \( A_i \) permute \( S \) so that the topmost row of \( A_i \) is in natural order. Now for the entry in the second row and first column of \( A_i \) (its \((2, 1)\)th entry) there must be an element from the \((n-1)\)-set \( S\setminus\{1\} \). Furthermore, the \((2, 1)\)th entries for \( A_i \) \( 1 \leq i \leq k \), must all be different, since, when we juxtapose \( A_i \) and \( A_j \), \( i \neq j \), all the ordered pairs of the form \((m, m)\), \( m \in S \), occur in the topmost row. It follows that \( k \leq n-1 \). A set of m.o.l.s. which has \( n-1 \) members is called a complete set (fig. 1.3 displays a complete set of m.o.l.s. of order four).

\[
\begin{array}{ccc}
0 & 1 & 2 & 3 \\
1 & 0 & 3 & 2 \\
2 & 3 & 0 & 1 \\
3 & 2 & 1 & 0 \\
\end{array}
\quad
\begin{array}{ccc}
0 & 1 & 2 & 3 \\
2 & 3 & 0 & 1 \\
3 & 2 & 1 & 0 \\
1 & 0 & 3 & 2 \\
\end{array}
\quad
\begin{array}{ccc}
0 & 1 & 2 & 3 \\
3 & 2 & 1 & 0 \\
1 & 0 & 3 & 2 \\
2 & 3 & 0 & 1 \\
\end{array}
\]

\[L_1 \quad \quad L_2 \quad \quad L_3\]

fig. 1.3

We notice that \( L_2 \) and \( L_3 \) have the special property that they are each orthogonal to the Latin square formed by their own transpose. A Latin square with this property is called self-orthogonal.

Many of the properties usually associated with the study of groups may be utilised in the study of quasigroups. For example, the concept of the direct product of two groups can easily be extended to that of two quasigroups. Formally we have:

**Definition 1.6.** Let \((G, \cdot)\) and \((H, \times)\) be quasigroups and define the operation \((\circ)\) on \( F = G \times H \) by \((x_1, y_1) \circ (x_2, y_2) = (x_1 \cdot x_2, y_1 \times y_2)\). Then \((F, \circ)\) is the direct product of \((G, \cdot)\) with \((H, \times)\).
In terms of their corresponding latin squares $L_1$ and $L_2$ we may interpret the direct product of two quasigroups as follows:

$$L_1 \times L_2 = \begin{array}{ccc}
L_1(1, 1) & L_1(1, 2) & \ldots & L_1(1, n) \\
L_1(2, 1) & L_1(2, 2) & \ldots & L_1(2, n) \\
\vdots & \vdots & \ddots & \vdots \\
L_1(n, 1) & L_1(n, 2) & \ldots & L_1(n, n)
\end{array}$$

where $L_1(i, j)$ is the latin square $L_1$ with each entry $x$ replaced by $(x, y^i_j)$, where $y^i_j$ is the entry in the $(i, j)$th cell of $L_2$.

We can then obtain the following well known result.

**Theorem 1.3.** Let $(G, \cdot)$ and $(G, \odot)$, $(H, \times)$ and $(H, \otimes)$ be pairs of orthogonal quasigroups and let $(F, \circ)$ and $(F, *)$ be the direct products of $(G, \cdot)$ with $(H, \times)$ and of $(G, \odot)$ with $(H, \otimes)$ respectively. Then $(F, \circ)$ and $(F, *)$ are orthogonal quasigroups.

**Proof.** We first show that the direct product of two quasigroups, is itself a quasigroup. Without loss of generality we may consider $(F, \circ)$. We are required to show that for any pair of elements $(x_1, y_1), (x_2, y_2)$ of $F$, the equations $(x_1, y_1) \circ (x, y) = (x_2, y_2)$ and $(x, y) \circ (x_1, y_1) = (x_2, y_2)$ are each uniquely soluble for $(x, y)$ in $F$. Now $(x_1, y_1) \circ (x, y) = (x_2, y_2)$ if and only if $x_1 \cdot x = x_2$ in $G$ and $y_1 \times y = y_2$ in $H$. But, since $(G, \cdot)$ and $(H, \times)$ are quasigroups, these equations are each uniquely soluble and so $(x, y)$ is unique and in $F$. The proof that $(x, y) \circ (x_1, y_1) = (x_2, y_2)$ is uniquely soluble for $(x, y)$ in $F$ is similar.

To show the orthogonality of $(F, \circ)$ and $(F, *)$ we are required to show that, for all $(x_1, y_1), (x_2, y_2) \in F$, the pair of simultaneous equations $(x_1, y_1) \circ (x_2, y_2) = (x_3, y_3)$ and $(x_1, y_1) * (x_2, y_2) = (x_4, y_4)$ has a unique solution in $F$. But these equations together imply the pair of equations $x_1 \cdot x_2 = x_3$ and $x_1 \otimes x_2 = x_4$ which has a unique solution in $G$ in virtue of the fact that $(G, \cdot)$ and $(G, \odot)$ are
orthogonal quasigroups. Similarly the pair of equations $y_1 \otimes y_2 = y_a$ and $y_1 \otimes y_2 = y_b$ has a unique solution in $H$. The result now follows. □

1.3. Complete and near complete mappings of groups

Consider a pair of orthogonal latin squares, for example $L_1$ and $L_2$ in fig 1.3, and imagine them to be juxtaposed so as to form an array of ordered pairs $A$. Then the ordered pairs of the form $(x,0)$ say, will have the property that the elements $x$ occur once in each row and once in each column of $L_1$ with each of the possible symbols occurring once. This observation leads us to make the following definition.

**Definition 1.7.** A transversal of a latin square of order $n$ is a set of $n$ cells, one in each row, one in each column, such that no two of the cells contain the same symbol.

It should be clear, by the remarks preceding the above definition, that a latin square will possess an orthogonal mate if and only if it can be decomposed into $n$ non-overlapping transversals (such transversals are said to be disjoint). It might now be asked: if the Cayley table of a quasigroup has a transversal, what if anything, may be said about the quasigroup? Before we answer this question we make the following definition.

**Definition 1.8.** A complete mapping of a quasigroup $(Q, \cdot)$ is a permutation $x \rightarrow \theta(x)$ of $Q$ such that the mapping $x \rightarrow \phi(x)$ defined by $\phi(x) = x \cdot \theta(x)$ is again a permutation of $Q$.

Complete mappings were first introduced by Mann in [38]. Johnson, Dulmage and Mendelsohn [30] have called the mapping $\phi$ an orthomorphism when $(Q, \cdot)$ is a group. We will use either terminology as it suits us. A complete mapping of a group for which $\theta(1) = 1$ is said to be in canonical form (we will also say that the corresponding orthomorphism $\phi$ is in canonical form).
Theorem 1.4. If \((Q, \cdot)\) is a quasigroup which possesses a complete mapping, then its Cayley table is a latin square with a transversal. Conversely, if \(L\) is a latin square which possesses a transversal, then any quasigroup which has \(L\) as its Cayley table has a complete mapping.

Proof. Suppose that \((Q, \cdot)\) has a complete mapping \(\theta\), let \(\phi(x) = x \cdot \theta(x)\) and consider the set of cells \(T = \{(x, \theta(x)): x \in Q\}\). Clearly \(T\) contains one cell from each row and one cell from each column of the Cayley table of \((Q, \cdot)\) (the latter follows since \(\theta\) is a permutation of \(Q\)). Moreover the entries in the cells of \(T\) are the elements \(\phi(x)\) which exhaust the set \(Q\) since \(\phi\) is a permutation of \(Q\). Hence \(T\) is a transversal of the Cayley table of \((Q, \cdot)\).

Conversely, if \(L\) is a latin square, defined on \(Q = \{q_1, q_2, \ldots, q_n\}\), which possesses a transversal comprising the set of cells \((1, a_1), (2, a_2), \ldots, (n, a_n)\), where the element \(b_i\) occupies the cell \((i, a_i)\), then we may border \(L\) with the symbols of \(Q\) (in any order) so as to form a quasigroup \((Q, \cdot)\) which has \(L\) as its Cayley table and for which \(q_1 q_n = b_1\). Thus \((Q, \cdot)\) has a complete mapping \(\theta\), where \(\theta(q_1) = q_n\). \(\Box\)

Before we move on to discuss which types of groups possess complete mappings we define a generalisation of this concept. Since this generalised concept has only been studied in connection with groups we shall assume that this is the case in what follows.

Definition 1.9. A near complete mapping of a group \((G, \cdot)\) is a mapping \(\theta\) from \(G \setminus h_2\) onto \(G \setminus h_1\) such that \(\phi\), defined by \(\phi(x) = x \cdot \theta(x)\), is again a mapping from \(G \setminus h_2\) onto \(G \setminus h_1\).

Hsu [26] has called the mapping \(\phi\) a near orthomorphism of the group. If \(h_1 = 1\), then we say that the near complete mapping (or near orthomorphism) is in canonical form and the element \(h_2\) is then called the exdomain element of the mapping (usually denoted by \(\eta\)). Notice that a canonical form near complete
mapping \( \theta \) for which \( \eta = 1 \) is also a canonical form complete mapping of the group when extended by the requirement that \( \theta(1) = 1 \).

Just as a complete mapping of a group \( (G, \cdot) \) defines a transversal in the Cayley table of \( (G, \cdot) \), so a near complete mapping of \( (G, \cdot) \) defines a set of \( (n-1) \) cells in the Cayley table of \( (G, \cdot) \) such that no two cells contain the same element, nor do they occur in the same row or column. Johnson [29] has called such a collection of cells an almost transversal of the Cayley table of \( (G, \cdot) \).

**Theorem 1.5.** A complete (or near complete) mapping of a group \( (G, \cdot) \) of order \( n \), in canonical form, defines \( n \) distinct complete (or near complete) mappings of \( (G, \cdot) \) and to every complete (or near complete) mapping of \( (G, \cdot) \) there corresponds a complete (or near complete) mapping of \( (G, \cdot) \) in canonical form which is unique.

**Proof.** Let \( \theta \) be a complete (or near complete) mapping of \( (G, \cdot) \), in canonical form, then \( \theta_p \) where \( \theta_p(g) = \theta(g).\theta_p \) is a complete (or near complete) mapping of \( (G, \cdot) \) \( \forall \ g \in G \). Furthermore, \( \theta_i = \theta_j \Leftrightarrow g_i = g_j \). Note that if \( g_1 = 1 \), then \( \theta_1 = \theta \).

Conversely, for any given complete mapping \( \theta' \) of \( (G, \cdot) \) in which \( \theta'(1) = g_k \) we can construct the unique complete mapping \( \theta \) such that \( \theta(g) = \theta'(g).\theta_k^{-1} \), which is in canonical form. Similarly, for any given near complete mapping \( \theta \) in which the element \( g_k \) has no preimage, we can construct the unique near complete mapping \( \theta \) such that \( \theta(g) = \theta'(g).\theta_k^{-1} \) which is in canonical form. \( \square \)

**Corollary 1.** The number of complete or near complete mappings of a group of order \( n \) is congruent to 0 modulo \( n \).

**Corollary 2.** The number of transversals of the Cayley table of a group of order \( n \) is congruent to 0 modulo \( n \).

Corollary 2 is a restatement of a result by Belyavskaya and Russu [2].

We now discuss the question: which classes of groups possess complete or
near complete mappings? The following theorem is due to Paige [44].

**Theorem 1.6.** If \((G, \cdot)\) is a group of odd order, then \((G, \cdot)\) has a complete mapping.

**Proof.** Let \(\theta\) be the identity permutation on \(G\). Then the mapping \(\phi(x) = x\theta(x) = x^2\) is also a permutation on \(G\). To see this suppose \(g^2 = g\) say, where \(g\) is of order \(2m-1\) (the order of \(g\) is odd since the group is of odd order). Then \(g^2 = g \Rightarrow g^{4m-2} = 1 \Rightarrow g^{2m-1} = 1\) (since \(g_1\) must be of odd order) and so we have \(g_1 = g_2^{2m} = g^m\). Similarly we have \(g_2 = g_2^{2m} = g^m\) and so \(g_1 = g_2\). □

In Chapter 9 we will prove that if \((G, \cdot)\) is a finite group of order \(n\) which has a complete mapping, then there exists an ordering of its elements, say \(a_1, a_2, \ldots, a_n\) such that \(a_1 a_2 \cdots a_n = 1\), this result is due to Paige [44]. Paige [42] has shown that this necessary condition is sufficient if \((G, \cdot)\) is abelian and has conjectured that it is also sufficient in other cases. In Chapter 9 we will show that the product of all the elements in an abelian group is 1 unless the group possesses a unique element of order two. Thus we have that an abelian group possesses a complete mapping if and only if it does not contain a unique element of order two.

Hall and Paige [22] have generalised this result to prove that for soluble groups the necessary and sufficient, and for groups of even order the necessary, condition for the existence of a complete mapping of the group is that its Sylow 2-subgroups should be non-cyclic. They conjectured further that this condition is also sufficient for non-soluble groups. Thus, for non-soluble groups we have two independent conjectures (1) that, if the product of all the elements in some order is equal to the identity element, then the group has a complete mapping; (2) if the Sylow 2-subgroups are non-cyclic, then the group has a complete mapping. The second of these two conditions is known to be satisfied by all non-soluble groups and, in [13], Dénes and Keedwell show that the first condition is also satisfied by all non-soluble groups. This led them to propose the conjecture that all non-soluble groups possess complete mappings. Similarly, as will be shown in Chapter 9, if
$(G, \cdot)$ is a finite group of order $n$ which has a near complete mapping (in canonical form), then there exists an ordering of its elements, say $a_1, a_2, \ldots, a_n$ such that $a_1 a_2 \cdots a_n = \eta$, where $\eta$ is the exdomain element of the mapping. It is widely conjectured that all finite groups possess either complete or near complete mappings, this is often called the Brualdi conjecture.
Chapter 2 Applications of Orthogonal Latin Squares

2.0. Introduction

In this chapter we present a brief overview of applications of orthogonal latin squares. It should be noted that the word 'application' is being used in a somewhat weak sense. The applications discussed are in recreational mathematics, experimental design, finite projective geometry, error detecting and correcting codes and graph theory. This overview is necessarily incomplete, the section on graph theory alone could have been expanded so as to form a chapter in its own right and some topics have been left out. Of the topics left out, of particular importance are the many connections which exist between sets of m.o.l.s. and the study of cryptography. The purpose of the present chapter is not to give an exhaustive account of the applications of orthogonal latin squares but rather to give a flavour of the different ways in which these applications arise.

In section 2.3 we show how to obtain the result \( N(p^r) = p^r - 1 \), where \( p \) is a prime.

2.1. Euler's 36 officers problem

Latin squares, and in particular orthogonal latin squares, were first defined by Euler [14], in 1782, in connection with the following problem. 'Thirty six officers wish to parade in a square formation. The officers are selected from six regiments; the six officers from each regiment holding six different ranks, where the ranks are the same for each regiment. Is it possible for the officers to parade so that no two officers of the same rank or regiment are in the same row or column?' Euler showed that this problem is equivalent to that of obtaining an orthogonal pair of latin squares of order six. To see this let the sets of symbols \( S_1 = \{a, b, c, d, e, f\} \) and \( S_2 = \{1, 2, 3, 4, 5, 6\} \) denote the six different regiments and the six different ranks respectively. Since for each of the 36 possible
combinations of regiment and rank there corresponds exactly one officer, there exists a bijection between the ordered pairs \((i, j), i \in S_1, j \in S_2\) and the officers. Now, if such a square formation of officers were possible, we could form a \(6 \times 6\) array \(A\) by replacing each officer by the corresponding ordered pair \((i, j)\). Furthermore we could consider \(A\) as being the result of juxtaposing two \(6 \times 6\) arrays \(L_1\), defined on \(S_1\), and \(L_2\), defined on \(S_2\). The condition that no two officers from the same regiment appear in any row or column of the formation requires that \(L_1\) forms a latin square. Similarly, the condition that no two officers of the same rank appear in the same row or column of the formation requires that \(L_2\) forms a latin square. Thus \(A\) would be the result of juxtaposing two \(6 \times 6\) latin squares and, since each ordered pair of symbols occurs exactly once in \(A\), these latin squares would have to be orthogonal.

Euler knew how to construct pairs of orthogonal latin squares for all odd orders and for all doubly even orders, however he failed to solve the 36 officers problem which led him to conjecture that no pair of orthogonal latin squares of order six exists. Euler further conjectured that no orthogonal latin squares of order \(n\) exist for \(n = 4m + 2\). This is the well known ‘Euler Conjecture’ which, for the case \(n = 6\), was eventually proved correct by Tarry [54] in 1900 after an exhaustive search (thus proving that \(N(6) = 1\)). The general conjecture was, however, shown to be incorrect when first Bose and Shrikhande [6] constructed a pair of orthogonal latin squares of order 22, then, independently, and at about the same time, Parker [47] constructed an orthogonal pair of order ten. Finally Bose, Shrikhande and Parker [7] provided a general construction for pairs of orthogonal latin squares for all orders \(n = 4m + 2, n > 6\).

From this somewhat trivial beginning the subject of orthogonal latin squares has grown in importance considerably.
2.2. Orthogonal latin squares as experimental designs

In the 1920's Fisher advocated the use of latin squares and sets of m.o.l.s. in the design of experiments (see, for example, the last section of [15]). These were seen as being of particular use in connection with agricultural field trials. Consider an approximately square field and suppose that the experimenter wishes to compare the yields of \( n \) different crops. One approach would be to divide the field up into \( n \) areas and to select, at random, the crop which is to be planted in each area, subject only to the restriction that each crop is to be planted once. It is easy to see the inadequacy of such a design. Different areas of any field may be expected to vary in fertility and so it would be impossible to distinguish variations between the crops from these other sources of variation, which are outside the experimenter's control. A better approach might be to divide the field up into \( n \) rows and \( n \) columns and plant the crops so that each crop occurs once in each row and once in each column. Such a design is called, for obvious reasons, a Latin Square Design and a technique, developed by Fisher, called the Analysis of Variance can be employed to analyse the results. Now suppose that the experimenter also wishes to analyse the effects of \( n \) different types of fertiliser (or \( n \) different levels of the same fertiliser etc.). If we can construct a pair of orthogonal latin squares of size \( n \), say \( L_1 \) and \( L_2 \), then we can assign the crops to the plots according to \( L_1 \) and the fertilisers to the crops according to \( L_2 \). The experiment will now not only allow for variations across the field for both crops and fertilisers but also each of the \( n^2 \) possible crop/fertiliser combinations will occur exactly once. Thus we are now eliminating potential variation between crops across fertilisers and between fertilisers across crops. Such a design is often called a Graeco-Latin Square Design since it is usual, when we juxtapose \( L_1 \) and \( L_2 \), to use Greek and Latin letters as the symbol sets for \( L_1 \) and \( L_2 \) respectively. Once again suitable Analysis of Variance procedures exist for the analysis of results.
2.3. Finite projective planes

In 1938 Bose [4] observed that a complete set of \( n-1 \) m.o.l.s. of order \( n \) both defines and is defined by a projective plane of order \( n \). Furthermore it is known that a projective plane, in particular the projective plane defined by the Galois field, exists for all orders \( n = p^r \), where \( p \) is prime. It follows that complete sets of m.o.l.s. exist for all prime power orders. It is not known whether any projective planes exist which are not of prime power order. There are, however, projective planes of prime power order which are isomorphically distinct from the Galois plane, the smallest examples being of order nine. The next theorem proves the equivalence of projective planes and complete sets of m.o.l.s. of order \( n \). First we require the following well known result, which we state without proof.

**Lemma 2.1.** A finite projective plane of order \( n \) has \( n+1 \) points on every line, \( n+1 \) lines through every point, and has \( n^2 + n + 1 \) points and \( n^2 + n + 1 \) lines altogether.

**Theorem 2.1.** A finite projective plane of order \( n \) both defines and is defined by a set of \( n-1 \) mutually orthogonal latin squares of order \( n \).

**Proof.** Suppose we have a finite projective plane of order \( n \). We pick any line of our plane and call it the line at infinity, \( \ell_\infty \). Let \( A, C, B_1, B_2, \ldots, B_{n-1} \) be the \( n+1 \) points of \( \ell_\infty \). Through each of these points there pass \( n \) lines distinct from \( \ell_\infty \), by Lemma 2.1. We label these lines as follows: \( a_1, a_2, \ldots, a_n \) and \( c_1, c_2, \ldots, c_n \) are the lines through \( A \) and \( C \) respectively and \( b_{h1}, b_{h2}, \ldots, b_{hn} \) are the lines through \( B_h \). Every finite point \( P(i, j) \) can then be identified with an ordered set of \( n+1 \) numbers \((i, j, k_1, k_2, \ldots, k_{n-1})\) describing the \( n+1 \) lines \( a_p, c_j, b_{lk_1}, b_{2k_2}, \ldots, b_{n-1k_{n-1}} \) with which it is incident, one through each point of \( \ell_\infty \). A complete set of m.o.l.s. can be formed in the following way: in the \( h \)th square, put \( k_h \) in the \((i, j)\)th cell. Now each square is latin since, as \( j \) varies with \( i \) fixed, so does \( k_h \), by the properties of a projective plane, and so no entry can occur twice in the \( i \)th row. Similarly for
columns we have that as $i$ varies with $j$ fixed so does $k_h$. Furthermore any two latin squares $L_p$ and $L_q$ ($p \neq q$) are orthogonal for suppose, when $L_p$ and $L_q$ are juxtaposed, the ordered pair $(k, l)$ occurred in both the $(i, j)$th and $(i', j')$th cells. This would imply that the distinct lines $b_{pk}$ and $b_{ql}$ both passed through the distinct points $(i, j)$ and $(i', j')$ in contradiction to the axioms of a projective plane.

Conversely, from a given complete set of m.o.l.s. of order $n$ we may define a set of $n^2$ finite points. Each of these points may be identified with a particular cell in the array $A^*$ formed by juxtaposing all the latin squares simultaneously so that each cell contains an ordered $(n-1)$-set of symbols $(k_1, k_2, \ldots, k_{n-1})$. We can now construct $n+1$ sets, each containing $n$ parallel lines, as follows: each line $b_{jk}$ contains either the $n$ points corresponding to those cells in a single row or column of $A^*$ or the $n$ points corresponding to those cells of $A^*$ whose $j$th entry is $k$. Since $1 \leq j \leq n-1$ and $1 \leq k \leq n$, there are $n(n+1)$ such lines, each containing $n$ points. Furthermore the lines $b_{jk}$ and $b_{j'k}$, $k \neq k'$, clearly contain no points in common whereas the lines $b_{jk}$ and $b_{j'k}$, $j \neq j'$, contain exactly one point in common, from the orthogonality of the latin squares. Hence the $n(n+1)$ lines are partitioned into $n+1$ parallel classes of size $n$. To construct our projective plane we form a set of $n+1$ new points and append a given point to all the lines belonging to a particular parallel class, thereby ensuring that these lines will now have exactly one point in common. We then define a new line, $\ell_\omega$, which consists of the $n+1$ new points (therefore $\ell_\omega$ meets every line at exactly one point). We now have $n^2 + n + 1$ points, $n^2 + n + 1$ lines, each line contains $n+1$ points, each point is incident with $n + 1$ lines and any two distinct lines have exactly one point in common. We therefore have a finite projective plane of order $n$. □

The following theorem provides a simple construction for complete sets of m.o.l.s. of prime power order from the corresponding Galois field.
Theorem 2.2. Let \( \{f_0, f_1, \ldots, f_{n-1}\} \) be the elements of the Galois field of order \( n \) \((n = p^r)\), where \( f_0 \) is the zero element, and define \( a^h_{ij} = f_i + f_j f_k \). Then the \( n \times n \) array \( A_h \), which has \( a^h_{ij} \) as its \((i, j)\)th entry, is a latin square when \( 1 \leq h \leq n - 1 \), and the \( n - 1 \) latin squares so formed are mutually orthogonal.

Proof. Firstly we show that \( A_h \) is indeed a latin square. Suppose that \( a^h_{ij} = a^h_{ik} \), then \( f_i + f_h f_j = f_i + f_h f_k \) which is true if and only if \( f_j = f_k \) since \( f_h \neq 0 \), from which it follows that \( j = k \). Hence no element occurs twice in any row of \( A_h \). Similarly, if \( a^h_{ij} = a^h_{jk} \) then \( f_i + f_h f_j = f_k + f_h f_j \) which is true if and only if \( f_i = f_k \) and so \( i = k \). Hence no element occurs twice in any column of \( A_h \) and, since \( A_h \) is an \( n \times n \) array defined on \( n \) symbols, it therefore forms a latin square.

Secondly we show that two distinct latin squares \( A_h \) and \( A_k \) are orthogonal.

Suppose \( (a^h_{ij}, a^k_{ij}) = (a^h_{mn}, a^k_{mn}) \), \( h \neq k \), then

\[
\begin{align*}
    f_i + f_h f_j &= f_m + f_h f_n \quad (1) \\
    f_i + f_k f_j &= f_m + f_k f_n \quad (2)
\end{align*}
\]

\((1) - (2) \Rightarrow (f_h - f_k)f_j = (f_h - f_k)f_n \)

\[\Rightarrow f_j = f_n, \text{ since } h \neq k.\]

But from \((1)\): \( f_j = f_n \Rightarrow f_i = f_m \) and so we have that both \( j = n \) and \( i = m \). Hence, when \( A_h \) and \( A_k \) are juxtaposed, no ordered pair occurs more than once and so \( A_h \) and \( A_k \) are orthogonal. □

The above construction was discovered independently by Bose [4] and Stevens [52] and is often called the Bose or Bose-Stevens construction. In fact the construction was first discovered much earlier by Moore [40]. The complete set of m.o.I.s. displayed in fig. 1.3 can be constructed from the Galois field of order four using the construction of Theorem 2.2.
It should be noted that the equivalence of a projective plane of order \( n \) and a complete set of m.o.l.s. of order \( n \) is not trivial. It was not until 1907 that MacInnes [36] proved the non-existence of a projective plane of order six. However this result is implicit in Tarry's assertion, made some seven years earlier, that there exists no pair of orthogonal latin squares of order six. [Recall that we require a set of five m.o.l.s. of order six for the existence of a projective plane of order six.]

2.4. Construction of error detecting and correcting codes

Sets of m.o.l.s. have also been used in the construction of error detecting and error correcting codes. By a code we mean a finite set of code words, each consisting of a sequence of \( n \) symbols from a finite symbol set \( S \). Suppose one of these code words is to be transmitted across a noisy channel, received and then decoded. Since our channel is noisy there is some probability that any given symbol in the received word will differ from the corresponding symbol in the code word sent. However, if errors do occur, the received word will only be decoded incorrectly if it forms a different code word. Suppose that we know, or can assume, that at most only a single error has occurred in transmission, if the received word is not a code word then a single error has been detected. Furthermore, if it is possible to deduce what the original code word must have been, then a single error has been corrected. In general a code is called \( n \) error detecting (or correcting) if it is always possible to detect (correct) \( n \) errors occurring in any code word. Intuitively we can see that these properties are going to depend on the number of places in which any two code words differ. Hamming [23] formalised this idea as follows.

**Definition 2.1.** Let \( a = (a_1, a_2, \ldots, a_n) \) and \( b = (b_1, b_2, \ldots, b_n) \) be two code words of length \( n \), then the *Hamming distance* \( d(a,b) \) is defined as the number of places in which the two code words differ.
Of particular importance with regard to the properties of a code is the minimum Hamming distance, $d_{\text{min}}$, taken over all pairs of code words. In general it is clear that a code can be $d_{\text{min}} - 1$ error detecting or the integer part of $(d_{\text{min}} - 1)/2$ error correcting. We will now show one way in which codes may be constructed from sets of m.o.l.s.

Consider a set of $k$ m.o.l.s., $A_1, A_2, \ldots, A_k$, of order $n$, defined on $S = \{1, 2, \ldots, n\}$ and let $a_{ij}^k$ denote the $(i, j)$th entry in $A_k$. We can construct $n^2$ code words of length $k + 2$ of the form $(i, j, a_{ij}^1, a_{ij}^2, \ldots, a_{ij}^k)$. This set of code words has minimum Hamming distance $k + 1$. The simplest way to see this is to note that each code word is defined by any two of its entries. Therefore two distinct code words cannot agree in more than one place. Hence the Hamming distance between any two code words must be at least $k + 1$. However, it is easy to find two code words which agree in one place and so the minimum Hamming distance is indeed $k + 1$. It can be shown that this code is optimal in the sense that it attains the Joshi bound which is an upper bound on the number of code words of, in this case, length $k + 2$, defined on a symbol set of size $n$ and having minimum Hamming distance $k + 1$.

Using the complete set of m.o.l.s. displayed in fig. 1.3 we obtain, after adding one to each entry, the $4 \times 4$ array of code words displayed in fig. 2.1.

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

fig. 2.1

2.5. Orthogonal latin square graphs

Several connections have been developed over the years between graphs and latin squares. We now discuss an interesting connection which has been made
between graphs and orthogonal latin squares. In [34] Lindner, Mendelsohn, Mendelsohn and Wolk defined the following concept.

**Definition 2.2.** An orthogonal latin square graph (o.l.s.g.) is a graph in which the vertices are latin squares, all of which are of the same order and defined on the same symbol set. Two vertices are adjacent if and only if the corresponding latin squares are orthogonal.

We will say that a finite graph $G$ is realisable as an o.l.s.g. if there is an o.l.s.g. isomorphic to $G$. The following theorem is due to Lindner et al.

**Theorem 2.4.** Every finite graph is realisable as an o.l.s.g. by idempotent latin squares.

**Proof.** Let $G = (V, E)$ be a graph with $V = \{1, 2, \ldots, v\}$. Let $B_1, B_2, \ldots, B_v$ be any $v$ mutually orthogonal idempotent latin squares of order $n$ defined on $B = \{1, 2, \ldots, n\}$ and $A_1, A_2, \ldots, A_v$ be any $v$ mutually orthogonal idempotent latin squares of order $m$ defined on $A = \{1, 2, \ldots, m\}$. [Note that in particular we could have $n = m = p^n$ where $p^n > v + 1$.] Then the direct products $A_i \times B_1, A_2 \times B_2, \ldots, A_v \times B_v$ are mutually orthogonal and idempotent. The fact that they are mutually orthogonal follows from Theorem 1.3; that they are idempotent is inherited from the fact that the $A_i$'s and $B_j$'s are all idempotent.

Now for each of the 2-subsets $\{i, j\}$ of $V$ we alter the direct products $A_i \times B_i$ and $A_j \times B_j$ as follows:

1. if $\{i, j\} \in E$, then leave $A_i \times B_i$ and $A_j \times B_j$ as they are;

2. if $\{i, j\} \notin E$, then we can assume $i < j$ and replace $A_i(i, j)$ in $A_i \times B_i$ with the latin square obtained from $A_j$ by replacing each entry $x$ by $(x, b_{ij})$ where $b_{ij}$ is the entry in the $(i, j)$th cell of $B_j$.

If we denote the latin squares obtained by $G_1, G_2, \ldots, G_v$ then $G = (V, E)$ with
$G_1, G_2, \ldots, G_v$ as the vertices is an o.l.s.g.. To see this, if $(i, j) \notin E$, then by (2) $G_i$ and $G_j$ are not orthogonal. Conversely, if $(i, j) \in E$, then by (1) the subsquares $A_i(i, j)$ and $A_j(i, j)$ in $A_i \times B_i$ and $A_j \times B_j$ remain as they are. Now if the subsquare $A_k(p, q)$ is changed in $A_i \times B_i$ for example, the subsquare $A_k(p, q)$ remains as it is in $A_j \times B_j$. Since $A_k(p, q)$ is replaced with a square $A_k(p, q)$ where $A_k$ and $A_j$ are orthogonal, this change does not affect the orthogonality of the resulting squares nor their idempotence. It follows that $G = (V, E)$ with $G_1, G_2, \ldots, G_v$ as the vertices is an o.l.s.g.. □

Lindner et al study o.l.s.g.'s whose vertices are all possible latin squares of order $n$ for small $n$. For $n = 7$ their analysis is incomplete, they state that "It is not yet known if any square of order seven that is not an isotope of the cyclic group of order seven has an orthogonal mate." In Chapter 6 our results will show that such an orthogonal pair does indeed exist.
Chapter 3 Indirect Construction of M.O.L.S.

3.0. Introduction

It is possible to identify two distinct approaches to the problem of constructing sets of m.o.l.s. The first approach is to use a knowledge of groups, fields or some other algebraic structure in order to construct sets of m.o.l.s. directly. An analysis of this approach will take up much of the sequel. The second approach, which we discuss in this chapter, is to construct orthogonal latin squares of a certain order by combining orthogonal latin squares of smaller orders in some way. This technique has been used to obtain the results $N(10) \geq 2$ and $N(n) \geq 3$ for $n \in \{18, 22, 26, 28, 30\}$.

3.1. Direct product of quasigroups

We discussed the concept of the direct product of two quasigroups in Chapter 1. In particular Theorem 1.3 tells us that if we have a set of $k$ m.o.l.s. of order $m$ and a set of $l$ m.o.l.s. of order $n$, then we can construct a set of $\min(k, l)$ m.o.l.s. of order $mn$. Since we know that complete sets of m.o.l.s. exist for any prime power order we have the following result, which was first stated by MacNeish [37] in 1922.

Theorem 3.1. If $n = \prod_{i=1}^{r} p_i^{a_i}$, where the $p_i$ are distinct primes, then $N(n) \geq \min_{i} (p_i^{a_i} - 1)$.

Proof. This follows immediately from Theorem 1.3 and Theorem 2.2. □

The lower bound on $N(n)$ given by MacNeish has been bettered for most values of $n$, one exception is the result $N(28) \geq 3$. 


3.2. Parker’s method

Note that MacNeish’s theorem fails to provide us with a counter example to Euler’s conjecture since for \( n = 4m + 2 = 2(2m + 1) \) we have \( \min (p_i^2 - 1) = 1 \). As has been stated previously, the first counter example to the Euler conjecture was a pair of orthogonal latin squares of order 22, constructed by Bose and Shrikhande in 1958 (subsequently published in [6]). Shortly afterwards Parker constructed an orthogonal pair of order ten. Finally Bose, Shrikhande and Parker combined their efforts to provide constructions of pairs of orthogonal latin squares for all orders \( n = 4m + 2 \), except \( n = 2 \) and 6. This result finally closed the question regarding for which orders orthogonal latin squares exist. The answer is that they exist for all orders except two and six. One of the main theorems used in the proof of this result follows.

**Theorem 3.2.** If \( m \) is an integer such that \( N(m) \geq 2 \), then \( N(3m + 1) \geq 2 \).

**Proof.** Consider the \( 4 \times 4m \) matrix \( A \) defined by

\[
\begin{pmatrix}
  i & i+1 & \cdots & i & i+2 & \cdots & i+m & i-1 & i-2 & \cdots & i-m & k_1 & k_2 & \cdots & k_m \\
  i+1 & i+2 & \cdots & i+m & i & i & \cdots & i & k_1 & k_2 & \cdots & k_m & i-1 & i-2 & \cdots & i-m \\
  i-1 & i-2 & \cdots & i-m & k_1 & k_2 & \cdots & k_m & i & i & \cdots & i & i+1 & i+2 & \cdots & i+m \\
  k_1 & k_2 & \cdots & k_m & i-1 & i-2 & \cdots & i-m & i+1 & i+2 & \cdots & i+m & i & i & \cdots & i
\end{pmatrix}
\]

If the integers 0, 1, 2, \ldots, \( m \) and \( i \) are regarded as residues taken modulo \( (2m + 1) \), we see that among the columns \( (x, y)' \) of each two rowed submatrix of \( A \), every non-zero residue occurs exactly once among the \( 2m \) differences \( x - y \) not involving the elements \( k_1, k_2, \ldots, k_m \). It can be deduced from this that every two rowed submatrix of the \( 4 \times 4m(2m + 1) \) matrix \( A = (A_0, A_1, \ldots, A_{2m}) \) contains every ordered pair \( (x, y)' \), just once as a column and that it also contains each pair of the form \( (k_i, x)' \) and \( (x, k_i)' \). If we adjoin to this matrix \( A \) the \( OA(m, 4) \) constructed from a pair of orthogonal latin squares defined on the symbols \( k_1, k_2, \ldots, k_m \) (such a pair exists since \( m \) is such that \( N(m) \geq 2 \)), and also adjoin a \( 4 \times (2m + 1) \) matrix whose \( i \)th column contains the residue \( i \) in every place, \( i = 0, 1, \ldots, 2m \), we shall obtain a
matrix of four rows and \(4m(2m + 1) + m^2 + 2m + 1 = 9m^2 + 6m + 1 = (3m + 1)^2\) columns which is an \(OA(3m + 1, 4)\). Hence \(N(3m + 1) \geq 2\). □

**Corollary.** For every positive integer \(s\), \(N(12s + 10) \geq 2\).

**Proof.** This follows on setting \(m = 4s + 3\) in the above theorem and noting that, by MacNeish’s Theorem, \(N(m) \geq 2\) since \(m\) is odd. □

Theorem 3.2 is essentially the method used by Parker in [47] and so we will refer to it as Parker’s method. Using Parker’s method we obtain the following pair of orthogonal latin squares of order ten (and hence the fact that \(N(10) \geq 2\)).

\[
\begin{array}{ccccccc}
0 & 6 & 5 & 4 & k_3 & k_2 & k_1 & 1 & 2 & 3 \\
k_1 & 1 & 0 & 6 & 5 & k_3 & k_2 & 2 & 3 & 4 \\
k_2 & k_1 & 2 & 1 & 0 & 6 & k_3 & 3 & 4 & 5 \\
k_3 & k_2 & k_1 & 3 & 2 & 1 & 0 & 4 & 5 & 6 \\
1 & k_3 & k_2 & k_1 & 4 & 3 & 2 & 5 & 6 & 0 \\
3 & 2 & k_3 & k_2 & k_1 & 5 & 4 & 6 & 0 & 1 \\
5 & 4 & 3 & k_3 & k_2 & k_1 & 6 & 0 & 1 & 2 \\
2 & 3 & 4 & 5 & 6 & 0 & 1 & k_1 & k_2 & k_3 \\
4 & 5 & 6 & 0 & 1 & 2 & 3 & k_3 & k_2 & k_1 \\
6 & 0 & 1 & 2 & 3 & 4 & 5 & k_3 & k_1 & k_2 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
0 & k_1 & k_2 & k_3 & 1 & 3 & 5 & 2 & 4 & 6 \\
6 & 1 & k_1 & k_2 & k_3 & 2 & 4 & 3 & 5 & 0 \\
5 & 0 & 2 & k_1 & k_2 & k_3 & 3 & 4 & 6 & 1 \\
4 & 6 & 1 & 3 & k_1 & k_2 & k_3 & 5 & 0 & 2 \\
k_3 & 5 & 0 & 2 & 4 & k_1 & k_2 & 6 & 1 & 3 \\
k_2 & k_3 & 6 & 1 & 3 & 5 & k_1 & 0 & 2 & 4 \\
k_1 & k_2 & k_3 & 0 & 2 & 4 & 6 & 1 & 3 & 5 \\
1 & 2 & 3 & 4 & 5 & 6 & 0 & k_1 & k_2 & k_3 \\
2 & 3 & 4 & 5 & 6 & 0 & 1 & k_3 & k_1 & k_2 \\
3 & 4 & 5 & 6 & 0 & 1 & 2 & k_2 & k_3 & k_1 \\
\end{array}
\]
3.3. Yamamoto’s generating principle

In [58] Yamamoto provided a "generating principle" for latin squares. As an application of this generating principle Yamamoto showed how it could be used to construct pairs of orthogonal latin squares of order \( n \), where \( n = 4m + 2, \ m \geq 2 \). Yamamoto’s construction for orthogonal latin squares has been generalised and christened Yamamoto’s method by Guérin [21]. We will show that Parker’s method and Yamamoto’s generating principle are related in the sense that latin squares obtained by Parker’s method are isotopic to latin squares which can be obtained by an application of Yamamoto’s generating principle. We will further show that Parker’s method and Yamamoto’s method are equivalent for certain orders. We first give an account of Yamamoto’s generating principle.

Let \( L \) be an \( n \times n \) latin square defined on a symbol set \( S \), which possesses a transversal \( T \), and let \( k \) be a symbol not in \( S \). If we replace the symbols in the transversal \( T \) of \( L \) by \( k \), then we can form a latin square \( L^* \) of order \( n+1 \) by appending an \((n+1)\)th row and \((n+1)\)th column to \( L \). Note that the entry in the \((i, j)\)th cell of \( T \) in \( L \) becomes both the entry in the \(i\)th row of the \((n+1)\)th column of \( L^* \) and the entry in the \(j\)th column of the \((n+1)\)th row of \( L^* \). Finally, the entry in the \((n+1, n+1)\)th cell of \( L^* \) is \( k \). Yamamoto called \( L^* \) a 1-extension of \( L \) and \( L \) a 1-contraction of \( L^* \). [Note that Belousov [1] independently discovered the concept of a 1-extension under the name prolongation.]

It is helpful to think of the elements of \( T \) as having been projected both horizontally and vertically onto the \((n+1)\)th column and \((n+1)\)th row of \( L^* \) respectively.
Example: consider the following $5 \times 5$ latin square (the Cayley table of $Z_5$).

$$
L =

\begin{array}{cccc}
0 & 1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 & 0 \\
2 & 3 & 4 & 0 & 1 \\
3 & 4 & 0 & 1 & 2 \\
4 & 0 & 1 & 2 & 3 \\
\end{array}
$$

If we take the cells of the leading diagonal to be the transversal $T$ (i.e. $T = \langle (i, i) : i = 0, 1, 2, 3, 4 \rangle$) and let $k = 5$, then the corresponding 1-extension of $L$ is given by:

$$
L^* =

\begin{array}{cccc}
5 & 1 & 2 & 3 & 4 & 0 \\
1 & 5 & 3 & 4 & 0 & 2 \\
2 & 3 & 5 & 0 & 1 & 4 \\
3 & 4 & 0 & 5 & 2 & 1 \\
4 & 0 & 1 & 2 & 5 & 3 \\
0 & 2 & 4 & 1 & 3 & 5 \\
\end{array}
$$

The above construction may easily be generalised. Let $L_1$ be an $n \times n$ latin square defined on a symbol set $H$, which possesses $m$ disjoint transversals, $T_1, T_2, \ldots, T_m$. Let $L_2$ be an $m \times m$ latin square defined on a symbol set $K = \langle k_1, k_2, \ldots, k_m \rangle$, such that $H \cap K = \emptyset$. We construct a latin square $L^*$ of order $m+n$ defined on $H \cup K$ as follows. The first $n$ rows and $n$ columns of $L^*$ are formed by $L_1$ except where we replace the symbols in the transversal $T_i$ of $L_1$ by the element $k_i$ of $K$. The entries of $T_i$ are projected both horizontally and vertically so as to form the first $n$ entries in the $(n+i)$th column and row of $L^*$ respectively. Finally $L_2$ is the subsquare formed by the last $m$ rows and $m$ columns of $L^*$. $L^*$ is then called an $m$-extension of $L_1$ and $L_1$ an $m$-contraction of $L^*$.
The following example of an \( m \)-extension, in which we translate our discussion into the language of quasigroups, will prove useful. Let \( H_1 \) and \( H_2 \) be a pair of m.o.l.s. of order \( n \) defined on the symbol set \( H = \{ h_1, h_2, \ldots, h_n \} \) and let \( K_1 \) be a latin square of order \( m \), \( m \leq n \), defined on \( K = \{ k_1, k_2, \ldots, k_m \} \). We will consider these latin squares to be the Cayley tables of the pair of orthogonal quasigroups \( (H, \cdot) \) and \( (H, \circ) \) and the quasigroup \( (K, \times) \) respectively. We now construct a quasigroup \( (L, *) \) of order \( m+n \) from \( (H, \cdot) \) and \( (K, \times) \) using \( (H, \circ) \). We use \( (H, \circ) \) to locate \( m \) disjoint transversals, \( T_1, T_2, \ldots, T_m \) in \( H_1 \), where \( T_i = \{ (i, j) : i \circ j = t^*_b, t_i \in H \} \). We then define the binary operation \( * \) on \( L = H \cup K \) as follows:

\[
\begin{align*}
    h_i * h_j &= h_i \cdot h_j : (i, j) \notin \cup T_i, \\
    h_i * h_j &= k_i : (i, j) \in T_i, \\
    k_i * k_j &= k_i \times k_j, \\
    k_i * h_j &= h_i \cdot h_j : (i, j) \in T_i, \\
    h_i * k_i &= h_i \cdot h_j : (i, j) \in T_i.
\end{align*}
\]

For example, from the three quasigroups defined by:

\[
\begin{array}{cccc}
\circ & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 1 & 2 & 3 & 4 & 0 \\
2 & 2 & 3 & 4 & 0 & 1 \\
3 & 3 & 4 & 0 & 1 & 2 \\
4 & 4 & 0 & 1 & 2 & 3
\end{array}
\quad
\begin{array}{cccc}
\cdot & 0 & 1 & 2 & 3 & 4 \\
0 & 0 & 1 & 2 & 3 & 4 \\
1 & 2 & 3 & 4 & 0 & 1 \\
2 & 4 & 0 & 1 & 2 & 3 \\
3 & 1 & 2 & 3 & 4 & 0 \\
4 & 3 & 4 & 0 & 1 & 2
\end{array}
\quad
\begin{array}{cc}
\times & 5 & 6 \\
5 & 5 & 6 \\
6 & 6 & 5 \\
\end{array}
\]

and on setting \( T_i = \{ (i, j) : i \circ j = t^*_b, t_0 = 0, t_1 = 1 \} \), we obtain:
3.4. Yamamoto’s method

Yamamoto’s method utilises the above generating principle to provide a framework for the construction of \( v \) m.o.l.s. of order \( m+n \) from sets of \( v+1 \) m.o.l.s. of order \( n \) and \( v \) m.o.l.s. of order \( m \), when \( vm \leq n \). We shall illustrate this method for \( v = 2 \), the case discussed explicitly in [58].

Let \( (H, H_2, H_3) \) be a set of three m.o.l.s. of order \( n \) defined on the symbol set \( H = \{h_1, h_2, \ldots, h_n\} \). Let \( (K, K_2) \) be a pair of m.o.l.s. of order \( m \), where \( 2m \leq n \), defined on \( K = \{k_1, k_2, \ldots, k_m\} \), where \( H \cap K = \emptyset \). Once more we consider these latin squares to be the Cayley tables of the sets of mutually orthogonal quasigroups \( ((H, \cdot), (H, \circ), (H, \otimes)) \) and \( ((K, \cdot), (K, \circ)) \). We use \( (H, \circ) \) to locate \( m \) disjoint transversals in the Cayley table of \( (H, \cdot) \) and \( m \) further disjoint transversals in the Cayley table of \( (H, \circ) \). This is achieved by labelling 2\( m \) distinct elements of \( H \) by \( t_1, t_2, \ldots, t_m, t'_1, t'_2, \ldots, t'_m \), and then defining \( T_i = \{(i, j); i \circ j = t_i\} \) and \( T'_i = \{(i, j); i \otimes j = t'_i\} \). We then construct an \( m \)-extension \( (L, \cdot) \) of \( (H, \cdot) \) using \( (K, \cdot) \) and the transversals \( T_i, i = 1, 2, \ldots, m \). Similarly we can construct an \( m \)-extension \( (L, \circ) \) of \( (H, \circ) \) using \( (K, \circ) \) and the transversals \( T'_i, i = 1, 2, \ldots, m \). In the following example we have \( t_1 = 0, t_2 = 1, t_3 = 2, t'_1 = 3, t'_2 = 4 \) and \( t'_3 = 5 \).
<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**•**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**⊙**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

**×**

<table>
<thead>
<tr>
<th></th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

**⊗**

<table>
<thead>
<tr>
<th></th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>8</td>
<td>9</td>
<td>7</td>
</tr>
</tbody>
</table>
Note, however, that \((L, \ast)\) and \((L, \ast')\) do not form orthogonal quasigroups, for example, when the Cayley tables are juxtaposed the ordered pair \((1, 4)\) occurs twice (corresponding entries underlined).

It remains to discuss under what conditions, if any, \((L, \ast)\) and \((L, \ast')\) do form orthogonal quasigroups. We observe that when the Cayley tables for \((L, \ast)\) and \((L, \ast')\) are juxtaposed so as to form an array \(A\) of ordered pairs, each ordered pair of the form \((k_p, k_j)\) will occur exactly once in the subsquare formed by the intersection of the final \(m\) rows and \(m\) columns of \(A\). Furthermore each ordered pair of the form \((k_p, h_j)\) or \((h_j, k_p)\) will occur in the intersection of the first \(n\) rows and \(n\) columns of \(A\). We are left to consider ordered pairs of the form \((h_p, h_j)\). Since \((H, \cdot)\) and \((H, \circ)\) are orthogonal no pair \((h_p, h_j)\) will be repeated in the intersection of the first \(n\) rows and first \(n\) columns of \(A\). What we then require is that the remaining ordered pairs \((h_p, h_j)\) are exhausted by the leading \(n\)-tuples of the final \(m\) rows and \(m\) columns of \(A\).

Yamamoto’s approach was to let \((H, \circ)\) be the additive group of an associative, commutative ring and then to obtain, algebraically, the necessary and sufficient conditions for the above construction to yield an orthogonal pair of latin squares. We have the following theorem, which forms part of Guérin’s generalisation of Yamamoto’s work in [21].
Theorem 3.3. Let \((H, +, \cdot)\) be an associative and commutative ring where \(H\) is a set \(\{h_1, h_2, \ldots, h_n\}\) of order \(n\). We will denote multiplication in the ring by juxtaposition of elements. Let \((H, \cdot)\) and \((H, \circ)\) be two quasigroups defined on the set \(H\) by the equations: 
\[x \cdot y = \alpha_1 x + \beta_1 y\]
and 
\[x \circ y = \alpha_2 x + \beta_2 y,
\]
for all \(x, y \in H\), where \(\alpha_1, \alpha_2, \beta_1, \beta_2, \alpha_1 - \beta_2, \alpha_2 - \beta_2\) and \(\alpha_2 \beta_2 - \alpha_2 \beta_1\) are all regular elements (i.e. not zero divisors) of the ring \((H, +, \cdot)\). Let \((K, \times)\) and \((K, \otimes)\) be a pair of orthogonal quasigroups defined on a set \(K = \{k_1, k_2, \ldots, k_m\}\) of order \(m\), where \(2m \leq n\) and \(K \cap H = \emptyset\). Let \(T_i = \{(i, j) : h_i + h_j = t_i\}\) and \(T'_i = \{(i, j) : h_i + h_j = t'_i\}\), where \(t_i, t'_i \in H, i = 1, 2, \ldots, m\) and \((t_1, t_2, \ldots, t_m)\) and \((t'_1, t'_2, \ldots, t'_m)\) are disjoint sets, each of size \(m\). Then \(T_i\) and \(T'_i\) \(i = 1, 2, \ldots, m\), form disjoint transversals in the Cayley tables of \((H, \cdot)\) and \((H, \circ)\) respectively. Furthermore, \((L, \ast)\), defined by the \(m\)-extension of \((H, \cdot)\) using \((K, \times)\) and the transversals \(T_p\), and \((L, \ast')\), defined by the \(m\)-extension of \((H, \circ)\) using \((K, \otimes)\) and the transversals \(T'_p\), are orthogonal quasigroups provided that \(A = B_1 \cup B_2\), where:

\[
A = \{(\alpha_1 x + \beta_1 y, \alpha_2 x + \beta_2 y) : x, y \in H, x + y \in \{t_1, t_2, \ldots, t_m\} \cup \{t'_1, t'_2, \ldots, t'_m\}\},
\]

\[
B_1 = \{(\alpha_1 x + \beta_1 y, \alpha_2 x + \beta_2 z) : x, y, z \in H, x + y = t_r, x + z = t'_r, r = 1, 2, \ldots, m\},
\]

\[
B_2 = \{(\alpha_1 x + \beta_1 y, \alpha_2 z + \beta_2 y) : x, y, z \in H, x + y = t_r, z + y = t'_r, r = 1, 2, \ldots, m\}.
\]

Proof. We first show that \((H, \cdot)\) and \((H, \circ)\) so defined are indeed quasigroups. To show that \((H, \cdot)\) is a quasigroup we are required to show that for all \(x, y \in H\) the equations \(x \cdot z = y\) and \(z \cdot x = y\) have a unique solution in \(H\). But \(x \cdot z = y \iff \alpha_1 x + \beta_1 z = y \iff \beta_1 z = y - \alpha_1 x\), which is uniquely solvable for \(z\) in \(H\) since \((H, +)\) is a group and \(\beta_1\) is regular in \((H, +, \cdot)\). Also we have \(z \cdot x = y \iff \alpha_1 z + \beta_1 x = y \iff \alpha_1 z = y - \beta_1 x\), which is uniquely solvable for \(z\) in \(H\) since \(\alpha_1\) is regular in \((H, +, \cdot)\). Similarly, \((H, \circ)\) is a quasigroup using the fact that \(\alpha_2\) and \(\beta_2\) are regular in \((H, +, \cdot)\).

Secondly we show that \((H, +), (H, \cdot), (H, \circ)\) is a set of mutually orthogonal quasigroups. To show that \((H, +)\) and \((H, \cdot)\) are orthogonal it is sufficient to show...
that, for all $u, v \in H$, the pair of equations $x + y = u$ and $\alpha x + \beta y = v$ has a unique solution in $H$. But $x + y = u \Leftrightarrow \beta x + \beta y = \beta u$ which, by subtraction, gives us $(\alpha - \beta)x = v - \beta u$. The latter equation is uniquely soluble for $x$ in $H$ since $\alpha - \beta$ is regular in $(H, +, \cdot)$. Furthermore, $y$ is unique since $y = u - x$. Hence $(H, +)$ and $(H, \cdot)$ are orthogonal. Similarly $(H, +)$ and $(H, \circ)$ can be shown to be orthogonal using the fact that $\alpha - \beta$ is regular in $(H, +, \cdot)$. To show that $(H, \cdot)$ and $(H, \circ)$ are orthogonal it is sufficient to show that, for all $u, v \in H$, the pair of equations $\alpha x + \beta y = u$ and $\alpha x + \beta y = v$ has a unique solution in $H$. But these equations imply that $\alpha \beta x + \beta \beta y = \beta u$ and $\alpha \beta x + \beta \beta y = \beta v$ which together imply that $(\alpha \beta - \alpha \beta)x = \beta (u - v)$, which is uniquely soluble for $x$ since $\alpha \beta - \alpha \beta$ is regular. It can similarly be shown that $y$ is unique. Hence $(H, \cdot)$ and $(H, \circ)$ are orthogonal.

Thirdly we observe that since $(H, \cdot)$ and $(H, \circ)$ are both orthogonal to $(H, +)$, then any set of $n$ cells, $(i, j): h_i + h_j = t$, where $t$ is some fixed element of $H$, forms a common transversal in the Cayley tables of $(H, \cdot)$ and $(H, \circ)$. Furthermore, transversals corresponding to distinct fixed elements $t$ of $H$ will be disjoint. Therefore the sets of cells $T_i$ and $T'_i$, $i = 1, 2, \ldots, m$, defined as in the statement of the theorem, each defines $m$ disjoint transversals in the Cayley tables of $(H, \cdot)$ and $(H, \circ)$. Hence we can define two quasigroups $(L, \ast)$ and $(L, \ast')$ to be the $m$-extensions of $(H, \cdot)$ using $(K, \times)$ and $T_i$ and $(H, \circ)$ using $(K, \circ)$ and $T'_i$, respectively.

Finally, we show that $(L, \ast)$ and $(L, \ast')$ are orthogonal quasigroups provided

$A = B_1 \cup B_2$, as defined in the statement of the theorem. Let $A$ be the array of ordered pairs formed when the Cayley tables for $(L, \ast)$ and $(L, \ast')$ are juxtaposed. Their method of construction ensures that each of the ordered pairs from $K \times K$, $K \times H$ and $H \times K$ occur exactly once. Furthermore, since $(H, \cdot)$ and $(H, \circ)$ are orthogonal no ordered pair from $H \times H$ can occur twice in the subsquare of $A$ formed by its first $n$ rows and $n$ columns. What we require, therefore, is that each
ordered pair of the form \((h_i, h_j, h_p, h_p h_j)\), where either \(h_i + h_j = t_i\) or \(h_i + h_j = t'_i\), occurs in \(A\). But these ordered pairs are exactly the elements of the set \(A\). Moreover \(B_1\) is the set of ordered pairs that occur in the leading \(n\)-tuples of the final \(m\) columns of \(A\) and \(B_2\) is the set of ordered pairs that occur in the leading \(n\)-tuples of the final \(m\) rows of \(A\). Thus, if \(A = B_1 \cup B_2\), then \((L, \ast)\) and \((L, \ast')\) are orthogonal. □

It should be noted that the above construction is a generalisation of the specific application of Yamamoto's generating principle made in [58]. We will, however, see that it is not necessary for the quasigroups \((H, \cdot)\) and \((H, \circ)\) to be orthogonal in order for them to possess \(m\)-extensions which are orthogonal.

We now show that the result stated in Theorem 3.2 (Parker's method), for \(m\) such that 3 does not divide \((2m+1)\), is a special case of Theorem 3.3 (Yamamoto's method).

The \(OA(3m+1, 4)\) obtained from Parker's method is composed of columns, all of which are of one of the following six types.

\[
\begin{align*}
(1) & \quad \begin{pmatrix} i & i+j & l & k_p \\
i+1 & 1 & k & k_2 \\
i+j & i & k_j & k_3 \\
\end{pmatrix} \\
(2) & \quad \begin{pmatrix} i & -i-j & l & k_p \\
i & k_{ij} & i & k_2 \\
i-j & i & k_j & k_3 \\
\end{pmatrix} \\
(3) & \quad \begin{pmatrix} i & i+j & l & k_p \\
i & k_{ij} & i & k_2 \\
i+j & i & k_j & k_3 \\
\end{pmatrix} \\
(4) & \quad \begin{pmatrix} i & i & l & k_p \\
i & k & i & k_2 \\
i & i & i & k_3 \\
\end{pmatrix} \\
(5) & \quad \begin{pmatrix} i & i & l & k_p \\
i & k & i & k_2 \\
i & i & i & k_3 \\
\end{pmatrix} \\
(6) & \quad \begin{pmatrix} i & i & l & k_p \\
i & k & i & k_2 \\
i & i & i & k_3 \\
\end{pmatrix}
\end{align*}
\]

What we are required to find are values of \(\alpha_1, \beta_1, \alpha_2\) and \(\beta_2\) which are consistent both with Yamamoto’s method and with the above column types. In fact we will use the following column types in which the residues in the top row have been replaced by their additive inverses.

\[
\begin{align*}
(1) & \quad \begin{pmatrix} -i & i+j & l & k_p \\
i+1 & 1 & k_{ij} & k_2 \\
i+j & i & k_j & k_3 \\
\end{pmatrix} \\
(2) & \quad \begin{pmatrix} -i & -i-j & l & k_p \\
i & k_{ij} & i & k_2 \\
i-j & i & k_j & k_3 \\
\end{pmatrix} \\
(3) & \quad \begin{pmatrix} -i & i+j & l & k_p \\
i & k_{ij} & i & k_2 \\
i+j & i & k_j & k_3 \\
\end{pmatrix} \\
(4) & \quad \begin{pmatrix} -i & i & l & k_p \\
i & k & i & k_2 \\
i & i & i & k_3 \\
\end{pmatrix} \\
(5) & \quad \begin{pmatrix} -i & i & l & k_p \\
i & k & i & k_2 \\
i & i & i & k_3 \\
\end{pmatrix} \\
(6) & \quad \begin{pmatrix} -i & i & l & k_p \\
i & k & i & k_2 \\
i & i & i & k_3 \\
\end{pmatrix}
\end{align*}
\]

The above transformation corresponds to a reversing of the first \(n\) rows in
each of the resulting latin squares. It is easily seen that such a transformation preserves orthogonality and results in latin squares which are isotopic to the original latin squares.

We now show that the orthogonal latin squares obtained from the $OA(3m+1, 4)$, where $2m+1$ is not a multiple of 3, with columns of the above type, are identical to latin squares which can be obtained by an application of Yamamoto's method. In particular, we let the ring $(H, +, \cdot)$ be formed by addition and multiplication carried out modulo $2m+1$, where $H$ is the set of residues $\{0, 1, \ldots, 2m\}$. We then use the equations implied by column types (1) and (2) to obtain the necessary parameters $\alpha_1$, $\beta_1$, $\alpha_2$, and $\beta_2$. Next we show that these parameters satisfy the conditions of Theorem 3.3 and construct the appropriate transversals. Finally we show that these parameters are consistent with all of the remaining column types.

From column type (1) we obtain the equation

$$\alpha_1(-l) + \beta_1(l + j) = l - j$$

$$\Rightarrow (\beta_1 - \alpha_1)l + \beta_1j = i - j$$

$$\Rightarrow \alpha_1 = -2, \beta_1 = -1$$

Similarly, from column type (2) we obtain the equation

$$\alpha_2(-l - j) + \beta_2j = i - j$$

$$\Rightarrow (\beta_2 - \alpha_2)l - \alpha_2j = i - j$$

$$\Rightarrow \alpha_2 = 1, \beta_2 = 2$$

Thus we have $\alpha_1 = -2$, $\beta_1 = -1$, $\alpha_2 = 1$, $\beta_2 = 2$, $\alpha_1 - \beta_1 = -1$, $\alpha_2 - \beta_2 = -1$ and $\alpha_1\beta_2 - \alpha_2\beta_1 = -3$, which are all regular provided $2m+1$ is not a multiple of 3 (note that $\pm 2$ are regular since $2m+1$ is odd).
From column type (1) we see that, in order to fit Yamamoto’s method, the fixed element \( k_j \) must have replaced the elements of the transversal \( T'_j \), defined by \( t'_j = -i + (i + j) \) which implies \( t'_j = j \). Similarly, from column type (2), the fixed element \( k_j \) must have replaced the elements of the transversal \( T'_j \), defined by \( t_j = (-i - j) + i \) which implies \( t_j = -j \). We note that the \( t_j \)'s and \( t'_j \)'s, \( j = 1, 2, \ldots, m \), so defined are all distinct residues in \( H \), and so \( T_j \) and \( T'_j \) satisfy the conditions required for the transversals in Yamamoto’s method.

We now check that the above parameters are consistent with those of Yamamoto’s method for the remaining column types.

Column type (3) tells us which residues have been horizontally projected onto the \((n+j)\)th columns of the orthogonal latin squares. From this fact we can check the residues \( t_j \) and \( t'_j \) which define the corresponding transversals \( T_j \) and \( T'_j \).

We obtain

\[ \alpha_1(-i + j) + \beta_1 h_{ij} = i \]

where \( h_{ij} \) is such that \((-i + j) + h_{ij} = t_j \)

\[ \Rightarrow h_{ij} = t_j + i - j \]

\[ \Rightarrow -2(-i + j) - (t_j + i - j) = i \]

\[ \Rightarrow t_j = -j, \text{ as before.} \]

Similarly,

\[ \alpha_2(-i + j) + \beta_2 h'_{ij} = i + j \]

where \( h'_{ij} \) is such that \((-i + j) + h'_{ij} = t'_j \)

\[ \Rightarrow h'_{ij} = t'_j + i - j \]

\[ \Rightarrow (-i + j) + 2(t'_j + i - j) = i + j \]

\[ \Rightarrow t'_j = j, \text{ as before.} \]
Column type (4) tells us which residues have been vertically projected onto the \((n+j)\)th rows of the orthogonal latin squares. Again we can check the residues \(t_j\) and \(t'_j\) which define the transversals \(T_j\) and \(T'_j\).

We obtain,
\[
\alpha_1 h_{ij} + \beta_1 (i - j) = i + j
\]
where \(h_{ij}\) is such that \(h_{ij} + (i - j) = t_j\)
\[
\Rightarrow h_{ij} = t_j - i + j
\]
\[
\Rightarrow -2t_j + i - j = i + j
\]
\[
\Rightarrow t_j = -j, \text{ as before.}
\]

Similarly,
\[
\alpha_2 h'_{ij} + \beta_2 (i - j) = i
\]
where \(h'_{ij}\) is such that \(h'_{ij} + (i - j) = t'_j\)
\[
\Rightarrow h'_{ij} = t'_j - i + j
\]
\[
\Rightarrow t'_j - i + j + 2(i - j) = i
\]
\[
\Rightarrow t'_j = j, \text{ as before.}
\]

From column type (5) we obtain the equations \(\alpha_1 (-i) + \beta_1 i = i\) and \(\alpha_2 (-i) + \beta_2 i = i\). For consistency we require \(\beta_1 - \alpha_1 = 1\) and \(\beta_2 - \alpha_2 = 1\), which are both satisfied.

Finally, column type (6) ensures that the intersection of the final \(m\) rows and \(m\) columns of Parker's orthogonal latin squares form orthogonal latin subsquares, as is the case with Yamamoto's method.

Thus we have shown that Yamamoto's method can be used to obtain orthogonal latin squares which are isotopic to those obtained from Theorem 3.2, provided \(2m+1\) is not a multiple of three.
When $m$ is an integer such that $2m+1$ is a multiple of 3, the orthogonal pair of latin squares obtained from Parker's method can still be obtained as the $m$-extensions of two latin squares, $L_1$ and $L_2$, of order $2m+1$. They are still, therefore, of a form which may be obtained by an application of Yamamoto's generating principle. The difference now is that $L_1$ and $L_2$ are not orthogonal. For example, with $m = 4$, Parker's method gives the following pair of orthogonal latin squares of order thirteen.

<table>
<thead>
<tr>
<th>0 8 7 6 5</th>
<th>$k_4$</th>
<th>$k_3$</th>
<th>$k_2$</th>
<th>$k_1$</th>
<th>1 2 3 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$k_1$</td>
<td>1 0 8 7 6</td>
<td>$k_4$</td>
<td>$k_3$</td>
<td>$k_2$</td>
<td>2 3 4 5</td>
</tr>
<tr>
<td>$k_2$</td>
<td>2 1 0 8 7</td>
<td>$k_4$</td>
<td>$k_3$</td>
<td>3 4 5 6</td>
<td></td>
</tr>
<tr>
<td>$k_3$</td>
<td>3 2 1 0 8</td>
<td>$k_4$</td>
<td>4 5 6 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$k_4$</td>
<td>4 3 2 1 0</td>
<td>$k_1$</td>
<td>5 6 7 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>$k_4$</td>
<td>$k_3$</td>
<td>$k_2$</td>
<td>$k_1$</td>
<td>5 4 3 2</td>
</tr>
<tr>
<td>3</td>
<td>2 $k_4$</td>
<td>$k_3$</td>
<td>$k_2$</td>
<td>$k_1$</td>
<td>6 5 4 3</td>
</tr>
<tr>
<td>5</td>
<td>4 3 $k_4$</td>
<td>$k_3$</td>
<td>$k_2$</td>
<td>$k_1$</td>
<td>7 6 5 4</td>
</tr>
<tr>
<td>7</td>
<td>6 5 $k_4$</td>
<td>$k_3$</td>
<td>$k_2$</td>
<td>$k_1$</td>
<td>8 7 6 5</td>
</tr>
<tr>
<td>2</td>
<td>3 4 5 6 7</td>
<td>8 0 1 2 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5 6 7 8 0</td>
<td>1 2 3 4 5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>7 8 0 1 2</td>
<td>3 4 5 6 7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0 1 2 3 4</td>
<td>5 6 7 8 9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0 $k_1$</th>
<th>$k_2$</th>
<th>$k_3$</th>
<th>$k_4$</th>
<th>1 3 5 7 2 4 6 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 $k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
<td>2 4 6 3 5 7 0</td>
</tr>
<tr>
<td>7 0 2 4</td>
<td>$k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
</tr>
<tr>
<td>6 8 1 3</td>
<td>$k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
</tr>
<tr>
<td>5 7 0 2 4</td>
<td>$k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
</tr>
<tr>
<td>$k_4$</td>
<td>6 8 1 3 5</td>
<td>$k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
</tr>
<tr>
<td>$k_3$</td>
<td>7 0 2 4 6</td>
<td>$k_1$</td>
<td>$k_2$</td>
<td>8 1 3 5</td>
</tr>
<tr>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
<td>8 1 3 5 7</td>
<td>$k_1$</td>
</tr>
<tr>
<td>$k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
<td>0 2 4 6 8 1 3 5 7</td>
</tr>
<tr>
<td>1 2 3 4 5 6 7 8 0</td>
<td>$k_1$</td>
<td>$k_2$</td>
<td>$k_3$</td>
<td>$k_4$</td>
</tr>
<tr>
<td>2 3 4 5 6 7 8 0 1</td>
<td>$k_3$</td>
<td>$k_4$</td>
<td>$k_1$</td>
<td>$k_2$</td>
</tr>
<tr>
<td>3 4 5 6 7 8 0 1 2</td>
<td>$k_1$</td>
<td>$k_3$</td>
<td>$k_2$</td>
<td>$k_1$</td>
</tr>
<tr>
<td>4 5 6 7 8 0 1 2 3</td>
<td>$k_2$</td>
<td>$k_1$</td>
<td>$k_4$</td>
<td>$k_3$</td>
</tr>
</tbody>
</table>
The above orthogonal latin squares can be formed by 4-extensions of the following latin squares of order 9.

\[
\begin{array}{cccccccc}
0 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \\
2 & 1 & 0 & 8 & 7 & 6 & 5 & 4 & 3 \\
4 & 3 & 2 & 1 & 0 & 8 & 7 & 6 & 5 \\
6 & 5 & 4 & 3 & 2 & 1 & 0 & 8 & 7 \\
8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
1 & 0 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\
3 & 2 & 1 & 0 & 8 & 7 & 6 & 5 & 4 \\
5 & 4 & 3 & 2 & 1 & 0 & 8 & 7 & 6 \\
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 8 \\
\end{array} \quad \begin{array}{cccccccc}
0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \\
2 & 1 & 0 & 8 & 7 & 6 & 5 & 4 & 3 \\
4 & 3 & 2 & 1 & 0 & 8 & 7 & 6 & 5 \\
6 & 5 & 4 & 3 & 2 & 1 & 0 & 8 & 7 \\
8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \\
1 & 0 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\
3 & 2 & 1 & 0 & 8 & 7 & 6 & 5 & 4 \\
5 & 4 & 3 & 2 & 1 & 0 & 8 & 7 & 6 \\
7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 & 8 \\
\end{array}
\]

When the above latin squares are juxtaposed to form an array of ordered pairs, we observe that if an ordered pair occurs once, then it occurs exactly three times in the array (the above latin squares are therefore not orthogonal).

3.5. Hedayat and Seiden's method

In [25] Hedayat and Seiden define a method for composing two latin squares $L_1$ and $L_2$ of orders $n_1$ and $n_2$ respectively, to obtain a latin square of order $n_1+n_2$, provided $L_1$ has a certain "combinatorial structure". They call this method sum composition. In fact their idea of sum composition is identical to Yamamoto's idea of an $n_2$-extension of $L_1$, as was first pointed out in [11]. Hedayat and Seiden go on to show how this method can be used to construct pairs of orthogonal latin squares for an infinite number of orders of the form $4m+2$. These constructions again turn out to be special cases of Yamamoto's method. By way of example we give the following theorem, which appeared in [25] as Theorem 6.1.

**Theorem 3.4.** Let $n = p^r$, $n \geq 7$, $n \neq 13$, where $p$ is an odd prime and $s$ any positive integer. Then, if $m = \frac{n-1}{2}$, there exists an orthogonal pair of latin squares of order $m+n$.
Proof. We take $GF(p^r)$ as the ring $(H, +, \cdot)$ of Theorem 3.3 and choose $\alpha_1 = \alpha \neq \pm 1$, $\alpha_2 = \alpha^{-1}$, $\beta_1 = \beta_2 = 1$. Note that these choices for $\alpha_1$, $\alpha_2$, $\beta_1$ and $\beta_2$ satisfy the conditions for $(H, +), (H, \cdot), (H, \circ)$ to be a set of mutually orthogonal quasigroups. Furthermore, since $m \neq 6$ ($m = 6$ would imply $n = 13$), there exists a pair of mutually orthogonal quasigroups $(K, \times)$ and $(K, \circ)$ of order $m$, where $K \cap H = \emptyset$. We take an arbitrary fixed element $\lambda$ of $GF(p^r)$. Then the elements of $GF(p^r)$ distinct from $\lambda/2$ can be separated into $m$ pairs $t_i$ and $t'_i = \lambda - t_i$, $i = 1, 2, \cdots, m$, which we use to define the transversals $T_i$ and $T'_i$, $i = 1, 2, \cdots, m$.

It then follows that the condition $A = B_1 \cup B_2$ is satisfied, and so $(L, *)$ and $(L, \cdot')$ form orthogonal quasigroups, as we shall now show.

We have $A = \{(\alpha x + y, \alpha^{-1} x + y) : x + y = \mu \in GF(p^r), \mu \neq \lambda/2\}$, also $B_1 = \{(\alpha x + y, \alpha^{-1} x + z) : x + y = t_i, x + z = t'_i = \lambda - t_i, i = 1, 2, \cdots, m\}$, and $B_2 = \{(\alpha x + y, \alpha^{-1} x + y) : x + y = t_i, z + y = t'_i = \lambda - t_i, i = 1, 2, \cdots, m\}$.

We first consider the set $B_1$ and show that there exist elements $x_1, y_1 \in GF(p^r)$ such that $\alpha x + y = \alpha x_1 + y_1$ and $\alpha^{-1} x + z = \alpha^{-1} x_1 + y_1$. By subtraction, and using the fact that $y - z = t_i - t'_i$, we get $(\alpha - \alpha^{-1}) x + t_i - t'_i = (\alpha - \alpha^{-1}) x_1$. Hence we find that $x_1 = x + (t_i - t'_i)/(\alpha - \alpha^{-1})$ and $y_1 = y - \alpha(t_i - t'_i)/(\alpha - \alpha^{-1})$. We deduce that $B_1$ contains all ordered pairs $(\alpha x_1 + y_1, \alpha^{-1} x_1 + y_1)$ where $x_1 + y_1 = (t_i + t'_i)/(1 + \alpha) = \alpha \lambda/(1 + \alpha) + (1 - \alpha) t_i/(1 + \alpha)$, $i = 1, 2, \cdots, m$.

Next we consider the set $B_2$ and show that there exist elements $x_2, y_2 \in GF(p^r)$ such that $\alpha x + y = \alpha x_2 + y_2$ and $\alpha^{-1} x + y = \alpha^{-1} x_2 + y_2$. Using the fact that $x - z = t_i - t'_i$, we find that $x_2 = x - \alpha(t_i - t'_i)/(\alpha^{-1} - \alpha)$ and $y_2 = y + (t_i - t'_i)/(\alpha^{-1} - \alpha)$, and we deduce that $B_2$ contains all ordered pairs $(\alpha x_2 + y_2, \alpha^{-1} x_2 + y_2)$ where $x_2 + y_2 = (\alpha t_i + t'_i)/(1 + \alpha) = \alpha \lambda/(1 + \alpha) + (1 - \alpha) t'_i/(1 + \alpha)$, $i = 1, 2, \cdots, m$. 
Since the $t_i$'s and $t_i'$'s ($i = 1, 2, \ldots, m$) are all distinct it follows that $A = B_1 \cup B_2$ as required. □

Hedayat and Seiden point out that the method of the above theorem produces infinitely many pairs of orthogonal latin squares of order $4t + 2$ since if $p \equiv 7 \mod 8$ and $s$ is odd, then $p^s = (8t + 5)/3$ and thus $n + m = 4t + 2$. The above proof, which is essentially the same as given in [11] (Theorem 12.2.2, although here the condition $n \geq 7$ was omitted), has been constructed so as to highlight the similarity with Yamamoto's construction.

Theorem 3.4, whilst being a special case of Yamamoto's method is itself a generalisation of a special case of Theorem 3.2. We have that when $n = p$, $p$ prime, and $\lambda = 0$, the constructions implied by Theorems 3.2 and 3.4 will give pairs of orthogonal latin squares which are isotopic.

In [25] Hedayat and Seiden further discuss a modification of sum composition which is equivalent to that of a $1$-extension or prolongation. This does not fit Yamamoto's method since the original latin squares are not orthogonal, but, as we have seen in our discussion of Parker's construction, orthogonality of the contracted squares is not a necessary condition for the orthogonality of the extended squares. We will return to the topic of prolongation in Chapter 8.

3.6. Wang's method

Finally, in this chapter, we describe Wang's construction [59] which proved that $N(n) \geq 3$ for $n \in \{18, 22, 26, 30\}$. Our discussion will follow closely that of Street and Street [53]. Wang's construction results in two orthogonal latin squares $L$ and $S$, where $L$ is self-orthogonal and $S$ is symmetric. Hence the three latin squares $L$, $L'$ and $S$ form a mutually orthogonal set (where $L'$ denotes the transpose of $L$). [Note that since $L$ and $S$ are orthogonal we have that $L'$ and $S'$ are
orthogonal but $S' = S$ and so $L'$ and $S$ are orthogonal.]

The latin squares $L$ and $S$ are defined on the set $(w, x, y, z, 0, 1, \ldots, n-3)$ and may be partitioned into the forms:

$$
L = \begin{array}{cc}
L_1 & L_2 \\
L_3 & L_4 \\
\end{array} \\
S = \begin{array}{cc}
S_1 & S_2 \\
S_3 & S_4 \\
\end{array}
$$

where,

$$
L_1 = \begin{array}{cccc}
w & y & z & x \\
z & x & w & y \\
x & z & y & w \\
y & w & x & z \\
\end{array} \\
S_1 = \begin{array}{cccc}
z & x & w & y \\
x & z & y & w \\
w & y & z & x \\
y & w & x & z \\
\end{array}
$$

The $(n-4) \times (n-4)$ arrays $L_4$ and $S_4$ are constructed from their topmost rows using the relation $a_{ij} = a_{i-1,j-1} + 1 \pmod{n-4}$ where the elements $w, x, y$ and $z$ act as additive identities in $L$ and $w$ and $z$ act as additive identities in $S$ but $x + 1 = y$ and $y + 1 = x$ in $S$.

The $4 \times (n-4)$ arrays $L_2$ and $S_2$ are constructed from their left most column by the relationship $a_{ij} = a_{i,j-1} + 1 \pmod{n-4}$ and the $(n-4) \times 4$ arrays $L_3$ and $S_3$ are constructed from there topmost row by the relationship $a_{ij} = a_{i-1,j} + 1 \pmod{n-4}$.

Thus we need only to specify the initial columns of $L_2$ and $S_2$ and the initial rows of $L_3, S_3, L_4$ and $S_4$ in order to define $L$ and $S$. The following table appears in [53].
Initial rows and columns for constructing sets of three m.o.l.s., $n = 18, 22, 26, 30$.

Initial columns for $L_2$, $S_2$:

\[
\begin{align*}
13 & 0 & 7 & 11 & 10 & 18 & 13 & 22 \\
3 & 10 & 5 & 0 & 20 & 5 & 8 & 7 \\
12 & 8 & 4 & 6 & 7 & 20 & 15 & 3 \\
2 & 1 & 16 & 1 & 3 & 4 & 18 & 8 \\
L_2 & S_2 & L_2 & S_2 & L_2 & S_2 & L_2 & S_2 \\
n = 18 & n = 22 & n = 26 & n = 30 \\
\end{align*}
\]

Initial rows for $L_3$, $S_3$, $L_4$, $S_4$:

\[
\begin{align*}
n = 18 \\
L_3: & 8 & 5 & 4 & 6 & L_4: & 0 & 7 & 13 & 12 & 11 & 10 & 2 & 1 & 9 & z & y & x & w & 3 \\
S_3: & 0 & 10 & 8 & 1 & S_4: & z & x & 13 & 6 & 9 & 7 & 4 & w & 12 & 2 & 5 & 3 & 11 & y \\
n = 22 \\
n = 26 \\
L_3: & 3 & 6 & 4 & 2 \\
S_3: & 18 & 5 & 20 & 4 \\
L_4: & 0 & 9 & 21 & 20 & 19 & 18 & 15 & 12 & 10 & 13 & 16 & 1 & 11 & 14 & 8 & 7 & 5 & z & y & x & w & 17 \\
S_4: & z & x & 21 & 9 & 16 & 13 & 7 & 17 & 0 & 11 & 3 & w & 15 & 2 & 14 & 10 & 1 & 8 & 12 & 6 & 19 & y \\
n = 30 \\
L_3: & 2 & 3 & 6 & 16 \\
S_3: & 22 & 7 & 3 & 8 \\
\end{align*}
\]

**Table 3.1**

Table 3.1 gives the following latin squares, $L$ and $S$, for $n = 18$. 
\[ L = \]

<table>
<thead>
<tr>
<th></th>
<th>(w)</th>
<th>(y)</th>
<th>(z)</th>
<th>(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>12</td>
<td>0</td>
<td>12</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
<td>12</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

\[ S = \]

<table>
<thead>
<tr>
<th></th>
<th>(w)</th>
<th>(y)</th>
<th>(z)</th>
<th>(x)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10</td>
<td>8</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
<td>9</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>2</td>
<td>12</td>
<td>10</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>3</td>
<td>13</td>
<td>11</td>
<td>4</td>
<td>15</td>
</tr>
<tr>
<td>4</td>
<td>14</td>
<td>12</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>13</td>
<td>6</td>
<td>17</td>
</tr>
<tr>
<td>6</td>
<td>16</td>
<td>14</td>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>7</td>
<td>17</td>
<td>15</td>
<td>8</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>18</td>
<td>16</td>
<td>9</td>
<td>20</td>
</tr>
<tr>
<td>9</td>
<td>19</td>
<td>17</td>
<td>10</td>
<td>21</td>
</tr>
<tr>
<td>10</td>
<td>20</td>
<td>18</td>
<td>11</td>
<td>22</td>
</tr>
<tr>
<td>11</td>
<td>21</td>
<td>19</td>
<td>12</td>
<td>23</td>
</tr>
<tr>
<td>12</td>
<td>22</td>
<td>20</td>
<td>13</td>
<td>24</td>
</tr>
<tr>
<td>13</td>
<td>23</td>
<td>21</td>
<td>14</td>
<td>25</td>
</tr>
</tbody>
</table>
Notice that although these squares cannot be constructed by an application of Yamamoto's generating principle they do have certain similarities with such squares. For example each square possesses a $4 \times 4$ latin subsquare of elements which, in the case of $L$, are also fixed elements in the broken diagonals of the subsquare formed by its final $(n-4)$ rows and columns. In $S$ the symbols $w$ and $z$ are also fixed in this subsquare however the symbols $x$ and $y$ alternate. In both $L$ and $S$ the remaining elements cycle within their subarray in just the same way as occurs with Yamamoto's squares. However even $L$ (which follows the Yamamoto pattern closer than $S$) does not possess a 4-contraction which would form a $14 \times 14$ latin square on the set $\{0, 1, \ldots, 13\}$ as would be the case if it had been generated by Yamamoto's principle.
Chapter 4 Direct Constructions of M.O.L.S. From Groups

4.0. Introduction

In Chapter 1 we showed that the Cayley table of a group is always a latin square (although the converse is false). In this chapter we discuss methods of constructing sets of m.o.l.s. directly from such Cayley tables. In particular we show how the results $N(12) \geq 5$, $N(15) \geq 4$, $N(21) \geq 4$ and $N(24) \geq 4$ were obtained in this way.

4.1. Mann's automorphism method

In [38] Mann made the following definition.

Definition 4.1. If $(G, \cdot)$ is a group and $\sigma$ and $\tau$ are permutations on $G$, then $\sigma$ and $\tau$ are said to be orthogonal permutations if the function $x \mapsto \sigma(x)\tau(x)^{-1}$ is also a permutation on $G$.

With each permutation $\sigma$ on $G$ one associates the latin square $L_\sigma$, with rows and columns indexed by $G$, in which the entry in the $(i, j)$th cell is given by $\sigma(i) \cdot j$.

We then have the following important result which is due to Mann.

Theorem 4.1. Let $\sigma$ and $\tau$ be two permutations defined on the elements of the group $(G, \cdot)$. Then $\sigma$ and $\tau$ are orthogonal if and only if $L_\sigma$ and $L_\tau$ are orthogonal.

Proof. Firstly, let $\sigma$ and $\tau$ be orthogonal permutations on $G$. We are required to show that $L_\sigma$ and $L_\tau$ are orthogonal. Let $A$ be the array of ordered pairs formed when we juxtapose $L_\sigma$ and $L_\tau$ and suppose that the ordered pair $(m, n)$ occurs in both the $(i, j)$th and $(k, l)$th cells of $A$. Then the following four equalities hold.

\[
\sigma(i) \cdot j = m, \quad \sigma(k) \cdot l = m
\]

\[
\tau(i) \cdot j = n, \quad \tau(k) \cdot l = n
\]
Together these imply that \( \sigma(i)\tau(j)^{-1} = mnr^{-1} = \sigma(k)\tau(k)^{-1} \)

and so \( i = k \) and \( j = l \), since \( \sigma \) and \( \tau \) are assumed to be orthogonal.

Thus each ordered pair occurs in at most one cell of \( A \) and so \( L_\sigma \) and \( L_\tau \) are orthogonal.

Conversely, let \( L_\sigma \) and \( L_\tau \) be orthogonal Latin squares, with \( A \) defined as before, and suppose that \( \sigma(x)\tau(x)^{-1} = \sigma(y)\tau(y)^{-1} \). We are required to show that \( x = y \).

Now let \((a, b)\) be the ordered pair which occurs in the \( x \)th row and \( j \)th column of \( A \) for some \( j \), then

\[
\begin{align*}
\sigma(x) \cdot j &= a \quad \text{and} \quad \tau(x) \cdot j = b \\
\text{hence} \quad \sigma(x)\tau(x)^{-1} &= ab^{-1} \\
\Rightarrow \quad \sigma(y)\tau(y)^{-1} &= ab^{-1} \\
\Rightarrow \quad \sigma(y)^{-1}a &= \tau(y)^{-1}b = j', \text{ say,} \\
\Rightarrow \quad \sigma(y) \cdot j' &= a \quad \text{and} \quad \tau(y) \cdot j' = b
\end{align*}
\]

and so \((a, b)\) occurs in the \( y \)th row and \( j' \)th column of \( A \). Hence \( x = y \), since \( L_\sigma \) and \( L_\tau \) were assumed orthogonal. □

In searching for sets of mutually orthogonal permutations on \( G \) it is sufficient to consider only those permutations which fix the identity of \( G \) and only those sets of permutations which contain the identity permutation \( i \) on \( G \). If \((G, +)\) is an abelian group, then the permutations \( \phi \) on \( G \) which are orthogonal to \( i \) are exactly those permutations on \( G \) which we called orthomorphisms in Chapter 1. This follows since we have that \( \phi \) is a permutation such that the mapping defined by \( x \rightarrow \phi(x) \cdot x^{-1} = x^{-1}\phi(x) \) is also a permutation on \( G \).
If a latin square $L$ is isotopic to the Cayley table of some group $(G, \cdot)$, then we will say that $L$ is based on $(G, \cdot)$. Mann's approach was to consider the permutations on $G$ induced by the automorphisms of $(G, \cdot)$. The following result is due to Mann.

**Theorem 4.2.** Let $(G, \cdot)$ be a group and suppose that there exist $h$ automorphisms $\tau_1, \tau_2, \ldots, \tau_h$ of $(G, \cdot)$, every pair of which possesses the property that $u \tau_i \neq u \tau_j$ for any element $u$ of $G$ except the identity element. Then we can construct $h$ m.o.l.s. based on the group $(G, \cdot)$.

**Proof.** Let $\tau_i$ and $\tau_j$ be automorphisms of $(G, \cdot)$ such that $\tau_i(u) = \tau_j(u) = u = 1$ and suppose that $\tau_i(x)\tau_j(x)^{-1} = \tau_i(y)\tau_j(y)^{-1}$. We are required to show that $x = y$ and hence $\tau_i$ and $\tau_j$ are orthogonal.

Now $\tau_i(x)\tau_j(x)^{-1} = \tau_i(y)\tau_j(y)^{-1}$

$\Rightarrow \tau_i(x)^{-1}\tau_j(y) = \tau_j(x)^{-1}\tau_i(y)$

$\Rightarrow \tau_i(x^{-1}y) = \tau_j(x^{-1}y)$, since $\tau_i$ and $\tau_j$ are automorphisms,

$\Rightarrow x^{-1}y = 1$ and so $x = y$. □

Mann's statement of Theorem 4.2 was motivated by Bose's construction of complete sets of m.o.l.s. of order $n$ from $GF(n)$. Bose's construction, which was described in Chapter 2, effectively uses the group of automorphisms of the additive group of $GF(n)$ induced by multiplication by its non-zero elements.

Mann's method, as implied by Theorem 4.2 (which Keedwell has called the automorphism method in [31]), was not successful in improving any of the known lower bounds for $N(n)$. In fact Mann himself gave the following theorem which
showed that the automorphism method could do no better than equal the bounds implied by MacNeish’s Theorem.

**Theorem 4.3.** Let \( c_q \) be the number of conjugacy classes of elements of order \( q \) of a group \((G, \cdot)\). Let \( s = \min c_q \), then not more than \( s \) mutually orthogonal latin squares can be constructed from \((G, \cdot)\) by the automorphism method.

**Proof.** Let \( \tau_i = i, \tau_2, \ldots, \tau_h \) be automorphisms of \((G, \cdot)\) such that for all \( i, j: i \neq j \), the automorphism \( \tau_i^{-1} \) leaves no element except 1 fixed. If \( x \) is of order \( q \), then \( \tau_i^{-1}(x) \) is also of order \( q \). Now suppose that \( \tau_i^{-1}(x) = p^{-1}xp \), for some \( p \in G \) (i.e. we assume that \( x \) and \( \tau_i^{-1}(x) \) belong to the same conjugacy class), we will show that \( x = 1 \).

Let \( q \) be the element of \( G \) such that \( p = q^{-1} \tau_i^{-1}(q) \) (such an element exists since \( \tau_i^{-1}(q_1) = q_1^{-1} \tau_i^{-1}(q_2) = q_1 q_2^{-1} = \tau_i^{-1}(q_1) \tau_i^{-1}(q_2) \tau_i^{-1}(q_1) = q_1 q_2^{-1} = 1 \Rightarrow q_1 = q_2 \) thus as \( q \) varies across the elements of \( G \) so does \( q^{-1} \tau_i^{-1}(q) \)). Then \( \tau_i^{-1}(q x q^{-1}) = q p p^{-1} x p^{-1} q^{-1} = q x q^{-1} \). Hence \( q x q^{-1} = 1 \) which implies that \( x = 1 \). Thus we have that, for all \( i, j: i \neq j, \tau_i \) and \( \tau_j \) must map non-identity elements into distinct conjugacy classes. Hence \( h \leq \min c_q \). \( \square \)

**Corollary.** If \( n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} \) (where the \( p_i \) are distinct primes), then not more than \( h = \min (p_i^{a_i} - 1) \) orthogonal latin squares of order \( n \) can be constructed from any group by the automorphism method.

**Proof.** A Sylow subgroup of order \( p_i^{a_i} \) contains a representative of every conjugacy class of elements of order \( p_i \) (since the Sylow \( p_i \)-subgroups of \((G, \cdot)\) are all conjugate for fixed \( i \)). Hence \( \min c_q \leq \min (p_i^{a_i} - 1) \). \( \square \)

### 4.2. The orthomorphism method

Although the results of Mann’s automorphism method were not encouraging, Theorem 4.1 did provide a method for the construction of five m.o.l.s. of order
twelve, four m.o.l.s. of order fifteen and four m.o.l.s. of order twenty four. We
will call this method, for obvious reasons, the \textit{orthomorphism method}.

In \cite{30} Johnson, Dulmage and Mendelsohn use the orthomorphism method
to construct a set of five m.o.l.s. of order twelve based on the group $C_2 \times C_6$
(thereby establishing that $N(12) \geq 5$). Working simultaneously, but independently,
Bose, Chakravarti and Knuth \cite{5} obtained further sets of five m.o.l.s. of order
twelve based on $C_2 \times C_6$. Both of these sets of authors obtained their results with
the aid of a computer using the method implied by Theorem 4.1, either explicitly,
as in the case of Johnson, Dulmage and Mendelsohn, or implicitly, as in the case
of Bose, Chakravarti and Knuth. It should be noted that, despite the similarity of
results, the methods employed by the computer searches were quite different.

In Figure 1 of Bose, Chakravarti and Knuth \cite{5} a set of five m.o.l.s. of order
twelve is given, which can be obtained as follows. Let $L_1$ be the basis square
defined by

$$
\begin{array}{cccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
1 & 2 & 3 & 4 & 5 & 0 & 7 & 8 & 9 & 10 & 11 & 6 \\
2 & 3 & 4 & 5 & 0 & 1 & 8 & 9 & 10 & 11 & 6 & 7 \\
3 & 4 & 5 & 0 & 1 & 2 & 9 & 10 & 11 & 6 & 7 & 8 \\
4 & 5 & 0 & 1 & 2 & 3 & 10 & 11 & 6 & 7 & 8 & 9 \\
5 & 0 & 1 & 2 & 3 & 4 & 11 & 6 & 7 & 8 & 9 & 10 \\
6 & 7 & 8 & 9 & 10 & 11 & 0 & 1 & 2 & 3 & 4 & 5 \\
7 & 8 & 9 & 10 & 11 & 6 & 1 & 2 & 3 & 4 & 5 & 0 \\
8 & 9 & 10 & 11 & 6 & 7 & 2 & 3 & 4 & 5 & 0 & 1 \\
9 & 10 & 11 & 6 & 7 & 8 & 3 & 4 & 5 & 0 & 1 & 2 \\
10 & 11 & 6 & 7 & 8 & 9 & 4 & 5 & 0 & 1 & 2 & 3 \\
11 & 6 & 7 & 8 & 9 & 10 & 5 & 0 & 1 & 2 & 3 & 4 \\
\end{array}
$$

$L_1$

Then each of the other four squares is obtained from $L_1$ by row permutation; the
four permutations give the following four first columns:
Note that $L_1$ is the Cayley table for $Z_2 \oplus Z_6$ (written in additive notation) where the element $(a, b)$ is denoted by the number $6a + b$. Since $L_1, L_2, L_3, L_4$ and $L_5$ so formed are mutually orthogonal we have that the permutations

\[
\alpha_1 = i,
\]
\[
\alpha_2 = (0)(1 2)(3 10 6)(4 9 7 5 11 8),
\]
\[
\alpha_3 = (0)(1 10 11 3 8 7)(2 4)(5 6 9),
\]
\[
\alpha_4 = (0)(1 5 7 4 10 3 2 9)(6 8 11),
\]
\[
\alpha_5 = (0)(1 6 2 5 4 11 9 3 7 8 10),
\]

form a mutually orthogonal set. Furthermore, since the identity permutation is in this set, $\alpha_2, \alpha_3, \alpha_4$ and $\alpha_5$ are orthomorphisms of $Z_2 \oplus Z_6$.

In [51] Schellenberg, van Rees and Vanstone constructed a set of four m.o.l.s. of order 15 thereby proving that $\mathcal{N}(15) \geq 4$. The latin squares in this set are all based on the Cayley table for $Z_{15}$. Their construction follows.

The topmost rows of the squares are given by:

\[
L_1 = 0  14  1  13  2  12  3  11  4  10  5  9  6  8  7
\]
\[
L_2 = 0  13  2  10  5  8  7  6  9  3  12  11  4  14  1
\]
\[
L_3 = 0  9  6  12  3  1  14  5  10  8  7  2  13  11
\]
$L_4 = 0 \ 5 \ 10 \ 9 \ 6 \ 14 \ 1 \ 4 \ 11 \ 13 \ 2 \ 8 \ 7 \ 3 \ 12$

If these rows are considered as zeroth rows, then the $i$th row of each square is obtained by adding $i$ (modulo 15) to every element of its zeroth row. Now if we take the transpose of these squares and rearrange their rows so that the leftmost column of $L_1'$ is in natural order, we obtain the following set of four mutually orthogonal permutations of $Z_{15}$.

$\sigma_1 = i$

$\sigma_2 = (0)(1 \ 2 \ 5 \ 12 \ 8 \ 14 \ 13 \ 10 \ 3 \ 7)(4 \ 9 \ 11 \ 6)$

$\sigma_3 = (0)(1 \ 6 \ 13 \ 12)(2 \ 3 \ 14 \ 9)(4 \ 10 \ 8 \ 11 \ 5 \ 7)$

$\sigma_4 = (0)(1 \ 10 \ 13 \ 9 \ 8 \ 3)(2 \ 6 \ 7 \ 12 \ 14 \ 5)(4 \ 11)$

In [46] Parker showed that $N(21) \geq 4$. This was the first time that the lower bound on $N(n)$, as implied by MacNeish's Theorem, had been improved upon. Parker in fact proved that $N(q^2 + q + 1) \geq N(q + 1)$ when $q$ is a prime power. The method of proof is quite lengthy, using several results from statistical design theory and projective geometry (see, for example, [11] Chapter 11), and will not be discussed here. The m.o.l.s. of order 21 obtained by Parker are, however, defined by the following set of four mutually orthogonal permutations of the group $Z_{21}$.

$\sigma_1 = i$

$\sigma_2 = (0)(1 \ 6 \ 18 \ 8)(2 \ 12 \ 16 \ 15)(3 \ 4 \ 11 \ 9)(5 \ 7 \ 20 \ 17)(10 \ 13 \ 19 \ 14)$

$\sigma_3 = (0)(1 \ 18)(2 \ 16)(3 \ 11)(4 \ 9)(5 \ 20)(6 \ 8)(7 \ 17)(10 \ 19)(12 \ 15)(13 \ 14)$

$\sigma_4 = (0)(1 \ 8 \ 18 \ 6)(2 \ 15 \ 16 \ 12)(3 \ 9 \ 11 \ 4)(5 \ 17 \ 20 \ 7)(10 \ 14 \ 19 \ 13)$
In [50] Roth and Peters explicitly used the orthomorphism method to prove that $N(24) \geq 4$. Roth and Peters displayed seven sets of three mutually orthogonal orthomorphisms of the group $Z_2 \oplus Z_2 \oplus Z_6$, which were found by a non-exhaustive computer search and from which seven sets of mutually orthogonal latin squares of order twenty four could be obtained. One such set of mutually orthogonal permutations is given below in which the element $(a, b, c)$ is represented by the integer $4a + 2b + c$.

$\sigma_1 = 1$

$\sigma_2 = (0)(1 2 3)(4 8 16 15 20 18)(5 10 23 19 14 6 11 17)(7 9 22 13)(12 21)$

$\sigma_3 = (0)(1 3 2)(4 12 9 14 16 10 5 17 21 6 19 8 22)(11 20 13 18 23 15)$

$\sigma_4 = (0)(1 5 14 3 12 19 9 8 11 23 18 13 15 7 22 16 21 4 10 20 6 2 17)$

Finally, in this chapter, we discuss the connection which exists between the orthomorphism method and the direct product construction implied by MacNeish’s Theorem. MacNeish’s Theorem states that $N(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \geq m = \min p_i^{a_i} - 1$. The lower bound $m$ can be attained with equality by taking a set of $m$ m.o.l.s. of each order $p_i^{a_i}$ (using the Bose construction of Theorem 2.2) and then forming direct products using one latin square from each of these sets for each product.

Just as the Bose construction can be thought of as a special case of the orthomorphism method so too can the direct product construction. To see this notice that if $\phi_1$ is an orthomorphism of the group $(G_1, \cdot)$ and $\phi_2$ is an orthomorphism of the group $(G_2, \circ)$, then $\phi$ is an orthomorphism of the direct product $(G_1 \times G_2, \otimes)$, where $\phi(g_1, g_2) = (\phi_1(g_1), \phi_2(g_2))$. Furthermore, if $\phi'_1$ and $\phi'_2$ are also orthomorphisms of $(G_1, \cdot)$ and $(G_2, \circ)$ respectively, then $\phi'(g_1, g_2) = (\phi'_1(g_1), \phi'_2(g_2))$ is also an orthomorphism of $(G_1 \times G_2, \otimes)$ and $\phi$ and $\phi'$ are orthogonal permutations if and only if the pairs $\phi_1, \phi'_1$ and $\phi_2, \phi'_2$ are orthogonal.
Chapter 5 Finite Left Neofields

5.0. Introduction

In this chapter we give some basic definitions and results concerning left neofields. This will prepare us for Chapter 6 in which we describe a general method of construction of sets of m.o.l.s. from left neofields. In Chapter 6 we will also present detailed information for all isomorphically distinct left neofields of order less than ten and summarised information for the remaining orders up to and including fourteen. Many of the properties presented in the results of Chapter 6 will be defined in this chapter.

5.1. Basic definitions

Definition 5.1. A left neofield \((N, +, \cdot)\) comprises a set \(N\) of elements on which two binary operations \((+\) and \((\cdot)\) are defined such that \((N, +)\) is a loop with identity element 0 say, \((N\setminus\{0\}, \cdot)\) is a group and \((\cdot)\) distributes from the left over \((+\).

If a left neofield also satisfies the right distributive law, then it is simply called a neofield. Neofields were originally introduced by Paige [43] who hoped to use them to construct new finite projective planes. In this Paige was unsuccessful although many properties of neofields were discussed.

A left neofield which has a given group \((G, \cdot)\) as its multiplication group will be said to be based on that group. Neofields which are based on cyclic groups are called cyclic neofields. In particular all Galois fields are cyclic neofields in which addition forms an abelian group. We shall be primarily interested in the latin squares formed by the addition tables of finite left neofields.

The smallest left neofield, in which addition does not form a group, is based on the Klein 4-group \((C_2 \times C_2\) with generator set \((a, b)\). An example of one such addition table follows.
\[ \begin{array}{c|cccc} + & 0 & 1 & a & ab \\ \hline 0 & 0 & 1 & a & ab \\ 1 & 1 & 0 & b & ab & a \\ a & a & ab & 0 & 1 & b \\ b & b & a & ab & 0 & 1 \\ ab & ab & b & 1 & a & 0 \end{array} \]

fig. 5.1.

[Note that addition in the above left neofield is neither associative nor commutative.]

Since, in a left neofield, \( x + y = x(1 + x^{-1}y) \), \( \forall x \neq 0 \), it is evident that a left neofield based on a given group \((G, \cdot)\) is completely determined by its presentation function \( \psi \) defined by \( \psi(w) = 1 + w \). This was first pointed out in [32] and the fact that it is so has been used in [28] and [27]. The presentation function for the left neofield whose addition table is displayed in fig. 5.1 is given by:

\[
\psi = \begin{pmatrix}
0 & 1 & a & ab \\
1 & 0 & b & ab & a
\end{pmatrix}
\]

It will be shown that if a group \((G, \cdot)\) possesses a complete or a near complete mapping, then there exists a left neofield based on \((G, \cdot)\).

Throughout the present chapter, we shall assume that all complete and near complete mappings are in canonical form.

5.2. Generalised orthomorphisms, near orthomorphisms and left neofields.

In [27] Hsu and Keedwell generalise the concepts of complete and near complete mappings, partly in order to characterise left neofields. As the authors themselves acknowledge (see [12], pp. 41-42) these generalisations, which were named \((K, \lambda)\) complete and \((K, \lambda)\) near complete mappings in [27] ought to have been called \((K, \lambda)\) orthomorphisms and \((K, \lambda)\) near orthomorphisms respectively.
We will adopt the latter terminology.

**Definition 5.2.** Let \((G, \cdot)\) be a group of order \(n\). A \((K, \lambda)\) orthomorphism of \((G, \cdot)\), where \(K = (k_1, k_2, \ldots, k_s)\) and the \(k_j\) are integers such that \(\sum_{j=1}^{s} k_j = \lambda(n - 1)\), is an arrangement of the non-identity elements of \(G\) (each used \(\lambda\) times) into \(s\) cyclic sequences of lengths \(k_1, k_2, \ldots, k_s\), say

\[
(g_{11} g_{12} \cdots g_{1k_1})(g_{21} g_{22} \cdots g_{2k_2}) \cdots (g_{s1} g_{s2} \cdots g_{sk_s})
\]

such that the elements \(g_{ij}^{-1}g_{i+j+1}\) together with the elements \(g_{1r}^{-1}g_{1+i}\), comprise the non-identity elements of \(G\) each counted \(\lambda\) times.

**Definition 5.3.** Let \((G, \cdot)\) be a group of order \(n\). A \((K, \lambda)\) near orthomorphism of \((G, \cdot)\), where \(K = (h_1, h_2, \ldots, h_r, k_1, k_2, \ldots, k_s)\) and the \(h_i\) and \(k_j\) are integers such that \(\sum_{i=1}^{r} h_i + \sum_{j=1}^{s} k_j = \lambda n\), is an arrangement of the elements of \(G\) (each used \(\lambda\) times) into \(r\) sequences with lengths \(h_1, h_2, \ldots, h_r\) and \(s\) cyclic sequences with lengths \(k_1, k_2, \ldots, k_s\), say

\[
[g_{11}' g_{12}' \cdots g_{1h_1}']['g_{11} g_{12} \cdots g_{1k_1})(g_{21} g_{22} \cdots g_{2k_2}) \cdots (g_{s1} g_{s2} \cdots g_{sk_s})
\]

such that the elements \((g_{ij}')^{-1}g_{i+j+1}'\) together with the elements \(g_{1r}^{-1}g_{1+i}\), comprise the non-identity elements of \(G\) each counted \(\lambda\) times. [Note that since \(\sum_{i=1}^{r} (h_i - 1) + \sum_{j=1}^{s} k_j = \lambda(n - 1)\), we have that \(r = \lambda\).]

The fact that the above definitions are a generalisation of the concepts of orthomorphism and near orthomorphism respectively is evident from the following theorem.

**Theorem 5.1.** (i) A \((K, 1)\) orthomorphism of a group \((G, \cdot)\) is equivalent to an orthomorphism of \((G, \cdot)\) in canonical form.

(ii) A \((K, 1)\) near orthomorphism of a group \((G, \cdot)\) is equivalent to a near orthomorphism of \((G, \cdot)\).
Proof. (i) Let \((g_{11} \, g_{12} \, \ldots \, g_{1k_1})(g_{21} \, g_{22} \, \ldots \, g_{2k_2}) \cdots (g_{n1} \, g_{n2} \, \ldots \, g_{nk_n})\) be a \((K, 1)\) orthomorphism of a group \((G, \cdot)\). Define \(\phi(1) = 1, \phi(g_{i1}) = g_{i,i+1}\) and \(\phi(g_{i1}) = g_{i1}\). Then \(\phi\) is an orthomorphism of \((G, \cdot)\) in canonical form.

Conversely, let \(x \rightarrow \phi(x)\) be the canonical form of an orthomorphism of \((G, \cdot)\). We suppose that the elements of \(G\) are \(g_1, g_2, \ldots, g_n\). Since \(\phi(1) = 1\), it follows that \(\phi(g_2) = g_2^{-1}\phi(g_2) \neq 1\) and so \(\phi(g_2) = g_3 \neq g_2\). Then \(\phi(g_2)\phi(g_3) = g_2^{-1}\phi(g_3)\). Let \(\phi(g_2) = g_4 \neq g_3\) since \(\phi(g_2) = g_3\). We have \(\phi(g_3) \neq g_2\) unless \(\phi(g_2)\phi(g_3) = 1\). If \(\phi(g_2)\phi(g_3) = 1\), then \((g_2, g_3)\) forms one cyclic sequence of the generalised orthomorphism. If not, we have \(\phi(g_2)\phi(g_3)\phi(g_4) = g_2^{-1}\phi(g_4)\) and let \(\phi(g_4) = g_5\). We repeat this process until, eventually, we obtain a product \(\phi(g_2)\phi(g_3)\phi(g_4) \cdots \phi(g_n) = 1\) and a corresponding cyclic sequence \((g_1, g_2, \ldots, g_n)\) of the generalised orthomorphism. Taking \(g_s\) distinct from the members of this cyclic sequence we have \(\phi(g_s) = g_s^{-1}\phi(g_s) \neq 1\) and so \(\phi(g_s) = g_{s+1} \neq g_s\) and not equal to any member of the previously constructed cyclic sequence because \(\phi\) is a bijection of \(G\). By repetition of the above argument we eventually separate the non-identity elements of \(G\) into disjoint cyclic sequences which form a \((K, 1)\) orthomorphism.

(ii) Let \([g_1' \, g_2' \, \ldots \, g_{n'}')(g_{11} \, g_{12} \, \ldots \, g_{1k_1}) \cdots (g_{n1} \, g_{n2} \, \ldots \, g_{nk_n})\) be a \((K, 1)\) near orthomorphism of a group \((G, \cdot)\). Define \(\phi(g_{i1}') = g_{i,i+1}', \phi(g_{i1}') = g_{i1,i+1}'\) and \(\phi(g_{i1}') = g_{i1}\) (note that \(g_{i1}'\) has no image). Then \(\phi\) is a near orthomorphism of \((G, \cdot)\) from \(G\{g_{i1}'\}\) onto \(G\{g_{i1}'\}\).

Conversely, let \(x \rightarrow \phi(x)\) be a near orthomorphism of \((G, \cdot)\) in which the element \(g_1\) has no preimage and the element \(g_h\) has no image. We suppose that the elements of \(G\) are \(g_1, g_2, \ldots, g_n\). Then \(\phi(g_1) = g_2 \neq g_1\). If \(g_2 = g_h\), then \([g_1, g_2]\) is the sequence in the generalised near orthomorphism. Otherwise we have \(\phi(g_2) = g_3 \notin (g_1, g_2)\). Since \(G\) is finite and \(g_1\) has no preimage under \(\phi\), repetition of this process will eventually lead to an element \(g_{h-1}\) such that \(\phi(g_{h-1}) = g_h\). We then take \([g_1, g_2, \ldots, g_{h-1}, g_h]\) to be the sequence of the generalised near orthomorphism. If the elements of the sequence do not exhaust the elements of \(G\),
then we may take $g_x$ distinct from the members of this sequence and construct cyclic sequences, in a way analogous to that used to complete the proof of part (i), to form a $(K, 1)$ near orthomorphism. □

Part (i) of the above theorem appeared in [27]. Note, however, that part (ii) of the above theorem is in contradiction to a remark made at the end of Chapter 2 in [12] which states that Hsu's definition of a near orthomorphism in [26] is different to that of a $(K, 1)$ near orthomorphism.

We now describe the relationships between $(K, 1)$ orthomorphisms, $(K, 1)$ near orthomorphisms and left neofields. From [27] we have the following three theorems.

**Theorem 5.2.** Let $(G, \cdot)$ be a finite group with identity element denoted by 1 which possesses a $(K, 1)$ orthomorphism and let $x \to \theta(x)$ be the corresponding complete mapping in canonical form whose existence is guaranteed by Theorem 5.1. Let 0 be a symbol not in the set $G$ and define $N = G \cup \{0\}$. Then $(N \setminus \{0\}, \cdot)$ is the given group $(G, \cdot)$ and we can define a second operation $(\circ)$ on $N$ by the statements $1 + z = z\theta(z)$ for all $z \in N \setminus \{0, 1\}$, $1 + 1 = 0$, $z + 0 = 0 + z = z$ for all $z \in N$ and $x + y = x(1 + x^{-1}y)$ whenever $x$ and $y$ are non-zero. If we also define $0 \cdot x = x \cdot 0 = 0$ for all $x \in N$, then $(N, +, \cdot)$ is a left neofield.

**Proof.** We need to show that $(N, +)$ is a loop with identity element 0 and that multiplication is left distributive over addition.

We first show that the addition table forms a latin square. Since $1 + z = z\theta(z) = \phi(z)$ for all $z \neq 0, 1$, and since $\phi$ is a bijection of $G$ with $\phi(1) = 1$ (because $\theta$ is a complete mapping in canonical form) the elements $1 + z$ are all distinct. Consequently, for $x \neq 0$, the elements $x + y = x(1 + x^{-1}y)$ as $y$ varies are all distinct. Thus the entries in each of the rows of the Cayley table of $(N, +)$ are all different.
Similarly for columns we have that for \( x, y \) non-zero, \( x \neq y, x + y = x(1 + x^{-1}y) = x \cdot x^{-1}y \cdot (x^{-1}y) = y \cdot (x^{-1}y) \), and since \( y + y = 0, 0 + y = y \), the elements \( x + y \) as \( x \) varies are all distinct. So the entries in each of the columns of the Cayley table of \((N, +)\) are all different.

The left distributivity of multiplication over addition follows immediately from the definition \( x + y = x(1 + x^{-1}y) \), for we have

\[
tu + tv = tu[1 + (tu)^{-1}tv] = tu(1 + u^{-1}v) = tu(1 + u^{-1}v) = t(u + v).
\]

The element 0 acts as identity for \((+\)) so \((N, +)\) is a loop. This completes the proof. \(\square\)

**Theorem 5.3.** Let \((G, \cdot)\) be a finite group which possesses a \((K, 1)\) near orthomorphism such that \( K = \langle h; k_1, k_2, \ldots, k_s \rangle \). Then there exists a left neofield \((N, +, \cdot)\) whose multiplicative group is \((G, \cdot)\).

**Proof.** Let the \((K, 1)\) near orthomorphism be as follows:

\[
[g_1', g_2', \ldots, g_h'](g_{11}, g_{12}, \ldots, g_{18}), \ldots, (g_{m1}, g_{m2}, \ldots, g_{mh})
\]

We define a \( \theta \) mapping \( G \) onto itself by the statements \( \theta(g_i) = g_i^{-1}g_{i+1} \) for \( i = 1, 2, \ldots, h - 1; \theta(g_{h}) = g_{h}^{-1}g_{1+1} \) for \( l = 1, 2, \ldots, s \), where the second suffix \( j \) is added modulo \( k_j \). Then, by definition of a near complete mapping, \( \theta \) maps \( G \setminus \{g_h'\} \) one to one onto \( G \setminus \{1\} \), where 1 denotes the identity element of \((G, \cdot)\).

Let 0 be a symbol not in the set \( G \) and define \( N = G \cup \{0\} \). Then \((N \setminus \{0\}, \cdot)\) is the given group \((G, \cdot)\) and we can define a second operation \((+\)) on \( N \) by the statements \( 1 + x = x\theta(x) \) for all \( x \in N \setminus \{0, g_h'\}, 1 + g_h' = 0, z + 0 = z = 0 + z \) for all \( z \in N, x + y = x(1 + x^{-1}y) \) whenever \( x \) and \( y \) are non-zero. We also define \( 0 \cdot x = 0 = x \cdot 0 \) for all \( x \in N \).

Since \( 1 + 0 = 1 = g_1'; 1 + g_i' = g_{i+1}' \) for \( i = 1, 2, \ldots, h - 1; 1 + g_h' = 0; \)
1 + \varepsilon_{ij} = \varepsilon_{i,j+1} \text{ for } i = 1, 2, \ldots, s \text{ where the second suffix } j \text{ is added modulo } k, \text{ it follows that the elements } 1 + z \text{ are all distinct. Consequently, for } x \neq 0, \text{ the elements } x + y = x(1 + x^{-1}y) \text{ as } y \text{ varies are all distinct. So the entries in each of the rows of the Cayley table of } (N, +) \text{ are all different.}

Since } x + y = x(1 + x^{-1}y) = y \cdot \theta(x^{-1}y) \neq y \text{ if } x \text{ and } y \text{ are not zero and } \neq 0 \text{ unless } x^{-1}y = \varepsilon_i \text{ and }, \text{ since } 0 + y = y, \text{ the elements } x + y \text{ as } x \text{ varies are all distinct. So the elements in each of the columns of the Cayley table of } (N, +) \text{ are all different.}

The remainder of the proof is exactly similar to that of Theorem 5.2. □

**Theorem 5.4.** Let \((A, T, +, \cdot)\) be a left neofield with multiplicative group \((G, \cdot)\) where \(G = N \setminus \{0\}. \) Then, if \(1 + 1 = 0, \) \((A, T, +, \cdot)\) defines a \((K, 1)\) orthomorphism of \((G, \cdot)\). If \(1 + 1 \neq 0, \) \((A, T, +, \cdot)\) defines a \((K, 1)\) near orthomorphism of \((G, \cdot).\)

**Proof.** Let \(Q: z \rightarrow 1 + z\) be the permutation of \(N\) induced by the presentation function of \((N, +, \cdot).\) If \(1 + 1 = 0, \) then \(Q\) takes the form

\[
Q = (0 1)(g_{11} g_{12} \cdots g_{1k_1}) \cdots (g_{s1} g_{s2} \cdots g_{sk_2})
\]

when written as a product of cycles, where \(1 + g_{hi} = g_{hi+1}. \) Define \(\theta(g_{hi}) = g_{hi}^{-1}g_{hi+1} \) and \(\theta(1) = 1. \) Then we claim that \((g_{11} g_{12} \cdots g_{1k_1}) \cdots (g_{s1} g_{s2} \cdots g_{sk_2})\) is a \((K, 1)\) orthomorphism of \((G, \cdot).\) Since \(\phi(g_{hi}) = g_{hi} \cdot \phi(g_{hi}) = g_{hi+1}, \) it is sufficient to prove that \(\theta(g_{hi}) \neq \theta(g_{ij}) \) unless \(g_{hi} = g_{ij}.\)

We have

\[
\theta(g_{hi}) = \theta(g_{ij}) \Rightarrow g_{hi}^{-1}(1 + g_{hi}) = g_{ij}^{-1}(1 + g_{ij})
\]

\[
\Rightarrow g_{hi}^{-1} + 1 = g_{ij}^{-1} + 1 \Rightarrow g_{hi} = g_{ij}
\]

since multiplication is left distributive over addition and addition forms a loop.
If $1 + 1 \neq 0$, then $Q$ takes the form

$$Q = [0 \ 1 \ g'_2 \ \cdots \ g'_h](g_{11} \ g_{12} \ \cdots \ g_{1h} \cdots \ (g_{s1} \ g_{s2} \ \cdots \ g_{sh})$$

where $1 + 1 = g'_2$ and $1 + g'_h = 0$. Then

$$[g'_1 \ g'_2 \ \cdots \ g'_h](g_{11} \ g_{12} \ \cdots \ g_{1h} \cdots \ (g_{s1} \ g_{s2} \ \cdots \ g_{sh})$$

is a $(K, 1)$ near orthomorphism of $(G, \cdot)$. We define $\theta(g_h) = g_{h(i+1)}^{-1}g_{h(i+1)}$ as before and $\theta(1) = g'_2, \theta(g'_i) = g_{i+1}^{-1}g_{i+1}$ for $i = 1, 2, \ldots, h - 1$. An argument exactly similar to the above shows that $\theta$ is a one to one mapping from $G \setminus g'_h$ onto $G \setminus (1)$ so we have a $(K, 1)$ near complete mapping. □

We may conveniently summarise the above three theorems in the following two statements, which we will refer to in later chapters.

Statement 1. The permutation $(g_{11} \ g_{12} \ \cdots \ g_{1h})(g_{21} \ g_{22} \ \cdots \ g_{2h}) \cdots \ (g_{s1} \ g_{s2} \ \cdots \ g_{sh})$ is a $(K, 1)$ orthomorphism of $(G, \cdot)$ if and only if the permutation

$$\psi = (0 \ 1)(g_{11} \ g_{12} \ \cdots \ g_{1h})(g_{21} \ g_{22} \ \cdots \ g_{2h}) \cdots \ (g_{s1} \ g_{s2} \ \cdots \ g_{sh})$$

is the presentation function for a left neofield based on $(G, \cdot)$.

Statement 2. The mapping $[1 \ g'_2 \ \cdots \ g'_h](g_{11} \ g_{12} \ \cdots \ g_{1h}) \cdots \ (g_{s1} \ g_{s2} \ \cdots \ g_{sh})$ is a $(K, 1)$ near orthomorphism of $(G, \cdot)$ if and only if the permutation

$$\psi = (0 \ 1 \ g'_2 \ \cdots \ g'_h)(g_{11} \ g_{12} \ \cdots \ g_{1h}) \cdots \ (g_{s1} \ g_{s2} \ \cdots \ g_{sh})$$

is the presentation function for a left neofield based on $(G, \cdot)$.

Now consider the following addition table, where the $g_i, \ 1 \leq i \leq n, \ g_1 = 1$, are the elements of some group $(G, \cdot)$, $0$ is an additional element and in which the remaining rows are completed by using the fact that $x + y = x(1 + x^{-1}y), \forall \ x \neq 0$. 
Then statements 1 and 2 imply the following result, which will give a more convenient method for constructing left neofields.

**Theorem 5.5.** The table displayed in fig. 5.2 forms the addition table of some left neofield \((N', +, \cdot)\) if and only if the set of elements \((1 + g_i)^{-1} g_i, 1 \leq i \leq n, 1 + g_i \neq 0,\) exhausts the set \(G \setminus \{1\} .\)

**Proof.** Suppose fig. 5.2 forms the addition table of some left neofield. Then \((1 + g_i)^{-1} g_i = \psi(g_i) = \theta(g_i)\) if \(g_i \neq 0\) and \(1 + g_i \neq 0,\) where \(\theta(g_i)\) is either a complete or a near complete mapping of \((G, \cdot)\). Also \(\psi(g_i) 
eq g_i\) since fig. 5.2 must form a latin square. Now, by definition of \(\theta,\) the set of elements \(\theta(g_i),\) where \(g_i\) is such that \(1 + g_i \neq 0,\) exhausts the set \(G \setminus \{1\} .\) Thus so do the elements \(\theta(g_i)^{-1}.\)

Conversely, suppose that \(1 + x\) is defined as in fig. 5.2 and that the set of elements \((1 + g_i)^{-1} g_i, 1 \leq i \leq n, 1 + g_i \neq 0,\) exhausts the set of elements \(G \setminus \{1\} .\) We can define a mapping \(\theta: g_i \mapsto g_i^{-1}(1 + g_i), 1 \leq i \leq n, 1 + g_i \neq 0,\) such that \(\theta\) is a near complete mapping of \((G, \cdot)\) if \(1 + 1 \neq 0,\) or a complete mapping of \((G, \cdot)\), with \(\theta(1) = 1,\) if \(1 + 1 = 0,\) and hence obtain a left neofield. □

5.3. Isomorphisms of left neofields

We now examine the conditions under which two left neofields are isomorphic.

**Theorem 5.6.** Two left neofields \((N, +, \cdot)\) and \((N', \circ, \cdot),\) each based on the same group \((G, \cdot),\) where \(N = G \cup \{0\}\) and \(N' = G \cup \{0\},\) are isomorphic if and only if
\[ \psi' = \alpha \psi \alpha^{-1}, \] where \( \alpha \in \text{aut} (G, \cdot) \), extended by the requirement that \( \alpha(0) = 0' \), and \( \psi \) and \( \psi' \) are the presentation functions of \((N, +, \cdot)\) and \((N', \circ, \cdot)\) respectively.

**Proof.** Let \( 1 + \eta = 0 \) in \((N, +, \cdot)\) and \( 1 \circ \eta' = 0' \) in \((N', \circ, \cdot)\). [If \((N, +, \cdot)\) defines a near complete mapping \( \theta \) of \((G, \cdot)\), then \( \eta \) is the exdomain element of \( \theta \). If, however, \((N, +, \cdot)\) defines a complete mapping, then \( \eta = 1 \).]

Suppose that \((N, +, \cdot)\) and \((N', \circ, \cdot)\) are isomorphic with \( \alpha: z \rightarrow z' \). By definition \( \psi(z) = 1 + z \) in \((N, +, \cdot)\) and \( \psi'(z) = 1 \circ z \) in \((N', \circ, \cdot)\). Then
\[
\alpha \psi(z) = \alpha(1 + z) = \alpha(1) \circ \alpha(z) = 1 \circ \alpha(z) = \psi'(z).
\]
Thus \( \alpha \psi = \psi' \alpha \) and so \( \psi' = \alpha \psi \alpha^{-1} \).

If we regard the isomorphic multiplication groups of \((N, +, \cdot)\) and \((N', \circ, \cdot)\) as being the same, then \( \alpha \) is an automorphism of this group, extended by the requirement that \( \alpha(0) = 0' \).

Conversely, suppose that there exists an automorphism \( \alpha \) of \((G, \cdot)\) such that \( \psi' = \alpha \psi \alpha^{-1} \). We show that the map defined by \( \alpha: z \rightarrow \alpha(z), \forall z \in G \) and \( \alpha(0) = 0' \), defines an isomorphism between \((N, +, \cdot)\) and \((N', \circ, \cdot)\), where \( N = G \cup \{0\} \) and \( N' = G' \cup \{0'\} \).

Now \( \alpha \) is a bijection from \( N \) to \( N' \) by definition. Also \( \alpha(z_1 z_2) = \alpha(z_1) \alpha(z_2) \) since \( \alpha \) is an automorphism of \((G, \cdot)\). [Note that this identity also holds if \( z_1 \) or \( z_2 = 0 \) since \( \alpha(0) = 0' \).]

\[
\therefore \alpha(z_1 + z_2) = \alpha[z_1(1 + z_1^{-1}z_2)] = \alpha(z_1) \alpha(1 + z_1^{-1}z_2) \text{ for } z_1 \neq 0,
\]
\[
= \alpha(z_1) \alpha \psi(z_1^{-1}z_2) = \alpha(z_1) \psi' \alpha(z_1^{-1}z_2) \text{ since } \alpha \psi = \psi' \alpha,
\]
\[
= \alpha(z_1) \psi'[\alpha(z_1)^{-1} \alpha(z_2)] \text{ since } \alpha(z_1^{-1}) = \alpha(z_1)^{-1},
\]
\[
\alpha(z_1)[1 \circ \alpha(z_1)^{-1} \alpha(z_2)] = \alpha(z_1) \circ \alpha(z_2).
\]

For the case \( z_1 = 0 \) we have \( \alpha(z_1 + z_2) = \alpha(z_2) = z_2' \) and \( \alpha(z_1) \circ \alpha(z_2) = 0' \circ z_2' = z_2' \) since \( \alpha(0) = 0' \).
Therefore the presentation functions of two left neofields, based on the same group \((G, \cdot)\), must be conjugate with respect to some \(\alpha \in \text{aut}(G, \cdot)\) if the left neofields they generate are isomorphic. □

The above theorem leads us on to the following interesting fact.

**Theorem 5.7.** The number of distinct isomorphs of a specific left neofield \((N, +, \cdot)\) based on a given group \((G, \cdot)\), divides the order of \(\text{aut}(G, \cdot)\).

**Proof.** The presentation functions are permutations of \(N\) and so belong to the symmetric group \(S_N\). By Theorem 5.6, two presentation functions define left neofields which are isomorphic if and only if they belong to the same conjugacy class with respect to \(\text{aut}(G, \cdot)\) in \(S_N\). But any such conjugacy class has cardinal which divides \(|\text{aut}(G, \cdot)|\) since two conjugates of the presentation function \(\psi\) of \((N, +, \cdot)\), say \(\alpha_1 \psi \alpha_1^{-1}\) and \(\alpha_2 \psi \alpha_2^{-1}\), are equal if and only if \(\alpha_1 \psi \alpha_2 \psi\) commutes with \(\psi\), which happens if and only if \(\alpha_1^{-1} \alpha_2 \in N(\psi) \cap \text{aut}(G, \cdot)\) (where \(N(\psi)\) is the normaliser of \(\psi\) in \(S_N\)), which happens if and only if \(\alpha_1\) and \(\alpha_2\) belong to the same coset of the subgroup \((H, \cdot) = N(\psi) \cap \text{aut}(G, \cdot)\) of \(\text{aut}(G, \cdot)\). Therefore the number of distinct isomorphs of \((N, +, \cdot)\) is the index of \((H, \cdot)\) in \(\text{aut}(G, \cdot)\) and thus divides \(|\text{aut}(G, \cdot)|\). □

When an isomorphism class has only one member we will say that all isomorphs of that member coincide.

**Corollary.** All isomorphs of a left neofield based on \((G, \cdot)\), with presentation function \(\psi\) coincide if and only if \(\text{aut}(G, \cdot) \subseteq N(\psi)\).

**Proof.** If and only if all isomorphs of a given group \((G, \cdot)\) coincide we have \(N(\psi) \cap \text{aut}(G, \cdot) = \text{aut}(G, \cdot) \Rightarrow \text{aut}(G, \cdot) \subseteq N(\psi)\). □
5.4. Some properties of left neofields which are preserved under isomorphism

We now discuss some of the properties of left neofields which are preserved under isomorphism.

Definition 5.4. A left neofield \( (N, +, \cdot) \) for which \( 1 + 1 \neq 0 \) and for which the presentation function \( \psi \) defines a permutation of \( N \) which consists entirely of cycles of length \( k \) is said to be a left neofield of characteristic \( k \).

Definition 5.5. A left neofield \( (N, +, \cdot) \) for which \( 1 + 1 = 0 \) and for which the presentation function \( \psi \) defines a permutation of \( N \setminus \{0, 1\} \) which consists entirely of cycles of length \( k \) is said to be a left neofield of pseudo-characteristic \( k \).

The concepts of characteristic and pseudo-characteristic of a left neofield were first introduced in [27]. [The concept of characteristic for a neofield was introduced earlier in [32].]

We note that if \( \alpha \) is an isomorphic mapping of a left neofield \( (N, +, \cdot) \) to \( (N', +', \cdot') \), then it preserves characteristic and pseudo-characteristic since, if we write the presentation function of \( (N, +, \cdot) \) as a product of disjoint cycles, then \( \alpha \) will map these cycles onto cycles of the same length. For a left neofield possessing pseudo-characteristic we also require the observation that \( (0, 1) \) will be mapped onto \( (0', 1') \).

A left neofield based on a group of order \( n \) can have characteristic of at most \( n + 1 \) and a pseudo-characteristic of at most \( n - 1 \). Hsu and Keedwell showed that these maximum values are related to the following group properties.

Definition 5.6. A finite group \( (G, \cdot) \) of order \( n \) is said to be sequenceable if its elements can be ordered in a sequence, \( a_1 = 1, a_2, a_3, \ldots, a_n \), such that all of the partial products \( b_1 = 1, b_2 = a_1a_2, b_3 = a_1a_2a_3, \ldots, b_n = a_1a_2a_3\cdots a_n \) are different.
Definition 5.7. A finite group \((G, \cdot)\) of order \(n\) is said to be \(R\)-sequenceable if its elements can be ordered in a sequence, \(a_1, a_2, a_3, \ldots, a_n\), such that all of the partial products \(b_1 = 1, b_2 = a_1a_2, b_3 = a_1a_2a_3, \ldots, b_{n-1} = a_1a_2a_3\cdots a_{n-1}\) are different and so that the product \(b_n = a_1a_2a_3\cdots a_n = 1\).

The following theorem appears in [27].

Theorem 5.8. Let \((G, \cdot)\) be a finite group of order \(n\). Then

(i) \((G, \cdot)\) is \(R\)-sequenceable if and only if it possesses a \(((n-1), 1)\) orthomorphism.

(ii) \((G, \cdot)\) is sequenceable if and only if it possesses an \(((n), 1)\) near orthomorphism.

Proof. (i) Suppose that \(c_1, c_2, \ldots, c_n\) is the cyclic sequence which defines a \(((n-1), 1)\) orthomorphism of \((G, \cdot)\). Define \(\theta(1) = 1, \theta(c_i) = c_i^{-1}c_{i+1} = a_{i+1}\) for \(i = 2, 3, \ldots, n-1\) and \(\theta(c_n) = c_n^{-1}c_2 = a_2\). Then \(\theta\) is a bijection of \(G\) by definition of a \(((n-1), 1)\) orthomorphism. Also \(b_1 = a_1 = 1, b_2 = a_1a_2 = c_2^{-1}c_2, b_3 = a_1a_2a_3 = c_3^{-1}c_3, b_4 = c_4^{-1}c_4, \ldots, b_{n-1} = c_{n-1}^{-1}c_{n-1}\) are all different and \(b_n = a_1a_2a_3\cdots a_n = c_n^{-1}c_n = 1\), so \((G, \cdot)\) is \(R\)-sequenceable.

Conversely, if \((G, \cdot)\) is \(R\)-sequenceable and if, with the notation of Definition 5.7, \(c\) is the element which does not occur amongst the distinct partial products \(b_1 = 1, b_2, \ldots, b_{n-1}\), then the elements \(c^{-1}, c^{-1}b_2, c^{-1}b_3, \ldots, c^{-1}b_{n-1}\) are the non-identity elements of \(G\) and form a cyclic sequence to define a \(((n-1), 1)\) orthomorphism of \((G, \cdot)\).

(ii) Suppose that \([c_1, c_2, c_3, \ldots, c_n]\) is the sequence which defines an \(((n), 1)\) near orthomorphism of \((G, \cdot)\). Define \(a_1 = 1, a_i = c_{i-1}^{-1}c_i\) for \(i = 2, 3, \ldots, n\). Then the \(a_i\)'s are all different by definition of a near complete mapping and the partial products \(b_1 = a_1 = 1, b_2 = a_1a_2 = c_2^{-1}c_2, b_3 = a_1a_2a_3 = c_3^{-1}c_3, \ldots, b_n = c_1^{-1}c_n\) are all different and so \((G, \cdot)\) is sequenceable.

Conversely, suppose that \((G, \cdot)\) is sequenceable with sequencing \(a_1 = 1,\)
\(a_2, a_3, \ldots, a_n\) and partial products \(b_1 = a_1 = 1, b_2 = a_1a_2, b_3 = a_1a_2a_3, \ldots, b_n = a_1a_2a_3\cdots a_n\). Then the sequence \([b_1, b_2, \ldots, b_n]\) defines an \((n, 1)\) near orthomorphism of \((G, \cdot)\). \(\square\)

By way of example, the left neofield based on \(C_2 \times C_2\) defined by the addition table in fig. 5.1, has maximum pseudo-characteristic three. The corresponding R-sequencing of \(C_2 \times C_2\) is given by: 1, \(ab, a, b\), which has the partial products 1, \(ab, a, b\). In general we may talk about the permutation of \(N\) induced by the presentation function of \((N, +, \cdot)\) and the \((K, 1)\) orthomorphism or near orthomorphism which defines \((N, +, \cdot)\).

From the statements immediately following Theorem 5.4 we see that a \((K, 1)\) orthomorphism of a group \((G, \cdot)\) defines a left neofield whose presentation function \(\psi\) induces a permutation of \(N\) of the form \((0 1)(\xi_1 \xi_2 \cdots \xi_{k_1}) \cdots (\xi_{k_1} \xi_{k_2} \cdots \xi_{k_2})\). Hence, if \(K = (k, k, \ldots, k)\), then \((N, +, \cdot)\) has pseudo-characteristic \(k\).

Similarly, a \((K, 1)\) near orthomorphism of a group \((G, \cdot)\) defines a left neofield whose presentation function \(\psi\) induces a permutation of \(N\) of the form \((0 1 \xi'_1 \cdots \xi'_{k})(\xi_{k_1} \xi_{k_2} \cdots \xi_{k_2}) \cdots (\xi_{k_1} \xi_{k_2} \cdots \xi_{k_2})\). Hence, if \(K = (k-1; k, \ldots, k)\), then \((N, +, \cdot)\) has characteristic \(k\).

We observe that, if \(\alpha\) is an isomorphism of \((N, +, \cdot)\), with isomorphic image \((N', \Theta, \cdot)\), then the permutation induced on \(N'\) by the presentation function \(\psi'\) of \((N', \Theta, \cdot)\) will have the same structure as the permutation induced on \(N\) by the presentation function \(\psi\) of \((N, +, \cdot)\). It follows immediately that both the properties of characteristic and pseudo-characteristic of a left neofield are preserved under isomorphism. [Again the above facts were first stated in [27].]
5.5. Main classes of addition tables

We now determine in what way, if any, the main class transformations, when applied to addition tables, preserve the left neofield structure. Let \((N, +, \cdot)\) be a left neofield based on a group \((G, \cdot)\) of order \(n\). We will consider the addition table of \((N, +, \cdot)\) to be defined by the \(OA(n+1, 3)\) in which the column \((g_i, g_j, g_k)^\prime\) will be interpreted to imply \(g_i + g_j = g_k\).

The main class transformations are then:

(1) apply the ordered triple of permutations \(T = (a, \beta, \gamma)\) to the elements in the rows of the \(OA(n+1, 3)\). That is \(T(g_i, g_j, g_k)^\prime \rightarrow (\alpha(g_i), \beta(g_j), \gamma(g_k))^\prime\).

(2) permute the rows of the \(OA(n+1, 3)\), using an element from the group \(S_3\).

For (1), if \(a = \beta = \gamma\), then, by Theorem 5.6, left neofield structure is preserved, if and only if \(a \in \text{aut} (G, \cdot)\).

For (2), first we note that it is sufficient to consider the permutations \((1 2)(3)\) and \((1 3)(2)\) since these permutations generate \(S_3\). The permutation \((1 2)(3)\) corresponds to taking the transpose of the addition table for \((N, +, \cdot)\). We have the following theorem.

**Theorem 5.9.** Let \((N, +, \cdot)\) be a left neofield based on \((G, \cdot)\), with addition table defined as in fig. 5.2, and consider the table formed when we transpose fig. 5.2. Then this table also forms the addition table of some left neofield \((N, @, \cdot)\) based on \((G, \cdot)\).

**Proof.** By Theorem 5.5 and the fact that \((N, +, \cdot)\) is a left neofield based on \((G, \cdot)\), we must have that the elements \((1 + g_i)^{-1}g_p\), \(1 \leq i \leq n, g_i \neq 0, \eta\), where \(1 + \eta = 0\), exhaust the set \(G \setminus \{1\}\). We are first required to show that the elements \((1 @ g_i)^{-1}g_p\), \(1 \leq i \leq n, g_i \neq 0, \eta^*\), also exhaust \(G \setminus \{1\}\), where \(\eta^* \in G\) is such that \(1 @ \eta^* = 0\). But \(1 @ g_i = g_i + 1\) so \(1 @ g_i = 0 \implies g_i + 1 = 0 \implies g_i(1 + g_i^{-1}) = 0 \implies g_i^{-1} = \eta \implies \eta^* = \eta^{-1}.\)
Similarly \((1 \oplus g_t)^{-1}g_t = (g_t + 1)^{-1}g_t = \left[g_t(1 + g_t^{-1})\right]^{-1}g_t = (1 + g_t^{-1})^{-1} = \psi(g_t^{-1}), \ g_t \neq 0, \eta^{-1}\).

But since \(\psi(g_t), \ g_t \neq 0, \eta\), exhausts \(G \setminus \{1\}\), then \(\psi(g_t^{-1}), \ g_t \neq 0, \eta^{-1}\), exhausts \(G \setminus \{1\}\).

Thus \(\psi^*(g_t) = 1 \oplus g_t, \ \psi^*(0) = 1, \ \psi^*(\eta^{-1}) = 0\) is certainly a presentation function, but we need to show that its addition table is given by the transpose of fig. 5.2.

In the addition table for \((N, \oplus, \cdot)\) the \((j, k)\)th cell contains \(g_j \oplus g_k = g_j(1 \oplus g_j^{-1}g_k) = g_j(g_j^{-1}g_k + 1) = g_k + g_j\). Thus the transpose of fig. 5.2 is indeed the addition table for the left neofield whose presentation function is \(\psi^*\). \(\square\)

**Corollary.** Addition in a left neofield which defines a near complete mapping of a group of odd order is never commutative.

**Proof.** Addition in \((N, +, \cdot)\) is commutative if and only if \(\psi^*\) coincides with \(\psi\). This requires \(\eta^{-1} = \eta\) and so \(\eta^2 = 1\). Now if \(\eta \neq 1\), then \((G, \cdot)\) must have even order and, by Theorem 5.4, \((N, +, \cdot)\) defines a near complete mapping of \((G, \cdot)\). On the other hand, if \(\eta = 1\), then \((N, +, \cdot)\) defines a complete mapping of \((G, \cdot)\). \(\square\)

Next we consider the permutation \((1 \ 3) (2)\). This corresponds to interchanging the roles of rows and symbols. We have the following result.

**Theorem 5.10.** Let \((N, +, \cdot)\) be a left neofield based on \((G, \cdot)\), with addition table defined as in fig. 5.2. Consider the table formed when we interchange the roles of rows and symbols in fig. 5.2. Then this table can be bordered by the elements of \(N\) in such a way as to form the addition table of some left neofield \((N, \oplus, \cdot)\) based on \((G, \cdot)\).

**Proof.** We are required to show that \((N, \oplus, \cdot)\), where the operation \((\oplus)\) is defined by \(g_k \oplus g_j \eta^{-1} = g_i \Rightarrow g_i + g_j = g_k\), forms a left neofield based on \((G, \cdot)\).

Now,

\[
g_i + g_j = g_k \Rightarrow g_k \oplus g_j \eta^{-1} = g_i \tag{1}
\]

and \(\forall g \in N, \quad eg_i + eg_j = eg_k \Rightarrow eg_k \oplus eg_j \eta^{-1} = eg_i \tag{2}\)
From (1) we obtain
\[ g(g_k \oplus g_j\eta^{-1}) = gg_j \] (3)

But (2) and (3) imply \[ gg_k \oplus gg_j\eta^{-1} = g(g_k \oplus g_j\eta^{-1}) \] and so (\oplus) distributes from the left over (\oplus).

Furthermore, \[ g + 0 = g \Rightarrow g \oplus 0\eta^{-1} = g \Rightarrow g \oplus 0 = g, \forall g \text{ and } g + g\eta = g(1 + \eta) \]
\[ = 0 \Rightarrow 0 \oplus g = g, \forall g \in N. \] Thus 0 is a two sided identity for \oplus.

Finally, we observe that for any elements \( g_k, g_j \in N \) we have \( g_k \oplus g = g_j \)
\[ \Rightarrow g_j + g\eta^{-1} = g_k \] which has a unique solution for \( g\eta^{-1} \) in \( N \) since \((N, +)\) is a quasigroup. Therefore, the equation \( g_i \oplus g = g_k \) has a unique solution for \( g \) in \( N \)
(similarly for \( g \oplus g_i = g_j \)). It follows that \((N, \oplus, \cdot)\) is a left neofield. \(\square\)
Chapter 6  Construction of M.O.L.S. Using Left Neofields

6.0. Introduction

We begin this chapter by investigating the conditions required for two left neofields to possess addition tables whose rows can be reordered so as to form orthogonal latin squares. We then present some computational results which exploit theorems presented in both this and the previous chapter.

6.1. Left neofields with orthogonal addition tables

Let the bordered latin squares $L_1$ and $L_2$, shown in fig. 6.1, represent the addition tables of two left neofields, based on the same group $(G, \cdot)$ of order $n$. We wish to obtain the conditions for the $(n + 1) \times (n + 1)$ latin squares $L_1$ and $L_2$ to be orthogonal. In fig. 6.1 the sets of elements \{x, x_1, x_2, \ldots, x_n\} and \{y, y_1, y_2, \ldots, y_n\} are two orderings of the set $N = G \cup \{0\}$.

\[
\begin{array}{c|cccc|c|cccc}
+ & 0 & 1 & g_2 & g_3 & \cdots & g_n & \oplus & 0 & 1 & g_2 & g_3 & \cdots & g_n \\
0 & 0 & 1 & g_2 & g_3 & \cdots & g_n & y & y & y_1 & y_2 & y_3 & \cdots & y_n \\
x & x_1 & x_2 & x_3 & \cdots & x_n & g_2 y & g_3 y & g_4 y & g_5 y & g_6 y & g_7 y & g_8 y & g_9 y \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x & g_n x \\
\end{array}
\]

Fig. 6.1.

We shall refer to the elements labelled $x$ and $y$ in $L_1$ and $L_2$ as the locational parameters of $L_1$ and $L_2$ respectively since they uniquely determine the order of the rows in each square.

Theorem 6.1. Let $L_1$ and $L_2$ be defined as in fig. 6.1, then they are orthogonal if the $n-2$ elements $d_i = x_i^{-1} y_i$, $1 \leq i \leq n$, where $x_i, y_i \neq 0$, exhaust the set $G \setminus \{1, x^{-1} y\}$.

Proof. Let $A$ be the array of ordered pairs formed when we juxtapose $L_1$ and $L_2$. 

We observe that all ordered pairs \([i, i]\) and \([ix, ly]\) occur in the zeroth row and zeroth column of \(A\) respectively.

We are required to show that:

1. The \((i, j)\)th cell never contains \([i, i]\) for \(i > 0\) or \([ix, ly]\) for \(j > 0\).

2. If the \((i, j)\)th and \((u, v)\)th cells both contain \([i, m]\), then \(i = u\) and \(j = v\).

Firstly, we suppose that the \((i, j)\)th cell does contain \([i, l]\) for some \(i > 0\), then we must have:

\[
g_i x + g_j = l \quad \text{and} \quad g_p y \oplus g_j = l
\]

\[
\Rightarrow g_i x + g_j = g_p y \oplus g_j
\]

\[
\Rightarrow g_i (x + g_i^{-1} g_j) = g_p (y \oplus g_i^{-1} g_j)
\]

\[
\Rightarrow (x + g_i^{-1} g_j)^{-1} (y \oplus g_i^{-1} g_j) = 1
\]

\[
\Rightarrow (x + g_k)^{-1} (y \oplus g_k) = 1, \text{ where } g_k = g_i^{-1} g_p
\]

\[
\Rightarrow x_k^{-1} y_k = 1, \text{ contrary to hypothesis.}
\]

Now suppose that the \((i, j)\)th cell contains \([ix, ly]\) for some \(i, j > 0\), then we must have:

\[
g_i x + g_j = ix \quad \text{and} \quad g_p y \oplus g_j = ly
\]

\[
\Rightarrow (g_i x + g_j)^{-1} (g_i y \oplus g_j) = x^{-1} y, \text{ since } l \neq 0,
\]

\[
\Rightarrow (x + g_i^{-1} g_j)^{-1} (y \oplus g_i^{-1} g_j) = x^{-1} y
\]

\[
\Rightarrow (x + g_k)^{-1} (y \oplus g_k) = x^{-1} y, \text{ where } g_k = g_i^{-1} g_p
\]

\[
\Rightarrow x_k^{-1} y_k = x^{-1} y, \text{ contrary to hypothesis.}
\]
Secondly, we suppose that both the $(i, j)$th and $(u, v)$th cells, $i, u \neq 0$, contain the ordered pair $[l, m]$, then

\[ g_i x + g_j = l \quad \text{and} \quad g_u y + g_v = m \]

from which we obtain:

\[ x + g_i^{-1} g_j = g_i^{-1} l \quad \text{(1)} \]

\[ y \oplus g_i^{-1} g_j = g_i^{-1} m \quad \text{(3)} \]

\[ x + g_u^{-1} g_v = g_u^{-1} l \quad \text{(2)} \]

\[ y \oplus g_u^{-1} g_v = g_u^{-1} m \quad \text{(4)} \]

**Remark.** In order to demonstrate that $i = u$ and $j = v$ we need only to show that $g_i^{-1} g_j = g_u^{-1} g_v$ since, by (1) and (2), $g_i^{-1} g_j = g_u^{-1} g_v \Rightarrow g_i^{-1} l = g_u^{-1} l$ and, by (3) and (4), $g_i^{-1} g_j = g_u^{-1} g_v \Rightarrow g_i^{-1} m = g_u^{-1} m$. Now $l$ and $m$ cannot both be $0$ since $i, u \neq 0$ and $[0, 0]$ occurs only in the $(0, 0)$th cell of $A$. Thus $g_i = g_u$ which implies that $g_j = g_v$ and so $i = u$ and $j = v$.

We now consider three separate cases.

If $l = 0$, then, by (1) and (2), we have

\[ x + g_i^{-1} g_j = x + g_u^{-1} g_v \]

Hence $g_i^{-1} g_j = g_u^{-1} g_v$ and so $i = u$ and $j = v$ by the above remark.

Similarly, if $m = 0$, then, by (3) and (4), we have

\[ y \oplus g_i^{-1} g_j = y \oplus g_u^{-1} g_v \]

which implies that $g_i^{-1} g_j = g_u^{-1} g_v$ and so $i = u$ and $j = v$ as before.

Finally, if $l, m \neq 0$, then

\[ (x + g_i^{-1} g_j)^{-1} (y \oplus g_i^{-1} g_j) = l^{-1} m, \text{ by (1) and (3)} \]

and 

\[ (x + g_u^{-1} g_v)^{-1} (y \oplus g_u^{-1} g_v) = l^{-1} m, \text{ by (2) and (4)} \]
Now let $g_i^{-1}g_j = g_k$ and $g_u^{-1}g_v = g_w$.

Then $x_i^{-1}y_k = x_v^{-1}y_w = t^{-1}m$ contrary to hypothesis unless $k = w$. If $k = w$, then $g_i^{-1}g_j = g_u^{-1}g_v$ and so $i = u$ and $j = v$ as before. □

If, in fig. 6.1, we have $x = 1$, then $L_1$ is in standard form and we obtain the following latin squares.

$$
\begin{array}{cccc}
0 & 1 & g_2 & g_3 & \cdots & g_n \\
0 & 1 & x_1 & x_2 & x_3 & \cdots & x_n \\
g_2 & g_2 & g_2 & g_3 & \cdots & g_n \\
g_3 & g_3 & g_3 & g_3 & \cdots & g_3 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
g_n & g_n & g_n & g_n & \cdots & g_n \\
\end{array}
\quad
\begin{array}{cccc}
0 & 1 & g_2 & g_3 & \cdots & g_n \\
y & y & y_1 & y_2 & y_3 & \cdots & y_n \\
\end{array}
$$

Corollary. $L_1$, as defined in fig. 6.2, is orthogonal to a latin square $L_2$, formed by a rearrangement of its own rows, excluding the first, if we have that for some $g \in G$ the set of elements $(1 + g_i)^{-1}(g + g_i), 1 \leq i \leq n, 1 + g_i \neq 0, g + g_i \neq 0$, exhausts the set $G \setminus \{1, g\}$.

Proof. This follows on setting $x = 1$ and $y = g$ and identifying the two operations $(\oplus)$ and $(\circ)$ in the above theorem. □

Theorem 6.2. Let $L_1$ and $L_2$ be orthogonal latin squares defined, as in fig. 6.2, such that $L_2$ is a rearrangement of the rows, excluding the first, of $L_1$, with $y (\neq 0)$ as locational parameter. Then $L_1$ is orthogonal to the latin square formed by a similar rearrangement of its own rows with $y^{-1}$ as locational parameter.

Proof. Since $L_1$ is the addition table for a left neofield we must have, by Theorem 6.1 with $x = 1$, that the set of elements
\[(1 + g)^{-1}(y + g), 1 + g \neq 0, y + g \neq 0, \text{exhausts the set } G \setminus \{1, y\},\]

\[\Rightarrow (1 + g)^{-1}y(1 + y^{-1}g), 1 + g \neq 0, y + g \neq 0, \text{exhausts the set } G \setminus \{1, y\},\]

\[\Rightarrow (y^{-1} + y^{-1}g)^{-1}(1 + y^{-1}g), 1 + g \neq 0, y + g \neq 0, \text{exhausts the set } G \setminus \{1, y\},\]

\[\Rightarrow (1 + y^{-1}g)^{-1}(y^{-1} + y^{-1}g), 1 + g \neq 0, y + g \neq 0, \text{exhausts the set } G \setminus \{1, y\},\]

\[\text{but } 1 + g_i \neq 0 \Rightarrow y^{-1} + y^{-1}g_i \neq 0 \text{ and } y + g_i \neq 0 \Rightarrow 1 + y^{-1}g_i \neq 0; \text{ thus we have,}\]

\[(1 + y^{-1}g_i)^{-1}(y^{-1} + y^{-1}g_i), 1 + y^{-1}g_i \neq 0, y^{-1} + y^{-1}g_i \neq 0, \text{exhausts the set } G \setminus \{1, y^{-1}\},\]

\[\Rightarrow (1 + g)^{-1}(y^{-1} + g), \text{ where } 1 + g \neq 0 \text{ and } y^{-1} + g \neq 0, \text{exhausts the set } G \setminus \{1, y^{-1}\}. \text{[Here } g_j = y^{-1}g_i]\]

It is possible for an addition table \(L_1\) to be orthogonal to a latin square formed by a rearrangement of its own columns, with locational parameter, say \(g\), defined in an analogous way to that previously. We may then make the following comment.

**Comment.** The addition table \(L_1\) of a left neofield \((N, +, \cdot)\), as defined in fig. 6.2, is orthogonal to a latin square, with first column in natural order, formed by a rearrangement of its own columns if we have that, for some \(g \in G\), the set of elements \((g_i + 1)^{-1}(g_i + g), 1 \leq i \leq n, g_i + 1 \neq 0, g_i + g \neq 0\) exhausts the set \(G \setminus \{1, g\}\). However, by Theorem 5.9 and the corollary to Theorem 6.1, the transpose of \(L_1\) will form the addition table of some left neofield which will then be orthogonal to the rearrangement of its own rows defined by \(g\).

The following theorem is of some interest in connection with the above statements.
Theorem 6.3. If the addition table $L_i$, defined as in fig. 6.2, of some left neofield $(N, +, \cdot)$ which is based on a group $(G, \cdot)$, is orthogonal to the latin square formed by a rearrangement of its own rows defined by the locational parameter $y$, then, if

$y \in Z(G)$ (where $Z(G)$ is the centre of $(G, \cdot)$), the addition table is also orthogonal to the latin square formed by the rearrangement of its own columns with locational parameter $y$.

Proof. By the above comment, we see that we are required to show that the elements $(g_i + 1)^{-1}(g_i + y)$, $1 \leq i \leq n$, $g_i + 1 \neq 0$, $g_i + y \neq 0$, exhausts the set $G \setminus \{1, y\}$.

By assumption we have that the set of elements

$$(1 + g_i)^{-1}(y + g_i), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y + g_i \neq 0,$$

exhausts the set $G \setminus \{1, y\}$, which, by Theorem 6.2, implies that the set of elements

$$(1 + g_i)^{-1}(y^{-1} + g_i), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y^{-1} + g_i \neq 0,$$

exhausts the set $G \setminus \{1, y^{-1}\}$,

$$(g_i^{-1} + 1)^{-1}(y^{-1} + g_i), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y^{-1} + g_i \neq 0,$$

exhausts the set $G \setminus \{1, y^{-1}\}$,

$$(g_i^{-1} + 1)^{-1}(y^{-1}g_i^{-1} + 1), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y^{-1} + g_i \neq 0,$$

exhausts the set $G \setminus \{1, y^{-1}\}$, since $y \in Z(G)$,

$$(g_i^{-1} + 1)^{-1}y^{-1}(g_i^{-1} + y), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y^{-1} + g_i \neq 0,$$

exhausts the set $G \setminus \{1, y^{-1}\}$,

$$_{y^{-1}}(g_i^{-1} + 1)^{-1}(g_i^{-1} + y), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y^{-1} + g_i \neq 0,$$

exhausts the set
$G \setminus \{1, y^{-1}\}$, since $y \in Z(G)$.

$\Rightarrow (g_i^{-1} + 1)^{-1}(g_i^{-1} + y), \ 1 \leq i \leq n, \ 1 + g_i \neq 0, \ y^{-1} + g_i \neq 0$, exhausts the set $G \setminus \{1, y\}$.

But $1 + g_i \neq 0 \Rightarrow g_i^{-1} + 1 \neq 0$ and $y^{-1} + g_i \neq 0 \Rightarrow g_i^{-1}y^{-1} + 1 \neq 0 \Rightarrow y^{-1}g_i^{-1} + 1 \neq 0$ 

$\Rightarrow g_i^{-1} + y \neq 0$ since $y \in Z(G)$. Thus we have $(g_j + 1)^{-1}(g_j + y), \ 1 \leq j \leq n, \ g_j + 1 \neq 0, \ g_j + y \neq 0$, exhausts the set $G \setminus \{1, y\}$. □

As was discussed in Chapter 1, one of the interesting properties which a latin square may possess is self-orthogonality.

Theorem 6.4. Let $L_2$ be defined as in fig. 6.2, then $L_2$ is self-orthogonal if $y$ is such that the set of elements $(y + g_k)^{-1}(g_ky + 1), \ 1 \leq k \leq n$, where $y + g_k \neq 0$, are all distinct and not equal to $y$. [Note that $y^{-1}$ will not occur amongst the set of ratios since $(y + g_k)^{-1}(g_ky + 1) = y^{-1} \Rightarrow (g_ky + 1)^{-1}(y + g_k) = y \Rightarrow (y + g_k)^{-1}(g_ky + 1) = y$, contrary to hypothesis.]

Proof. Let $A$ be the array of ordered pairs formed when we juxtapose $L_2$ with its transpose. We observe that all ordered pairs $[i, ly]$ and $[ly, l]$ occur in the zeroth row and zeroth column of $A$ respectively. In fact we have that the ordered pair in the $(i, j)$th cell of $A$ is $[g_iy + g_j, g_jy + g_i]$.

We are required to show that

(1) the $(i, j)$th cell never contains $[l, ly]$ for $i > 0$ or $[ly, l]$ for $j > 0$.

(2) if the $(i, j)$th and $(u, v)$th cells both contain $[l, m]$, then $i = u$ and $j = v$.

Firstly, suppose $[l, ly]$ occurs in the $(i, j)$th cell of $A$ with $i > 0$, then

$g_iy + g_j = l$ and $g_jy + g_i = ly$
\[ \Rightarrow (g_y + g_j)^{-1}(g_y y + g_i) = y \]
\[ \Rightarrow (y + g_j^{-1}g_i)^{-1}(g_j^{-1}g_y y + 1) = y \]
\[ \Rightarrow (y + g_k)^{-1}(g_k y + 1) = y, \text{ where } g_k = g_j^{-1}g_i, \text{ contrary to hypothesis.} \]

Now suppose that \([y, i]\) occurs in the \((i, j)\)th cell of \(A\) with \(i, j > 0\), then

\[ g_i y + g_j = l y \text{ and } g_i y + g_i = l \]
\[ \Rightarrow (g_i y + g_j)^{-1}(g_i y + g_j) = y, \text{ which is the same condition as before with } i \text{ and } j \text{ interchanged and so this too is contrary to hypothesis.} \]

Secondly, suppose that the ordered pair \([l, m]\) occurs in both the \((i, j)\)th and \((u, v)\)th cells of \(A\), then we have:

\[ g_i y + g_j = l \quad (1) \quad g_u y + g_v = m \quad (3) \]
\[ g_i y + g_v = l \quad (2) \quad g_u y + g_u = m \quad (4) \]
\[ \Rightarrow (g_i y + g_j)^{-1}(g_i y + g_j) = (g_u y + g_v)^{-1}(g_u y + g_u) \text{ if } l \neq 0, \]
\[ \Rightarrow (y + g_j^{-1}g_i)^{-1}(g_j^{-1}g_i y + 1) = (y + g_u^{-1}g_v)^{-1}(g_u^{-1}g_v y + 1) \]
\[ \Rightarrow (y + g_u)^{-1}(g_u y + 1) = (y + g_u)^{-1}(g_u y + 1), \text{ where } g_k = g_j^{-1}g_i \text{ and } \]
\[ g_u = g_u^{-1}g_v, \]
\[ \Rightarrow g_k = g_u, \text{ by hypothesis.} \]

But \(g_i^{-1}g_j = g_u^{-1}g_v \iff i = u \text{ and } j = v\) by a modification of the remark made on page 76.

If \(l = 0\), we have \(y + g_j^{-1}g_i = y + g_u^{-1}g_v\) by (1) and (2), which implies that \(g_i^{-1}g_j = g_u^{-1}g_v\) and so once more \(i = u \text{ and } j = v\). \(\square\)
6.2. Results

Table 6.1 gives detailed information for all isomorphically distinct left neofields of order less than ten. For each left neofield its presentation function is displayed as a product of disjoint cycles, from which its characteristic or pseudo-characteristic (if it possesses either) can easily be determined. Column (1) indicates those cases in which it is known that the addition table of the left neofield is a member of a complete set of m.o.l.s.. Such a complete set defines a projective plane. Note that in column (1) the following abbreviations are used: $D =$ Desarguesian plane, $T =$ translation plane, $DT =$ dual translation plane. Column (2) gives the size of the isomorphism class of which the particular left neofield is a representative. Column (3) indicates whether addition is commutative ($C =$ commutative, $NC =$ non-commutative). If addition is commutative, then, when the table is arranged in the form denoted by $L_1$ in fig. 6.2, it is symmetric. If the addition table can be rearranged into the form denoted by $L_2$ in fig.6.2 so as to form a self-orthogonal latin square, then the set of locational parameters for which this is possible (see Theorem 6.4) is given in column (4); if there are none we denote this fact by $\emptyset$, if the set contains all the non-identity elements of the group we use $G \setminus \{1\}$ etc. Similarly if the addition table, when in the form of $L_1$ in fig. 6.2, is orthogonal to a latin square formed by a rearrangement of its own rows, as in $L_2$ in fig. 6.2, then the set of locational parameters for which this is possible is given in column (5). Finally each presentation function is preceded by a number which is used to denote the isomorphism class of which the particular left neofield is a representative. If the transpose of the addition table of the representative of the $n$th isomorphism class defines an isomorphically distinct left neofield, then the presentation function of this distinct left neofield is chosen as the representative of its isomorphism class, which is then denoted by $n'$. Similarly if the latin square formed when we interchange the roles of rows and symbols of the representative of the $n$th isomorphism class (see Theorem 5.10) forms the addition table of an
isomorphically distinct left neofield, then the presentation function of this distinct left neofield is chosen as the representative of its isomorphism class, which is then denoted by $na$. We note that one of the representations of the Dual Translation plane of order nine by eight m.o.l.s. contains the addition tables of four isomorphically distinct neofields based on $C_g$. This particular representation was obtained by Preece [48] from the latin squares published by Paige and Wexler [45]. Preece's representation of the Paige-Wexler squares appears as Fig. 4 in [41].

Table 6.2 contains information about sets of mutually orthogonal latin squares, including orthogonal pairs which are not of the type included in Table 6.1. Orthogonal pairs based on $C_g$ have not been included since there are too many of them, although it is worth noting that every addition table possesses at least one orthogonal mate. For each group we give a series of lists of presentation functions. Each presentation function is numbered according to the isomorphism class, in Table 6.1, of which it is a member and is followed by a locational parameter (or set of locational parameters). To obtain a set of m.o.l.s. from each list of presentation functions we use each of the locational parameters given to construct a latin square which has the form of $L_4$ in fig. 6.2. The resulting set of latin squares will be mutually orthogonal. For example, from the second list of presentation functions based on $C_g$ we obtain the addition tables exhibited in fig. 6.3, which form a set of four m.o.l.s. of order nine.

Table 6.3 contains summarised information for left neofields of orders ten to fourteen. In column (1), for each group, we give the total number of left neofields based on this group. In column (2) we display the composition of the isomorphism classes for orders up to twelve. In column (2) $x(y)$ denotes the fact that there are $x$ isomorphism classes each containing $y$ members. In column (3) we give the number of isomorphism classes of each size whose members possess an orthogonal mate. In column (3) $x(y)$ denotes the fact that there are $x$
isomorphism classes of size \( y \) whose members possess an orthogonal mate. In column (4) we give the size of the maximal set of m.o.l.s. formed by the addition tables of left neofields, based on each group, except that for \( C_{19} \) we exclude the complete set defined by the Desarguesian plane of order eleven. In Table 6.4 we give an example of each such maximal set using the same format as that of Table 6.2.

In Table 6.5 we consider those groups studied which possess both complete and near complete mappings. We recall, from Chapter 5, that there is a bijection from the presentation functions of the left neofields based on a group \((G, \cdot)\) to the complete and near complete mappings of \((G, \cdot)\). In Chapter 1 we stated that an abelian group possesses a complete mapping unless it possesses a unique element of order two, in which case it possesses a near complete mapping. We also stated that a non-abelian group \((G, \cdot)\) does not possess a complete mapping unless there is an ordering of its elements, say \( a_1, a_2, \ldots, a_n \), such that \( a_1 a_2 \cdots a_n = 1 \). For each group \((G, \cdot)\) covered by the above remarks the number of complete or near complete mappings which it possesses can be determined by counting the total number of presentation functions which define left neofields which are based on \((G, \cdot)\). For example, \( C_8 \) does have a unique element of order two and so possesses near complete mappings. From column (2) of Table 6.1 it can be seen that the presentation functions of left neofields based on \( C_8 \) form twelve isomorphism classes of size four and eight isomorphism classes of size two. Thus \( C_8 \) possesses 64 near complete mappings. For each group not covered by the above remarks, columns (1) and (2) give the numbers of complete and near complete mappings of the group respectively.
Here \( L_1, L_3 \) and \( L_4 \) are the representatives of the isomorphism classes numbered 8, 4 and 4' respectively and \( L_2 \) is a distinct member of the isomorphism class numbered 8.

fig. 6.3.
<table>
<thead>
<tr>
<th>Order 2</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( G = C_1 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1))</td>
<td>(D)</td>
<td>1</td>
<td>(C)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_2 &lt;a: a^2 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1 \ a))</td>
<td>(D)</td>
<td>1</td>
<td>(C)</td>
<td></td>
<td>(G \backslash {1})</td>
</tr>
<tr>
<td>Order 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_3 &lt;a: a^3 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1)(a \ a^2))</td>
<td>(D)</td>
<td>1</td>
<td>(C)</td>
<td>(G \backslash {1})</td>
<td>(G \backslash {1})</td>
</tr>
<tr>
<td>Order 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_4 &lt;a: a^4 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1 \ a \ a^2 \ a^3))</td>
<td>(D)</td>
<td>2</td>
<td>(C)</td>
<td>({a, a^3})</td>
<td>(G \backslash {1})</td>
</tr>
<tr>
<td>( G = C_2 \times C_2 &lt;a, b: a^2 = b^2 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1)(a \ b \ ab))</td>
<td>(\text{No})</td>
<td>2</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>Order 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_5 &lt;a: a^5 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1)(a \ a^4)(a^2 \ a^3))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>1'. ((0 \ 1)(a \ a^2 \ a^4 \ a^3))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>Order 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_6 &lt;a: a^6 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1 \ a^2 \ a^4 \ a^5 \ a^3))</td>
<td>(D)</td>
<td>2</td>
<td>(C)</td>
<td>({a, a^2, a^4, a^5})</td>
<td>(G \backslash {1})</td>
</tr>
<tr>
<td>2. ((0 \ 1 \ a^2 \ a^4 \ a^5 \ a^3))</td>
<td>(\text{No})</td>
<td>2</td>
<td>(NC)</td>
<td>({a^2, a^3})</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>2'. ((0 \ 1 \ a \ a^3)(a^2 \ a^4 \ a^5))</td>
<td>(\text{No})</td>
<td>2</td>
<td>(NC)</td>
<td>({a, a^4})</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>2a. ((0 \ 1 \ a \ a^4)(a \ a^2 \ a^3))</td>
<td>(\text{No})</td>
<td>2</td>
<td>(C)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>( G = D_3 &lt;a, b: a^3 = b^2 = 1, ab = ba^{-1}&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1 \ b)(a \ a^2 \ ab \ a^2 b))</td>
<td>(\text{No})</td>
<td>6</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>Order 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_7 &lt;a: a^7 = 1&gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. ((0 \ 1)(a \ a^3)(a^2 \ a^6)(a^4 \ a^5))</td>
<td>(D)</td>
<td>2</td>
<td>(C)</td>
<td>(G \backslash {1})</td>
<td>(G \backslash {1})</td>
</tr>
<tr>
<td>2. ((0 \ 1)(a \ a^3)(a^2 \ a^6)(a^5 \ a^4))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>2'. ((0 \ 1)(a \ a^2 \ a^6)(a^3 \ a^5 \ a^4))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>2a. ((0 \ 1)(a \ a^4 \ a^5)(a^3 \ a^6 \ a^2))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(C)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>3. ((0 \ 1)(a \ a^2 \ a^5 \ a^6 \ a^4))</td>
<td>(\text{No})</td>
<td>6</td>
<td>(NC)</td>
<td>({a^2})</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>3'. ((0 \ 1)(a \ a^4 \ a^3 \ a^5 \ a^6))</td>
<td>(\text{No})</td>
<td>6</td>
<td>(NC)</td>
<td>({a^2})</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>4. ((0 \ 1)(a \ a^3 \ a^2 \ a^4 \ a^5))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>4'. ((0 \ 1)(a \ a^2 \ a^4 \ a^5 \ a^3))</td>
<td>(\text{No})</td>
<td>1</td>
<td>(NC)</td>
<td>(\emptyset)</td>
<td>(\emptyset)</td>
</tr>
<tr>
<td>Order 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( G = C_8 \times \langle a \mid a^8 = 1 \rangle )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. (0 1 ( a^3 )) (( a^2 \ a^6 )) (( a^2 \ a^3 \ a^3 ))</td>
<td>( D, T )</td>
<td>2</td>
<td>( C )</td>
<td>( G \setminus { 1, a^4 } )</td>
<td>( G \setminus { 1 } )</td>
</tr>
<tr>
<td>2. (0 1 ( a^2 )) (( a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( \langle a^2, a^3 \rangle )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>2'. (0 1 ( a^3 )) (( a^7 \ a^6 \ a^6 )) (( a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( \langle a^2, a^3 \rangle )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>2a. (0 1 ( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^3 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( C )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>3. (0 1 ( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( { a^3, a^7 } )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>3a. (0 1 ( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( C )</td>
<td>( { a^3 } )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>4. (0 1 ( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( DT' )</td>
<td>2</td>
<td>( NC )</td>
<td>( \langle a^2, a^3 \rangle )</td>
<td>( \langle a^4 \rangle )</td>
</tr>
<tr>
<td>4a. (0 1 ( a^3 )) (( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( DT' )</td>
<td>2</td>
<td>( NC )</td>
<td>( \langle a^2, a^3 \rangle )</td>
<td>( \langle a^4 \rangle )</td>
</tr>
<tr>
<td>5. (0 1 ( a^4 )) (( a^2 \ a^4 )) (( a^4 \ a^4 \ a^4 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( { a^2, a^3 } )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>5a. (0 1 ( a^2 \ a^4 )) (( a^2 \ a^6 )) (( a^2 \ a^3 \ a^3 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( { a^2, a^3 } )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>6. (0 1 ( a^2 \ a^6 )) (( a^2 \ a^2 )) (( a^2 \ a^3 \ a^3 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>6a. (0 1 ( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>6a'. (0 1 ( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>4</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>7. (0 1 ( a^3 )) (( a^2 \ a^3 )) (( a^2 \ a^3 \ a^3 \ a^3 ))</td>
<td>( \text{No} )</td>
<td>2</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>7a. (0 1 ( a^2 \ a^4 )) (( a^2 \ a^2 \ a^2 \ a^2 \ a^2 \ a^2 ))</td>
<td>( \text{No} )</td>
<td>2</td>
<td>( NC )</td>
<td>( \langle a, a^3, a^5, a^7 \rangle )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>8. (0 1 ( a^4 )) (( a^2 \ a^3 \ a^3 \ a^4 ))</td>
<td>( DT )</td>
<td>2</td>
<td>( NC )</td>
<td>( \langle a, a^3, a^5, a^7 \rangle )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>( G = C_2 \times C_4 &lt; \langle a, b \mid a^2 = b^2 = 1 \rangle &gt; )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. (0 1) (( a^2 \ b )) (( a^3 \ a^2 b \ a^2 b ))</td>
<td>( \text{No} )</td>
<td>8</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>1a. (0 1) (( a^2 b \ a^2 \ a^2 b \ a^2 )) (( b \ a^b ))</td>
<td>( \text{No} )</td>
<td>8</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>1a'. (0 1) (( a^2 b \ a^2 \ a^2 b )) (( b \ a^b ))</td>
<td>( \text{No} )</td>
<td>8</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>1a'. (0 1) (( a^2 b \ a^2 \ a^2 b )) (( b \ a^b ))</td>
<td>( \text{No} )</td>
<td>8</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>1a'. (0 1) (( a^2 b \ a^2 \ a^2 b )) (( b \ a^b ))</td>
<td>( \text{No} )</td>
<td>8</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>( G = C_2 \times C_2 \times C_2 &lt; \langle a, b, c \mid a^2 = b^2 = c^2 = 1 \rangle )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. (0 1) (( a \ b \ c \ a \ b \ c \ a \ b ))</td>
<td>( \text{No} )</td>
<td>24</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
<tr>
<td>1a. (0 1) (( a \ b \ a \ c \ a \ b \ a \ c \ a \ b ))</td>
<td>( \text{No} )</td>
<td>24</td>
<td>( NC )</td>
<td>( \emptyset )</td>
<td>( \emptyset )</td>
</tr>
</tbody>
</table>
\[ G = D_4 \langle a, b; a^4 = b^2 = 1, ab = ba^{-1} \rangle \]

<table>
<thead>
<tr>
<th>( G = Q_4 \langle a, b; a^4 = 1, a^2 = b^3, ab = ba^{-1} \rangle )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ((0 , 1)(a , a^2 , a^3 , a^4 , a^6 , a^7 , a^8))</td>
</tr>
<tr>
<td>2. ((0 , 1)(a , a^2 , a^3 , a^4 , a^6 , a^7 , a^8))</td>
</tr>
<tr>
<td>3. ((0 , 1)(a , a^2 , a^3 , a^4 , a^6 , a^7 , a^8))</td>
</tr>
<tr>
<td>4. ((0 , 1)(a , a^2 , a^3 , a^4 , a^6 , a^7 , a^8))</td>
</tr>
</tbody>
</table>

**Table 6.2**

| \( C_4 \) | \( L \) |
|---|
| 2. \((0 \, 1)(a \, a^2 \, a^4 \, a^3)\) | 1 |
| 2'. \((0 \, 1)(a \, a^2 \, a^4 \, a^3)\) | \( a^2 \) |
| 3. \((0 \, 1)(a \, a^2 \, a^4 \, a^3)\) | \( a^3 \) |
| 3. \((0 \, 1)(a \, a^2 \, a^4 \, a^3)\) | \( a^7 \) |

| \( C_8 \) | \( L \) |
|---|
| 3a. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | 1 |
| 3. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | 1 |
| 3. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | 1 |
| 4. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | 1 |
| 4. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | \( a^2 \) |
| 4. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | \( a^3 \) |
| 4a. \((0 \, 1)(a \, a^2 \, a^3 \, a^4 \, a^5 \, a^6 \, a^7 \, a^8)\) | \( 1, a^2, a^3, a^6 \) |

This column continued on next page.
<table>
<thead>
<tr>
<th>(D_4)</th>
<th>(Q_4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (0 1) ((a b a^3 ab a^2 b a^2 a))</td>
<td>4. (0 1) ((a b a^3 b a^2 ab a^2 a))</td>
</tr>
<tr>
<td>1. (0 1) ((a a^2 b b ab a^2 a^2 ab))</td>
<td>4. (0 1) ((a a^2 b a^2 b a^2 a^2 b a^2 b))</td>
</tr>
<tr>
<td>3. (0 1) ((a a^2 b a^2 b))</td>
<td>4. (0 1) ((a b b a^2 b a^2 b a^2 b a^2 b))</td>
</tr>
<tr>
<td>2. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>1. (a^2)</td>
</tr>
<tr>
<td>2. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>4. (0 1) ((a a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
</tr>
<tr>
<td>4. (0 1) ((a a^2 b a^2 b a^2 b))</td>
<td>1. (a^3)</td>
</tr>
<tr>
<td>2. (0 1) ((a b b a^2 b a^2 b a^2 b a^2 b))</td>
<td>4. (0 1) ((a b b a^2 b a^2 b a^2 b a^2 b))</td>
</tr>
<tr>
<td>1. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>4. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
</tr>
<tr>
<td>3. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>a</td>
</tr>
<tr>
<td>3. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>2. (0 1) ((a b ab a^2 a^2 b a^2))</td>
</tr>
<tr>
<td>3. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>2. (0 1) ((a b ab a^2 a^2 b a^2))</td>
</tr>
<tr>
<td>2. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>2. (0 1) ((a b ab a^2 a^2 b a^2))</td>
</tr>
<tr>
<td>2. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>2. (0 1) ((a b ab a^2 a^2 b a^2))</td>
</tr>
<tr>
<td>2. (0 1) ((a b a^2 b a^2 b a^2 b a^2 b a^2 b))</td>
<td>2. (0 1) ((a b ab a^2 a^2 b a^2))</td>
</tr>
</tbody>
</table>
Table 6.3.

<table>
<thead>
<tr>
<th>Order</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_9$</td>
<td></td>
<td></td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>$C_2 \times C_3$</td>
<td>249</td>
<td>1(1), 4(6), 2(8), 1(16), 4(48)</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Order 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$C_{10}$</td>
<td>928</td>
<td>12(2), 226(4)</td>
<td>12(2), 218(4)</td>
<td>4</td>
</tr>
<tr>
<td>$D_5$</td>
<td>820</td>
<td>12(10), 35(20)</td>
<td>12(10), 35(20)</td>
<td>2</td>
</tr>
<tr>
<td>Order 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$C_{11}$</td>
<td>3,441</td>
<td>9(1), 6(2), 12(5), 336(10)</td>
<td>6(5), 300(10)</td>
<td>2</td>
</tr>
<tr>
<td>Order 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$C_{12}$</td>
<td>17,336</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$C_2 \times C_6$</td>
<td>16,512</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$D_6$</td>
<td>17,280</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$A_4$</td>
<td></td>
<td></td>
<td>16,704</td>
<td></td>
</tr>
<tr>
<td>$Q_8$</td>
<td>17,280</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Order 14</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$C_{13}$</td>
<td>79,259</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6.4.

<table>
<thead>
<tr>
<th>$C_9 &lt;a: a^9 = 1&gt;$</th>
<th>$L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0 1)(a a')(a^3 a^6 a^4 a^8 a^5 a^7)</td>
<td>1</td>
</tr>
<tr>
<td>(0 1)(a a^8 a^4 a^6 a^2 a^3 a^7)</td>
<td>$a^6$</td>
</tr>
<tr>
<td>$C_{10} &lt;a: a^{10} = 1&gt;$</td>
<td></td>
</tr>
<tr>
<td>(0 1) a^2 a a^5)(a^2 a^6 a^3 a^2 a^4)</td>
<td>$1, a^3$</td>
</tr>
<tr>
<td>(0 1) a^6 a^4 a^2 a^5)(a^3 a^7)(a^6 a^8)</td>
<td>$a^4, a^9$</td>
</tr>
<tr>
<td>$D_5 &lt;a, b: a^5 = b^2 = 1, ab = ba^{-1}$</td>
<td></td>
</tr>
<tr>
<td>(0 1) a a^3 b a^2 b a^4 ab a^3 b a^4 b)</td>
<td>1</td>
</tr>
<tr>
<td>(0 1) a^6(a^4 a^2 b)(a^2 a^3 b a^6 b)</td>
<td>$a$</td>
</tr>
<tr>
<td>$C_{11} &lt;a: a^{11} = 1&gt;$</td>
<td></td>
</tr>
<tr>
<td>(0 1)(a a^5 a^7 a^8 a^6 a^3 a^{10} a^2)(a^4 a^6)</td>
<td>1</td>
</tr>
<tr>
<td>(0 1)(a a^{10} a^4 a^8 a^5 a^7 a^3)(a^3 a^6)</td>
<td>$a$</td>
</tr>
</tbody>
</table>

Table 6.5

<table>
<thead>
<tr>
<th>$Q_4$</th>
<th>(1)</th>
<th>(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>48</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>$D_4$</td>
<td>48</td>
<td>16</td>
</tr>
<tr>
<td>$D_6$</td>
<td>6,336</td>
<td>10,994</td>
</tr>
<tr>
<td>$A_4$</td>
<td>3,840</td>
<td>12,864</td>
</tr>
</tbody>
</table>

6.3. Observations

Firstly we observe the fact, which at first sight seems rather remarkable, that the total numbers of complete mappings and near complete mappings of the pairs of groups $C_2 \times C_4$, $C_2 \times C_2 \times C_2$ and $Q_4$, $D_4$ of order eight are equal. In Chapter 9 we
provide an explanation of why this is necessarily the case.

Secondly we observe that the isomorphism classes of size one so far found have all been of even order and have had the property that $1 + x^i = x^{i^d}$, when $1 \leq i < n$. For example, one of the cyclic neofields of order six has presentation function $\psi = (0 1)(x^2 x^4 x^3)$. The following theorem shows that this property is sufficient for all isomorphs of a cyclic neofield of even order to coincide, however it turns out not to be necessary.

Theorem 6.5. Let $(N, +, \cdot)$ be a cyclic neofield of even order, based on the cyclic group of order $n$, such that $(N, +, \cdot)$ possesses the property $1 + x^i = x^{i^d}$, when $1 \leq i < n$. Then all isomorphs coincide.

Proof. Let $x \rightarrow y$, where $y = x^u$, be an isomorphic mapping from $(N, +, \cdot)$ to $(N', \oplus, \cdot)$. We are required to show that $1 + x^i = x^{i^d} \implies 1 \oplus y^i = y^{i^d}$ when $1 \leq i < n$. [Note that we know $1 + 0 = 1$ and $1 + 1 = 0$ in $(N, +, \cdot)$ and $1 \oplus 0 = 1$ and $1 \oplus 1 = 0$ in $(N', \oplus, \cdot)$] Now $1 \oplus y^i$ is equal to the image of $1 + (x^u)^i$ under the isomorphism but $1 + (x^u)^i = (x^u)^{i^d}$ which is mapped onto $y^{i^d}$. Thus $1 \oplus y^i = y^{i^d}$ and the theorem is proved. $\Box$

We will show that, in general, the converse to the statement made in Theorem 6.5 is false. However the following theorem shows that it is true for cyclic neofields of certain orders.

Theorem 6.6. Let $(N, +, \cdot)$ be a cyclic neofield of even order $n^H = p + 1$, where $p$ is a prime. Then the necessary and sufficient condition for all isomorphs of $(N, +, \cdot)$ to coincide is that $(1 + x^i) = x^{i^d}$, when $1 \leq i < n$.

Proof. Let $1 + x^i = x^{i^d}$, when $1 \leq i < n$. Now isomorphic mappings $x \rightarrow y$, where $y = x^u$, exist for all $u$ when $1 \leq u < n$ since the multiplicative cyclic group is of
prime order. By considering each isomorphism applied separately we observe that
the condition $1 + x^u = (x^n)^u$, when $1 \leq u < n$, is necessary in order for all
isomorphs to coincide. But this is equivalent to insisting that $v_i = v_j t$, when
$1 \leq i < n$ which, we know by Theorem 6.5, is sufficient for all isomorphs to
coincide. Thus the condition specified in the statement of the theorem (with
$v = v_j$) is both necessary and sufficient for all isomorphs to coincide in the case of
neofields which are based on cyclic groups of order an odd prime. □

Theorem 6.6 cannot be extended to neofields based on cyclic groups of
order $n$, $n$ composite (although it is true in the special case of $n = 9$). We
demonstrate this fact by constructing a counter-example for the smallest order not
yet examined, namely $n = 15$.

For $n = 15$ a presentation function which satisfies the conditions of
Theorem 6.5 is $\psi = (0 1 5)(1 2 4 8)(3 6 12 9)(5 10)(7 14 13 11)$. Notice that $1 + x^3 = x^5$,
$1 + x^6 = x^{12}$, $1 + x^9 = x^{3}$ and $1 + x^{12} = x^9$. We rearrange these elements so as to
form a new presentation function in which $1 \circ x^3 = x^{12}$, $1 \circ x^6 = x^9$, $1 \circ x^9 = x^6$ and
$1 \circ x^{12} = x^3$. Note that for this subset we have $1 \circ x^j = x^{4j}$ where $j \in \{3, 6, 9, 12\}$. Consider the permutation $\psi' = (0 1 5)(1 2 4 8)(3 12)(6 9)(5 10)(7 14 13 11)$, which differs
from $\psi$ only with respect to the elements $j$ above. In order to check that $\psi'$ is
indeed a presentation function we need only look at the entries in which $\psi$ and $\psi'$
differ. From $\psi$ we obtain the differences $3-6=12$, $6-12=9$, $9-3=6$ and $12-9=3$.
Similarly from $\psi'$ we obtain the differences $3-12=9$, $6-9=3$, $9-6=3$ and $12-3=9$.
Thus we have that if $\psi$ is a presentation function, then so is $\psi'$. Furthermore, all
isomorphs of the neofield defined by $\psi'$ coincide. To see this we observe that in
the neofield defined by $\psi'$ we have

$1 \circ x^i = x^{2i}$, when $i \in \phi = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14\}$

$1 \circ x^j = x^{4j}$, when $j \in \theta = \{3, 6, 9, 12\}$
but $i \in \phi \Rightarrow 2i \in \phi$ and $j \in \theta \Rightarrow 4j \in \theta$.

Now consider any isomorphic mapping $x \to y$ where $y = x^u$ (and therefore $u \in \{1, 2, 4, 7, 8, 11, 13, 14\}$). Before the mapping is applied we have $1 \otimes x^i = x^{2i}$, when $i \in \phi$ and $1 \otimes x^j = x^{4j}$, when $j \in \theta$, since any element of $\phi$ or $\theta$ when multiplied by a number relatively prime to 15 and reduced modulo 15 will always remain an element of $\phi$ or $\theta$ respectively. Therefore after the mapping $x \to y$ we must have $1 \otimes y^i = y^{2i}$ when $i \in \phi$ and $1 \otimes y^j = y^{4j}$, when $j \in \theta$, from which it follows that all isomorphs must coincide.
Chapter 7 Property D Neofields

7.0. Introduction

In [31] Keedwell defined the concept of a property D neofield. As we will show, the motivation for this concept comes from the fact that a property D neofield of order \( n \) defines a pair of orthogonal latin squares of order \( n \). In this chapter we generalise some of Keedwell's results within the framework of left neofield theory and make some new observations.

7.1. Existence and construction of property D neofields

Definition 7.1. A property D neofield is a cyclic neofield which possesses the additional property that \( (1 + x^i)/(1 + x^{i-1}) = (1 + x^j)/(1 + x^{j-1}) \Rightarrow i = j \), where \( x \) is any generating element of the multiplicative group.

That a property D neofield of order \( n \) defines a pair of orthogonal latin squares of order \( n \) follows directly from the corollary to Theorem 6.1. In fact the addition table of a property D neofield possesses an orthogonal mate which is formed by permuting its own non-identity rows, with the generating element \( x \) as locational parameter. Using the notation of Theorem 6.1 we then have that

\[
d_i = (x + x^i)/(1 + x^i), \quad 1 \leq i \leq n, \quad 1 + x^i \neq 0, \quad x + x^i \neq 0
\]

\[
\Rightarrow d_i = x[(1 + x^i)/(1 + x^{i-1})]^{-1}, \quad 1 \leq i \leq n, \quad 1 + x^i \neq 0, \quad x + x^i \neq 0.
\]

Hence, \( d_i = d_j \Rightarrow [(1 + x^i)/(1 + x^{i-1})]^{-1} = [(1 + x^j)/(1 + x^{j-1})]^{-1} \Rightarrow i = j \), by property D. Thus the \( d_i \)'s are all distinct and, since clearly \( d_i \neq 1 \) or \( 0 \), the conditions for the corollary to Theorem 6.1 are satisfied.

In this chapter it will sometimes prove useful to adopt a different notation for cyclic neofields, which we will call index notation. In index notation we represent the element \( x^i \) by \( i \). In this notation the element 1 is represented by 0.
and so we need a new symbol for the additive identity, which we will write as \( n \), where \( n \) is the order of the multiplicative group.

In [31] necessary and sufficient conditions are given for a property \( D \) neofield to exist. In the following Theorem we generalise these conditions so as to include arbitrary cyclic neofields.

**Theorem 7.1.** A necessary and sufficient set of conditions for a cyclic neofield of order \( n+1 \) to exist is that \( n-2 \) (not necessarily distinct) residues modulo \( n \) from the set \( \{2, 3, \ldots, n-1\} \) can be arranged in a row array \( P \) such that:

(i) the partial sums of the first one, two, \( \ldots \), \( (n-2) \) elements are all distinct and non-zero modulo \( n \);

(ii) when each element of the array is reduced by one the new array, say \( P' \), also satisfies (i).

**Proof.** Suppose we are given a cyclic neofield \( (N, +, \cdot) \), based on the cyclic group of order \( n \), which is written in index notation. We know that any one of the non-identity rows of its addition table uniquely defines the entire square. Now consider the \( h \)'th row, where \( h \) is such that \( h + 0 = n \) (which corresponds to \( x^h + 1 = 0 \) in the original notation). We know that for \( n \) odd, \( h = 0 \), and for \( n \) even, \( h = n/2 \).

We claim that the differences between successive entries in the \( h \)'th row, where we exclude the first two elements namely \( h \) and \( n \) respectively, form an array \( P \) of the type specified in the statement of the theorem. We write the addition table for \( (N, +, \cdot) \) as follows.
We have that $a_{ij} = a_{i-1,j-1} + 1$ if $a_{i-1,j-1} \neq n$; $a_{ij} = n$ otherwise. If we define

$$p_1 = a_{hl} - a_{h1}$$

$$p_2 = a_{h2} - a_{h3}$$

$$\vdots$$

$$p_{n-2} = a_{h,n-1} - a_{h,n-2}$$

then the elements $p_i$, $1 \leq i \leq n-2$ are not equal to 0 or 1 (if $p_1 = 1$, then $a_{h,i+1} - a_{hi} = 1$ which implies that $a_{h,i+1} = 1 + a_{hi}$ but $a_{h+1,i+1} = 1 + a_{hi}$ and so the same element would appear twice in the $(i+1)$th column of the addition table, which cannot happen). Furthermore their partial sums are given by:

$$p_1 = a_{h2} - a_{h1}$$

$$p_1 + p_2 = a_{h3} - a_{h1}$$

$$\vdots$$

$$p_1 + p_2 + \cdots + p_{n-2} = a_{h,n-1} - a_{h1}$$

That these partial sums are all distinct and not equal to 0 follows directly from the fact that the $a_{hi}$'s are all distinct.

Let us now consider the differences between consecutive entries in the column headed by zero. We have
\[ a_{h+1,0} - a_{h+2,0} = a_{h+1,0} - (a_{h+1,n-1} + 1) \]
\[ = (a_{h+1,0} - a_{h+1,n-1}) - 1 \]
\[ = (a_{h,n-1} - a_{h,n-2}) - 1 \]
\[ a_{h+2,0} - a_{h+3,0} = a_{h+2,0} - (a_{h+2,n-1} + 1) \]
\[ = (a_{h+2,0} - a_{h+2,n-1}) - 1 \]
\[ = (a_{h,n-2} - a_{h,n-3}) - 1 \]
\[ \vdots \]
\[ a_{n-2,0} - a_{n-1,0} = a_{h-2,0} - (a_{h-2,n-1} + 1) \]
\[ = (a_{h-2,0} - a_{h-2,n-1}) - 1 \]
\[ = (a_{h-2} - a_{h}) - 1 \]

Notice that \((a_{h,j+1} - a_{h,j})\) is just the \(l\)th element of \(P\). Therefore the above equations may be written as \(p_1 - 1 = a_{h-2,0} - a_{h-1,0} \), \(p_2 - 1 = a_{h-3,0} - a_{h-2,0} \), \(\vdots\), \(p_{n-2} - 1 = a_{h+1,0} - a_{h+2,0} \). Thus the differences between successive entries in the column headed by zero, where we ignore the first two entries, forms a row array \(P' = p_1 - 1, p_2 - 1, \ldots, p_{n-2} - 1\). Now \((p_1 - 1) + \cdots + (p_1 - 1) = a_{h-1,0} - a_{h-1,0}\), thus the partial sums of \(P'\) are all distinct and not equal to 0 since the \(a_{h,j}\)'s are all distinct.

Conversely, suppose that the \(n - 2\) residues modulo \(n\) can be arranged in the manner described in the statement of the theorem. Then a cyclic neo-field of order \(n+1\) exists. All that is required is to construct the elements of the \(k\)'th row of what will be the addition table of \(\langle N, +, \cdot \rangle\) from the partial sums of the array and complete this table using the distributivity of \((\cdot)\) over \((+))\). \(\square\)
Clearly, by definition of the row array \( P \), \((N, +, \cdot)\) will have property D if and only if the entries of \( P \) are all distinct.

We will say that the row array \( P \) of the type described in the above theorem, defines the corresponding cyclic neofield.

The converse part of the above proof is best illustrated by way of examples. From the following row array \( P \) we construct a cyclic neofield.

\[
P = 4, 6, 5, 5, 3 \quad P' = 3, 5, 4, 4, 2.
\]

The partial sums of the elements of \( P \) and \( P' \) are given by:

\[
\begin{align*}
4 &= 4 \mod 7 & 3 &= 3 \mod 7 \\
4 + 6 &= 3 \mod 7 & 3 + 5 &= 1 \mod 7 \\
4 + 6 + 5 &= 1 \mod 7 & 3 + 5 + 4 &= 2 \mod 7 \\
4 + 6 + 5 + 5 &= 6 \mod 7 & 3 + 5 + 4 + 4 &= 2 \mod 7 \\
4 + 6 + 5 + 5 + 3 &= 2 \mod 7 & 3 + 5 + 4 + 4 + 2 &= 4 \mod 7.
\end{align*}
\]

Thus, by Theorem 7.1, \( P \) defines a cyclic neofield and we construct the corresponding presentation function in the following way:

\[
\psi = \begin{pmatrix}
0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\
1 & 0 & x^2 & x^{a+4} & x^{a+3} & x^{a+1} & x^{a+6} & x^{a+2}
\end{pmatrix}
\]

however we must have \( x^{a+5} = 1 \) and so \( a = 2 \), hence:

\[
\psi = \begin{pmatrix}
0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\
1 & 0 & x^2 & x^5 & x^3 & x & x^4
\end{pmatrix}.
\]
From the following array $P$ we construct a property D neofield.

$$P = 3, 2, 4, 6, 5; \quad P' = 2, 1, 3, 5, 4.$$ 

Now the partial sums of $P$, modulo 7, are 3, 5, 2, 1 and 6 respectively, so the entries of the $h$'th row are

$$h \quad n \quad x \quad x+3 \quad x+5 \quad x+2 \quad x+1 \quad x+6$$

where the residue $x$ has yet to be determined. We notice that $x+4$ does not occur explicitly as one of the entries, however we know that all possible elements must occur somewhere in this row and so we conclude that $x+4 \equiv h \mod 7$. We also know that for a cyclic neofield of even order we must have $h = 0$ which implies that $x = 3$. Thus the required presentation function is $\psi = (0 7)(1 3)(2 6)(4 5)$.

We have seen that the existence of a cyclic neofield of order $n+1$ is equivalent to the existence of a row array, $P$, of length $n-2$, which has certain properties. We have thus reduced the question regarding the existence of cyclic neofields to a problem in number theory. In so doing we are exploiting the isomorphism that exists between cyclic groups and modular arithmetic. It would be wrong to expect that the existence of left neofields in general could be expressed in a similar way.

7.2. Dual and mirror image row arrays

We now state two results which are generalisations of concepts introduced by Keedwell with regard to property D neofields. In the following theorems we shall assume that $P$ is a row array which defines a cyclic neofield and $P'$ is the row array formed by subtracting one from the corresponding entries of $P$.

Theorem 7.2. With each row array $P$ there corresponds a dual row array $P^{\ominus}$ which also defines a cyclic neofield and is obtained by replacing each entry $q$ of the row array $P'$ by its complement $(n-q) \mod n$, where $n$ is the order of the cyclic
group. Furthermore, the row array $P^{(d)}$ defines a cyclic neofield which has property D if and only if the cyclic neofield defined by $P$ has property D.

**Proof.** If $P$ and $P'$ are transformed in the manner described in the statement of the theorem, then the entries in the transform of $P'$ become one greater than the corresponding entries in the transform of $P$. However the partial sums of the transforms of $P$ and $P'$ are just the transforms of the partial sums of $P$ and $P'$ respectively and so must all be distinct and non-zero modulo $n$. Thus the transform of $P'$ defines a cyclic neofield. Furthermore the transform of $P'$ will define a property D neofield if and only if all the entries in the transform of $P'$ are distinct and this will be true if and only if the entries of $P$ are all distinct (and so $P$ defines a property D neofield). □

**Theorem 7.3.** With each row array $P$ there corresponds a mirror image row array $p^{(m)}$ which defines a cyclic neofield and is obtained from $P$ by reversing its entries. Furthermore $P^{(m)}$ defines a property D neofield if and only if $P$ does.

**Proof.** Let $P = p_1, p_2, \ldots, p_{n-2}$ and so $P^{(m)} = p_{n-2}, p_{n-3}, \ldots, p_1$. If the partial sums of $P$ are $s_1 = p_1$, $s_2 = p_1 + p_2$, $\ldots$, $s_{n-2} = p_1 + p_2 + \ldots + p_{n-2}$, then the partial sums of $P^{(m)}$ are $s_1^{(m)} = s_{n-2}$, $s_2^{(m)} = s_{n-3}$, $\ldots$, $s_{n-2}^{(m)} = s_1$. That these partial sums are all distinct and non-zero follows since $s_1, s_2, \ldots, s_{n-2}$ are all distinct and non-zero. A similar result applies when the entries of $P^{(m)}$ are all reduced by one, thus $P^{(m)}$ defines a cyclic neofield. The fact that $P^{(m)}$ defines a property D neofield if and only if $P$ does follows directly from the definition of mirror image. □

The following two theorems show how the concepts of dual and mirror image can be interpreted in terms of the theory developed in Chapter 5.

**Theorem 7.4.** If the cyclic neofield $(N, +, \cdot)$ is defined by the row array $P$, then its isomorphic image $(N', \oplus, \cdot)$ under the mapping $x \to y$, where $y = x^{-1}$ is defined by the row array $P^{(m)}$. 

Proof. Suppose \( P = (d_1, d_2, \ldots, d_{n-2}) \) and let \( P^* = (d_1^*, d_2^*, \ldots, d_{n-2}^*) \) be the row array which defines \( (N', +, \cdot) \), we are required to show that \( P^* = P^{(n)} \) where \( P^{(n)} = (d_{n-2}, d_{n-3}, \ldots, d_1) \).

Case 1, \( n \) is odd (i.e. cyclic neofield is of even order and so \( 1 + 1 = 0 \)).

By definition \((1 + x^l)/(1 + x^{l-1}) = x^{d_l-1}, \) when \( 2 \leq l \leq n - 1, \)
\[\Rightarrow [1 \oplus (y^{-1})]/[1 \oplus (y^{-1})^{l-1}] = (y^{-1})^{d_l-1} \quad (1)\]
\[\Rightarrow [1 \oplus y^{n-l}\oplus l)/[1 \oplus y^{n-l}] = y^{d_l-1}, \text{ by inverting both sides of (1),}\]
\[\Rightarrow d_{n-l}^* = d_{n-1} \]

But \( d_{n-1} \) is the \((n-1) - (l-1) = (n-l)'\)th entry of \( P^{(n)} \)
\[\Rightarrow P^* = P^{(n)}. \]

Case 2, \( n \) is even (i.e. cyclic neofield is of odd order and so \( 1 + x^{\sqrt{n}} = 0 \)).

We have \((1 + x^{(n/2)+1})(1 + x^{(n/2)(l-1)}) = x^{d_l-1}, \) when \( 2 \leq l \leq n - 1, \)
\[\Rightarrow [1 \oplus y^{-l}(l-1)]/[1 \oplus y^{-l}] = x^{d_l-1} \]
\[\Rightarrow d_{n-l}^* = d_{n-1} \]
\[\Rightarrow P^* = P^{(n)}. \]

Theorem 7.5. Let \((N', +, \cdot)\) be a cyclic neofield based on the cyclic group of order \( n \), defined by the row array \( P = d_1, d_2, \ldots, d_{n-2} \). Then the cyclic neofield \((N', \oplus, \cdot)\), where \( x \oplus y = y + x \), is defined by the row array \( P^T = (1-d_{n-2}, (1-d_{n-3}), \ldots, (1-d_1). \)

Proof. That \((N', \oplus, \cdot)\) so defined forms a cyclic neofield is a consequence of Theorem 5.9. Now suppose \( P^T = d_1^T, d_2^T, \ldots, d_{n-2}^T \), then \( x^T d_1^T = (1 \oplus x^{i+1}))/x(1 + x^l) = (x^T + 1)/x^l = x^{d_1^T-1}/x(1 + x^l) = x^{-d_1^T} \Rightarrow d_1^T = 1 - d_{n-1}. \) Hence \( d_1^T = 1 - d_{n-2}, d_2^T = 1 - d_{n-3}, \ldots, d_{n-2}^T = 1 - d_1. \)
Corollary. Let $P$ be as defined in the statement of Theorem 7.5. Then the cyclic neofields defined by $P^{(a)}$ and $(P^{(m)})^T$ are identical.

Proof. $P^{(m)} = d_{n-2}, d_{n-3}, \ldots, d_1$, hence, by the above theorem, $(P^{(m)})^T = 1 - d_1, 1 - d_2, \ldots, 1 - d_{n-2} = P^{(a)}$. □

The concepts of dual and mirror image row arrays, when applied to property D neofields, were defined by Keedwell in [31]. The results of Theorem 7.1, Theorem 7.4 and the corollary to Theorem 7.5, when applied to property D neofields, appear in [32].
Chapter 8 Implicit Use of Cyclic Neofields

8.0. Introduction

In this chapter we look at how several authors have implicitly used the addition tables of cyclic neofields in the construction of orthogonal latin squares. In some cases we are able to show how knowledge of the cyclic neofield structure would have helped these authors in obtaining and interpreting their results.

This chapter contains the constructions for the results $N(14) \geq 3$ and $N(20) \geq 4$.

8.1. Prolongation and left neofields

The addition tables of those left neofields which define complete mappings of groups (see statement 1 on page 64) can be obtained by the prolongation (or 1-extension) of a special type of latin square. Before we discuss this further we need to make the following definition.

Definition 8.1. The $k$th broken diagonal of a latin square of order $n$, is the set of cells $\{(i, j): i - j \equiv k \mod n\}$. In particular, the 0th broken diagonal is the leading diagonal.

As we have seen in Chapter 3, any given latin square of order $n$, defined over the set $\{1, 2, \ldots, n\}$ and which possesses a transversal, can be extended to form a latin square of order $n + 1$, defined over the set $\{0, 1, 2, \ldots, n\}$. This can be done by first replacing the elements in all the cells of the transversal by 0 and then adding a zeroth row and a zeroth column of elements so as to form a new latin square. For any given transversal this can be done in only one way. [Note that in Chapter 3 we extended latin squares by adding an $(n+1)$th row and $(n+1)$th column. The reason for this change of convention will become apparent.]

As has been previously stated the idea of a 1-extension was discovered
independently by Belousov [1] who called it prolongation. In fact the idea was first employed by Bruck in [10]. [Bruck constructed unipotent quasigroups (i.e. quasigroups \((Q, \ast)\) in which \(x \ast x = 0 \forall x \in Q)\) of order \(n + 1\) from idempotent quasigroups of order \(n\) in a manner exactly similar to that of prolongation. Bruck then showed that, if the original quasigroup has the inverse property, then so does the constructed quasigroup, where \((Q, \ast)\) has the inverse property if, \(\forall a, b \in Q \exists a^L\) and \(a^R \in Q\) such that \(a^L \ast (a \ast b) = (b \ast a) \ast a^R = b.\) The following theorem demonstrates the connection between prolongation and left neofields.

**Theorem 8.1.** The addition table of any left neofield \((N, +, \cdot)\) of order \(n + 1\), based on a particular group \((G, \cdot)\), and whose construction defines a complete mapping of \((G, \cdot)\), is identical to the latin square obtained by the prolongation of an appropriate latin square of order \(n\).

**Proof.** In any such left neofield we must have that 1 + 1 = 0, by statement (1), \(\rho \in G \in \mathcal{A}\), which, by the left distributivity of \((\cdot)\) over \((+),\) implies that \(x + x = 0, \forall x \in N.\) Thus, if, in the addition table for \((N, +, \cdot),\) we replace 0 in the \((x, x)\)th cell with the element \(x,\) and then remove the zeroth row and zeroth column, we obtain a latin square of order \(n\) in which the leading diagonal forms a transversal. Clearly this latter latin square can be prolonged, using the transversal defined by its leading diagonal, to form the addition table for \((N, +, \cdot).\) \(\square\)

In this chapter we demonstrate how several authors have implicitly applied the method of prolongation (or 1-extension) to a particular type of latin square of odd order, which we now define.

**Definition 8.2.** A left diagonally cyclic latin square is a latin square whose broken diagonals are cyclic permutations of the symbol set on which it is defined.

Using Theorem 8.1, it can easily be seen that the square constructed by the prolongation of a left diagonally cyclic latin square is isotopic to the addition table
of a cyclic neofield.

8.2. The squares of Ljamzin and Weisner

Ljamzin [35] and Weisner [57] have each given examples of a pair of orthogonal latin squares of order ten. Although the methods used to construct these pairs are not given, it can be seen that the latin squares are in fact equivalent to the addition tables of cyclic neofields and were most probably generated by the method of prolongation.

One member of Ljamzin's pair is given below. Its orthogonal mate is obtained by rearranging its rows so that its first column is (0, 2, 3, 4, 5, 6, 7, 8, 9, 1).

\[
\begin{array}{cccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & 0 & 5 & 8 & 3 & 2 & 7 & 9 & 6 & 4 \\
2 & 5 & 0 & 6 & 9 & 4 & 3 & 8 & 1 & 7 \\
3 & 8 & 6 & 0 & 7 & 1 & 5 & 4 & 9 & 2 \\
4 & 3 & 9 & 7 & 0 & 8 & 2 & 6 & 5 & 1 \\
5 & 2 & 4 & 1 & 8 & 0 & 9 & 3 & 7 & 6 \\
6 & 7 & 3 & 5 & 2 & 9 & 0 & 1 & 4 & 8 \\
7 & 9 & 8 & 4 & 6 & 3 & 1 & 0 & 2 & 5 \\
8 & 6 & 1 & 9 & 5 & 7 & 4 & 2 & 0 & 3 \\
9 & 4 & 7 & 2 & 1 & 6 & 8 & 5 & 3 & 0
\end{array}
\]

Now, if we apply the mapping

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8
\end{pmatrix},
\]

then we obtain the addition table of a cyclic neofield whose presentation function is given by (0 1)(x x^2)(x^3 x^4 x^5 x^6 x^7 x^8).

If we take the pair of orthogonal latin squares given in fig. 2 of Weisner's paper and move the last rows and last columns so that they form the zeroth rows and zeroth columns respectively and take the transpose of these squares, then they are still orthogonal and one of the squares has the following form.
[Note that its orthogonal mate is found by rearranging its rows so that its first column is given by \((9, 1, 2, 3, 4, 5, 6, 7, 8, 0)\). If we now apply the mapping

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
1 & y & y^2 & y^3 & y^4 & y^6 & y^7 & y^8 & y^9
\end{pmatrix}
\]

we obtain the addition table of a cyclic neofield whose presentation function is \((0 1)(y y^6 y^7 y^8 y^9)(y^5 y^9)\). Finally, we note that the cyclic neofields which correspond to the latin squares of Ljamzin and Weisner are isomorphic since, if we apply the isomorphic mapping \(x \rightarrow y^8\) to Ljamzin’s presentation function, then we obtain that of Weisner. The fact that these latin squares are isotopic was first noted in [11] (p235).

As was mentioned at the end of section 3.5, Hedayat and Seiden [25] stated that the construction which they called sum composition can be modified so as to enable the use of trivial orthogonal latin squares of order one. In particular, they display an orthogonal pair of latin squares of order ten which were formed by the (modified) sum composition of (non-orthogonal) latin squares of order nine and the trivial pair of orthogonal latin squares of order one.

The \(9 \times 9\) latin squares are given below. The underlined cells form a transversal in each square.
Hedayat and Seiden use the indicated transversals and the trivial latin square '9' to obtain the following orthogonal pair of latin squares of order ten.

\[
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
1 & 3 & 6 & 8 & 7 & 2 & 0 & 5 & 4 \\
2 & 6 & 7 & 5 & 1 & 4 & 8 & 3 & 0 \\
3 & 8 & 5 & 4 & 0 & 6 & 2 & 1 & 7 \\
4 & 7 & 1 & 0 & 2 & 3 & 5 & 8 & 6 \\
5 & 2 & 4 & 6 & 3 & 8 & 7 & 0 & 1 \\
6 & 0 & 8 & 2 & 5 & 7 & 1 & 4 & 3 \\
7 & 5 & 3 & 1 & 8 & 0 & 4 & 6 & 2 \\
8 & 4 & 0 & 7 & 6 & 1 & 3 & 2 & 5 \\
\end{array}
\]  
\[
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
2 & 5 & 7 & 6 & 1 & 8 & 4 & 3 & 0 \\
3 & 5 & 6 & 4 & 0 & 3 & 7 & 2 & 8 \\
4 & 7 & 4 & 3 & 8 & 5 & 1 & 0 & 6 \\
5 & 6 & 0 & 8 & 1 & 2 & 4 & 7 & 5 \\
6 & 1 & 3 & 5 & 2 & 7 & 6 & 8 & 0 \\
7 & 8 & 7 & 1 & 4 & 6 & 0 & 3 & 2 \\
8 & 4 & 2 & 0 & 7 & 8 & 3 & 5 & 1 \\
9 & 3 & 8 & 6 & 5 & 0 & 2 & 1 & 4 \\
\end{array}
\]

\(L_1\)
\(L_2\)

However each of these squares is equivalent to the addition table of a cyclic neofield. To see this we once again move the last row and last column of each square so that they form the first row and first column respectively. We then apply the mapping

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
1 & y & y^2 & y^3 & y^4 & y^5 & y^6 & y^7 & y^8 \\
\end{pmatrix}
\]

to obtain the addition table of a cyclic neofield whose presentation function is given by \((0,1)y y^6 y^7 y^2 y^4 y^9(y^5 y^8)\) and whose orthogonal mate is obtained by a reordering of its rows so that its first column is \((0,1)y y^2 y^3 y^4 y^5 y^6 y^7)\). We
observe that this orthogonal pair is now identical to that obtained by Weisner (and hence isomorphic to the orthogonal pair obtained by Ljamzin).

8.3. Self-orthogonal latin squares of order ten

In [57] Weisner gives the first published example of a self-orthogonal latin square of order ten, which we now reproduce.

\[
\begin{array}{cccccccccc}
0 & 2 & 5 & 8 & 6 & 3 & 1 & 9 & 7 & 4 \\
8 & 1 & 3 & 6 & 0 & 7 & 4 & 2 & 9 & 5 \\
9 & 0 & 2 & 4 & 7 & 1 & 8 & 5 & 3 & 6 \\
4 & 9 & 1 & 3 & 5 & 8 & 2 & 0 & 6 & 7 \\
7 & 5 & 9 & 2 & 4 & 6 & 0 & 3 & 1 & 8 \\
2 & 8 & 6 & 9 & 3 & 5 & 7 & 1 & 4 & 0 \\
5 & 3 & 0 & 7 & 9 & 4 & 6 & 8 & 2 & 1 \\
3 & 6 & 4 & 1 & 8 & 9 & 5 & 7 & 0 & 2 \\
1 & 4 & 7 & 5 & 2 & 0 & 9 & 6 & 8 & 3 \\
6 & 7 & 8 & 0 & 1 & 2 & 3 & 4 & 5 & 9 \\
\end{array}
\]

Now on applying the mapping

\[
\begin{pmatrix}
9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
0 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8 & 1 & x & x^2
\end{pmatrix}
\]

and moving the last row and last column to form the zeroth row and zeroth column respectively we obtain the addition table of a cyclic neofield (with rows rearranged) whose presentation function is \((0 \ 1) (x^2 \ x^3 \ x^4 \ x^5 \ x^6 \ x^7 \ x^8 \ 1 \ x \ x^2)\) and whose first column is given by \((0 \ x^7 \ x^8 \ 1 \ x^2 \ x^3 \ x^4 \ x^5 \ x^6)\). We can easily check that such an addition table does indeed form a self-orthogonal latin square by using Theorem 6.4. In the notation of Theorem 6.4 we have that \(y = x^7, g_k = x^{k-1}\) and \(1 \leq k \leq 9\). We therefore require that the set of elements \((x^7 + x^{k-1})^{-1}(x^{k-1}x^7 + 1), 1 \leq k \leq 9\), where \(x^7 + x^{k-1} \neq 0\) are all distinct and not equal to \(x^7\). Now since

\[
(x^7 + x^{k-1})^{-1}(x^{k-1}x^7 + 1) = (1 + x^2x^{k-1}^{-1}x^{k-1}x^7(1 + x^2x^{k-1}^{-1})) = (1 + x^{k+1})^{-1}x^{k-1}(1 + x^{k-1})
\]
as \(k\) varies we obtain the following elements:

\[k = 1: (1 + x^2)^{-1}(1 + x^2) = 1\]
Since these elements are all distinct and not equal to \( x^7 \) the conditions of Theorem 6.4 are satisfied.

In [24] Hedayat uses the method of sum composition to construct a self-orthogonal latin square of order ten. Again this latin square is not only isotopic to the addition table of some cyclic neo-field but is also isotopic to Weisner's self-orthogonal latin square, as we shall now show. We start with Hedayat's self-orthogonal latin square of order ten.

\[
\begin{array}{cccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 9 & 8 & 7 \\
3 & 6 & 5 & 4 & 0 & 8 & 7 & 1 & 9 & 2 \\
9 & 0 & 1 & 7 & 8 & 6 & 3 & 2 & 5 & 4 \\
7 & 9 & 6 & 5 & 2 & 3 & 1 & 0 & 4 & 8 \\
8 & 2 & 9 & 1 & 7 & 4 & 0 & 5 & 6 & 3 \\
1 & 3 & 4 & 9 & 5 & 2 & 8 & 6 & 7 & 0 \\
2 & 5 & 0 & 8 & 9 & 7 & 4 & 3 & 1 & 6 \\
5 & 4 & 7 & 6 & 3 & 9 & 2 & 8 & 0 & 1 \\
6 & 7 & 8 & 2 & 1 & 0 & 9 & 4 & 3 & 5 \\
4 & 8 & 3 & 0 & 6 & 1 & 5 & 7 & 2 & 9 \\
\end{array}
\]
If we move the last row and last column to form the first row and first column respectively and apply the permutation $(0 3 2 8 1 5 6 4)(7)(9)$ we obtain the following latin square:

\[
\begin{array}{cccccccccc}
9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
7 & 3 & 5 & 8 & 2 & 0 & 6 & 4 & 9 & 1 \\
8 & 2 & 4 & 6 & 0 & 3 & 1 & 7 & 5 & 9 \\
0 & 9 & 3 & 5 & 7 & 1 & 4 & 2 & 8 & 6 \\
1 & 7 & 9 & 4 & 6 & 8 & 2 & 5 & 3 & 0 \\
2 & 1 & 8 & 9 & 5 & 7 & 0 & 3 & 6 & 4 \\
3 & 5 & 2 & 0 & 9 & 6 & 8 & 1 & 4 & 7 \\
4 & 8 & 6 & 3 & 1 & 9 & 7 & 0 & 2 & 5 \\
5 & 6 & 0 & 7 & 4 & 2 & 9 & 8 & 1 & 3 \\
6 & 4 & 7 & 1 & 8 & 5 & 3 & 9 & 0 & 2 \\
\end{array}
\]

which on applying the mapping

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8 & 0
\end{pmatrix}
\]

gives the addition table of a cyclic neofield whose presentation function is given by $(0 1)(x x^3 x^7 x^8 x^3 x^2 x^6)$ and whose first column is given by $(0 x^7 x^8 1 x^2 x^3 x^4 x^5 x^6)$ which is identical to that obtained by Weisner.

The present author is in fact unaware of the existence of any self-orthogonal latin square of order ten which is not equivalent to the addition table of some cyclic neofield. In particular Brayton, Coppersmith and Hoffman [8] and [9] use Hedayat's square for their results.

8.4. Todorov's constructions for the results $N(14) \geq 3$ and $N(20) \geq 4$

Todorov [55] constructs an $OA(14, 5)$ which is equivalent to the existence of a set of three mutually orthogonal latin squares of order fourteen. His construction is given below.
First he adds a point \( \infty \) to \( Z_{13} \) and defines, for every \( a \in Z_{13} \)

\[
a + \infty = \infty + a = a \infty = \infty - a = \infty
\]

the remaining addition and multiplication is assumed to be in \( Z_{13} \). Todorov then defines a \( 5 \times 15 \) matrix \( A = [a_{ij}] \) over the set \( Z_{13} \cup \{ \infty \} \) to have the DS property if its rows are mutually orthogonal. However the concept of orthogonal rows has had to be altered slightly to accommodate the element \( \infty \).

**Definition 8.3.** Let \( r_1 = (x_1, x_2, \ldots, x_{13}) \), \( r_2 = (y_1, y_2, \ldots, y_{13}) \) be two rows of \( A \). Then \( r_1 \) and \( r_2 \) are orthogonal if:

(i) \((x_i, y_i) \neq (\infty, \infty), i = 1, 2, \ldots, 15;\)

(ii) \( \exists i, j \) such that \( x_i = \infty, y_j = \infty; \)

(iii) \( \forall a \in Z_{13} \exists (x_i, y_j) \) such that \( x_i - y_j = a. \)

Now for \( b \in Z_{13} \) Todorov defines \( A \oplus b = \|a_{ij} + b\| \) and considers the following \( 5 \times 14^2 \) array, where \( A \) is a \( 5 \times 15 \) DS-matrix defined on \( Z_{13} \cup \{ \infty \} \).

\[
\begin{array}{cccc}
\infty & \infty & A & A \oplus 1 & \cdots & A \oplus 12 \\
\infty & \infty & & & & \\
\infty & & & & & \\
\end{array}
\]

This is clearly an \( OA(14, 5) \) over \( Z_{13} \cup \{ \infty \} \) since, if the rows of \( A \) are mutually orthogonal, then so are the rows of \( A + i \), when \( 1 \leq i \leq 12 \). Thus, instead of searching for an \( OA(14, 5) \), Todorov is able to search for a \( 5 \times 15 \) matrix defined on \( Z_{13} \cup \{ \infty \} \), with the DS property. Todorov goes on to simplify this search even further.

Since an element of \( Z_{13} \) can be added to any row or column of \( A \) without
affecting orthogonality between rows, Todorov standardises the matrix $A$ by assuming that its first row is $(\infty, a, a, \ldots, a)$ and its first column is $(\infty, a, a, \ldots, a)$ for some $a \in Z_{13}$. It is then only necessary to consider the matrix $AR$ formed by deleting the first row and first column of $A$. We then have that the following statements are true.

(i) Every row of $AR$ is a permutation of $Z_{13} \cup \{\infty\}$, since if $r = (x_1, x_2, \ldots, x_{14})$ is a row from $AR$, then $(a, x_1, x_2, \ldots, x_{14})$ is a row from $A$ which is orthogonal to $(\infty, a, a, \ldots, a)$. Thus the set $\{x_i - a, 1 \leq i \leq 14\}$ must all be distinct, which implies that the elements $(x_1, x_2, \ldots, x_{14})$ are themselves all distinct.

(ii) Every column of $AR$ contains distinct elements from $Z_{13} \cup \{\infty\}$, since if $r_1 = (x_1, x_2, \ldots, x_{14})$ and $r_2 = (y_1, y_2, \ldots, y_{14})$ are two rows from $AR$, then $r_1' = (\infty, x_1, x_2, \ldots, x_{14})$ and $r_2' = (\infty, y_1, y_2, \ldots, y_{14})$ are two orthogonal rows from $A$. But the fact that $a - a = 0$ forces $x_i \neq y_i \forall 1 \leq i \leq 14$.

(iii) If $r_1 = (x_1, x_2, \ldots, x_{14})$ and $r_2 = (y_1, y_2, \ldots, y_{14})$ are two rows from $AR$, then $\forall a \in Z_{13} \setminus \{0\}$ exactly one pair $(x_i, y_i)$ such that $a = x_i - y_i$ since $r_1'$ and $r_2'$ are assumed orthogonal.

Note that if the columns of the matrix $AR$ are rearranged so that its first row is $(\infty, 0, 1, \ldots, 12)$ and if we replace the element $\infty$ by 0 and replace the element $i$ by $x^i$, where $x$ is assumed to be a generator for $C_{13}$, then the second, third and fourth rows of $AR$, when written as a permutation of the first row of $AR$, correspond exactly to the presentation functions of cyclic neofields. The orthogonality conditions carry over in an analogous manner so that $AR$ would be equivalent to the existence of a set of three m.o.l.s., each of which is equivalent to the addition table of some cyclic neofield.

Todorov simplifies the search for such a matrix $AR$ as follows:
Suppose \( r_1 = (x_1, \ldots, x_m, x_{m+2}, \ldots, x_{\sigma-1}, \alpha, x_{\sigma+1}, \ldots, x_{14}) \)

\[ r_2 = (y_1, \ldots, y_m, \beta, y_{m+2}, \ldots, y_{\sigma-1}, \alpha, y_{\sigma+1}, \ldots, y_{14}) \]

are orthogonal rows of \( AR \) then

\[
(x_1 - y_1) + \cdots + (x_m - y_m) + (x_{m+2} - y_{m+2}) + \cdots + (x_{\sigma-1} - y_{\sigma-1}) + (x_{\sigma+1} - y_{\sigma+1}) + \cdots + (x_{14} - y_{14}) = 0
\]

since each non-zero \( b \in \mathbb{Z}_{13} \) appears exactly once as \( x_i - y_i = b \) and

\[
\sum_{i=1}^{12} i = (12 \times 13)/2 \equiv 0 \mod 13. \text{ Therefore } \sum_{i=1}^{14} x_i = \sum_{i=1}^{14} y_i \text{ but } (\sum_{i=1}^{14} x_i) + \alpha = 0 \text{ (since } \sum_{i=1}^{12} i \equiv 0 \mod 13) \text{ and } (\sum_{i=1}^{14} y_i) + \beta = 0 \text{ which implies that } \alpha = \beta.
\]

We can then deduce that four columns of \( AR \) represent a symmetric matrix of the form

\[
\begin{pmatrix}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_2 & \alpha_3 & \alpha_4 & \alpha_5 \\
\alpha_3 & \alpha_4 & \alpha_5 & \alpha_6 \\
\alpha_4 & \alpha_5 & \alpha_6 & \alpha_7
\end{pmatrix}
\]

Since, if \( A \) is a DS-matrix so is \( A + b \forall b \in \mathbb{Z}_{13} \), we can further standardise \( AR \) (by adding \(-\alpha\)) to obtain its first four columns in the form

\[
\begin{pmatrix}
\alpha_1 & \alpha_2' & \alpha_3' & \\
\alpha_2' & \alpha_3' & \alpha_4' & \\
\alpha_3' & \alpha_4' & \alpha_5' & \\
\alpha_4' & \alpha_5' & \alpha_6' & \alpha_7
\end{pmatrix}
\]

[In terms of left neofields this represents a rearrangement of the rows of all the addition tables so that the first column of one addition table is in some natural order.]

Furthermore, by using the fact that if \( A \) is a DS-matrix, then so is \( bA \forall b \in \mathbb{Z}_{13} \) we can obtain (by putting \( b = \alpha_2^{-1} \)) the first four columns of \( AR \) in the form
In terms of left neofields this transformation restricts us to finding a set of three latin squares which are unique up to isomorphism.

Todorov carried out an exhaustive computer search which led to three matrices AR being found. On rearranging the columns for one of them we obtain

\[
\begin{bmatrix}
\infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
0 & \infty & \beta_2 & \beta_3 & \beta_4 \\
1 & \beta_2 & \infty & \beta_3 & \beta_4 \\
\beta_1 & \beta_2 & \beta_3 & \infty \\
\end{bmatrix}
\]

In [56] Todorov uses essentially the same technique to construct a set of four m.o.l.s. of order twenty. In fact Todorov presents the following transversal design:

\[
\begin{bmatrix}
\infty & 0 & 7 & 1 & 11 & 1 & 7 & 11 & 2 & 14 & 3 & 4 & 9 & 6 & 5 & 16 & 17 & 10 & 13 & 15 \\
0 & \infty & 0 & 1 & 11 & 7 & 7 & 11 & 1 & 14 & 3 & 2 & 9 & 6 & 4 & 16 & 17 & 5 & 13 & 15 & 10 \\
0 & 0 & \infty & 11 & 7 & 1 & 11 & 1 & 7 & 3 & 2 & 14 & 6 & 4 & 9 & 17 & 5 & 16 & 15 & 10 & 13 \\
7 & 1 & 11 & \infty & 0 & 0 & 16 & 5 & 17 & 9 & 4 & 6 & 14 & 2 & 3 & 7 & 1 & 11 & 15 & 13 & 10 \\
1 & 11 & 7 & 0 & \infty & 0 & 17 & 16 & 5 & 6 & 9 & 4 & 3 & 14 & 2 & 11 & 7 & 1 & 10 & 15 & 13 \\
11 & 7 & 1 & 0 & 0 & \infty & 5 & 17 & 16 & 4 & 6 & 9 & 2 & 3 & 14 & 1 & 11 & 7 & 13 & 10 & 15 \\
\end{bmatrix}
\]

which, on standardising so that the first row becomes \((\infty, 0, \ldots, 0)\) and first column becomes \((\infty, 0, 0, 0, 0, 0)\) we obtain (after deleting the first row and first column and rearranging the remaining columns)

\[
\begin{bmatrix}
19 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\
0 & 19 & 8 & 16 & 5 & 13 & 2 & 10 & 18 & 7 & 15 & 6 & 12 & 1 & 4 & 17 & 9 & 14 & 3 & 11 \\
13 & 4 & 16 & 12 & 17 & 10 & 3 & 8 & 6 & 2 & 18 & 11 & 14 & 0 & 19 & 7 & 1 & 5 & 9 & 15 \\
10 & 6 & 9 & 1 & 18 & 8 & 17 & 15 & 2 & 13 & 12 & 19 & 5 & 3 & 11 & 16 & 7 & 4 & 14 & 0 \\
15 & 9 & 3 & 5 & 11 & 18 & 6 & 12 & 17 & 0 & 13 & 7 & 4 & 10 & 1 & 8 & 19 & 2 & 16 & 14 \\
\end{bmatrix}
\]

Using the same format as that of Table 6.4 we can say that Todorov's results are equivalent to:
8.5. Other related work

In [16] Franklin uses the method of sum composition to obtain what he calls a \textit{bordered cyclic latin square} of order \(2n + 2\) from a left diagonally cyclic latin square of order \(2n + 1\) and the trivial latin square. In fact this method corresponds exactly to the prolongation of a left diagonally cyclic latin square and the bordered cyclic latin squares so obtained are each equivalent to the addition table of some cyclic neofield.

Franklin notes that a left diagonally cyclic latin square is generated from its first row. The following conditions are given for a row \(\sigma\) to generate a left diagonally cyclic latin square, which is defined on the elements \(Z_n\), with addition assumed in \(Z_n\).

Franklin denotes the symbols in positions \(j, j'\) (\(j \neq j'\)) of \(\sigma\) by \(s_j, s_{j'}\) \((0 \leq j, j', s_j, s_{j'} < n)\), then, to generate a left diagonally cyclic latin square, the symbols must satisfy the following two conditions.

\begin{itemize}
  \item[(i)] \(s_j \neq s_{j'}\),
  \item[(ii)] \(s_{j'} - s_j \neq j - j'\) i.e. \(s_j - j \neq s_{j'} - j'\).
\end{itemize}

Now if we define a mapping \(\phi\) such that \(\phi(j) = s_j\) \(0 \leq j < n\), we see that, by (i) \(\phi\) is both one to one and onto \(Z_n\). Furthermore, if we define a mapping \(\theta\) such
that $\theta(j) = s_j - j$, $0 \leq j < n$, then (ii) implies that $\theta$ is also one to one and onto $\mathbb{Z}_n$. Since $\phi(j) = j + \theta(j)$ we must have that $\theta(j)$ is a complete mapping of $\mathbb{Z}_n$ and so Franklin's conditions are exactly those required to construct a cyclic neofield of even order.

For $n = 9$ Franklin obtains 225 such left diagonally cyclic latin squares which he separates into a number of disjoint classes. Franklin then constructs what he calls a bordered cyclic latin square of order $2n + 2$ by replacing the elements of any broken diagonal of a left diagonally cyclic latin square of order $2n + 1$ by a fixed element and then putting the element from the $(i, j)$th cell of this broken diagonal into the $i$th row of the $(n + 1)$th column and the $j$th column of the $(n + 1)$th row. Finally the $(n + 1, n + 1)$th cell contains the fixed element. That this is exactly equivalent to the prolongation of a left diagonally cyclic latin square is easily seen.

Franklin's analysis differs from ours only in that he uses any broken diagonal of a left diagonally cyclic latin square to form a bordered cyclic latin square. In fact if all possible left diagonally cyclic latin squares are generated and we want to generate all possible bordered cyclic latin squares from them, then it is only necessary to use one broken diagonal, say the leading diagonal in each square. We illustrate this with an example. The following is a left diagonally cyclic latin square of order seven.

\[
\begin{bmatrix}
0 & 2 & 6 & 5 & 3 & 1 & 4 \\
5 & 1 & 3 & 0 & 6 & 4 & 2 \\
3 & 6 & 2 & 4 & 1 & 0 & 5 \\
6 & 4 & 0 & 3 & 5 & 2 & 1 \\
2 & 0 & 5 & 1 & 4 & 6 & 3 \\
4 & 3 & 1 & 6 & 2 & 5 & 0 \\
1 & 5 & 4 & 2 & 0 & 3 & 6
\end{bmatrix}
\]

If we now prolong this latin square using the leading and underlined transversals
respectively we obtain the bordered latin squares

<table>
<thead>
<tr>
<th>7</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>7</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>7</td>
<td>5</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>7</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3</td>
<td>7</td>
</tr>
</tbody>
</table>

The left hand square is obviously the addition table of some cyclic neofield.

If we rearrange the rows and columns of the right hand square we can obtain

<table>
<thead>
<tr>
<th>7</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>7</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>0</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>7</td>
<td>0</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>7</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

which is also the latin square obtained if we prolong the following left diagonally cyclic latin square using the leading diagonal.

<table>
<thead>
<tr>
<th>0</th>
<th>4</th>
<th>3</th>
<th>1</th>
<th>6</th>
<th>2</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>2</td>
<td>6</td>
<td>5</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>6</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>4</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

By using each broken diagonal of every left diagonally cyclic latin square to
form a bordered cyclic latin square Franklin, in effect, constructs every bordered cyclic latin square of order $n + 1$, $n$ times.

In [16] Franklin studies orthogonality in both sets of left diagonally cyclic and bordered cyclic latin squares. In Theorem 7.1 of [16] (reproduced below) Franklin gives necessary and sufficient conditions for two left diagonally cyclic latin squares to generate two pairs of orthogonal bordered cyclic latin squares.

**Theorem 8.2** Let $s$ and $r$ be first rows of left diagonally cyclic latin squares $S$ and $R$ of order $n$ such that there are $n - 2$ distinct differences $d_j = s_j - r_j$. Select $n - 2$ columns for which these differences occur. Denote the other two columns by $i$ and $i'$ and the unobserved differences by $d'$ and $d''$. If $s_i - r_i = d'$ say and $s_i + r_i - i = s_i' + r_i' - i'$, then two pairs of orthogonal bordered cyclic latin squares can be constructed.

These orthogonal bordered latin squares are constructed by using either the transversal of $S$ which contains the $i$th element of $s$ and that of $R$ which contains the $i'$th element of $r$ or vice versa.

In a second paper [17] Franklin constructs self-orthogonal bordered cyclic latin squares of even orders $n$, $n \leq 30$, $n \neq 2, 6$. We remind the reader in passing that we have shown that self-orthogonal latin squares exist which are equivalent to the addition tables of cyclic neofields of odd orders $n = 5, 7, 9, 11$ as well as for the left neofield whose multiplicative group is $Q_4$ (i.e. the quaternion group of order eight), see Table 6.1.

In [3] Beresina and Berezina also have applied the method of prolongation to construct pairs of orthogonal latin squares. They noticed that the two latin squares of order nine, which Hedayat and Seiden [25] extended into a pair of orthogonal latin squares of order ten and the latin square of order nine which Hedayat [24] extends to form a self-orthogonal latin square of order ten are all
isomorphic to idempotent left diagonally cyclic latin squares of order nine. Thus
they decided to compute left diagonally cyclic latin squares for various odd orders
and check for orthogonality.

Beresina and Berezina give a condition which is necessary but not sufficient
for two such idempotent left diagonally cyclic latin squares of order \( n \) to extend
into orthogonal latin squares of order \( n + 1 \), namely that in the set of differences
(\( \text{mod} \ n \)) corresponding to the first rows of each of the original latin squares
exactly two of the differences must appear twice.

In fact this necessary condition corresponds exactly to the first part of
Theorem 8.2 above given by Franklin. Finally Beresina and Berezina give
examples of pairs of orthogonal latin squares constructed in this way for orders 8,
10, 12 and 14.
Chapter 9 Further Work

9.0. Introduction

The computational work, which we have carried out, and which led to the results stated in Chapter 6, raised some interesting questions, two of which we discuss now.

In Chapter 6 a surprising result was noted concerning the four non-cyclic groups of order eight. Each of these groups was found to possess the same number of complete mappings. Furthermore, the two non-abelian groups of order eight were found to possess the same number of near complete mappings. These results motivated an investigation into why this was the case and the result of this investigation is presented in section 9.1.

In Chapter 5 we discussed the sequenceability and R-sequenceability of groups in connection with the properties of characteristic and pseudo-characteristic of left neofields. In section 9.2 we discuss a related question which was raised by R.L. Graham [20].

9.1. Complete and near complete mappings of the non-cyclic groups of order 8

In this section we exhibit a natural bijection between the transversals of the Cayley tables of $D_4$ and $Q_4$ (the dihedral and quaternion groups of order eight) and between those of $C_2 \times C_4$ and $C_2 \times C_2 \times C_2$. Furthermore, we show that a similar bijection exists between the near complete mappings of $D_4$ and $Q_4$.

We now exhibit a natural bijection between the canonical form complete mappings of $D_4$ and $Q_4$.

Notation:

$D_4 = \langle a, b, c : a^2 = b, b^3 = c^3 = 1, a \cdot b = b \cdot a, b \cdot c = c \cdot b, c \cdot a = a \cdot b \cdot c \rangle$, 
Theorem 9.1. There exists a natural bijection between the complete mappings of $D_4$ and $Q_4$.

Proof. Let $\theta_d$ be a complete mapping of $D_4$, in canonical form, then

$$\theta_d = \left( \begin{array}{cccc}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \end{array} \right) \left( \begin{array}{cccc}
\beta_1 & \beta_2 & \beta_3 & \beta_4 \\
\beta_5 & \beta_6 & \beta_7 & \beta_8 \end{array} \right)$$

where $\alpha_i \in (a, b, ab)$ and $\beta_i \in B$, for all $i$.

Furthermore, since $\theta_d$ is a complete mapping of $D_4$, we have that $\phi_d(x) = x \cdot \theta_d(x)$ is a bijection of $D_4$.

[Note that if $\theta_d$ is a mapping with a different structure, e.g.

$$\theta_d = \left( \begin{array}{cccc}
\alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\
\alpha_5 & \alpha_6 & \alpha_7 & \alpha_8 \end{array} \right) \left( \begin{array}{cccc}
\beta_1 & \beta_2 & \beta_3 & \beta_4 \\
\beta_5 & \beta_6 & \beta_7 & \beta_8 \end{array} \right), \text{ then } x \cdot \theta(x) \text{ is not a bijection on } D_4.]$

We now consider two cases.

(1) If $\phi_d(\beta_3) = b \cdot \phi_d(\beta_3)$, then $\theta_d = \theta_d$ is a canonical form complete mapping of $Q_4$.

This follows since $\phi_d(x) = \phi_d(x), \forall x \in A \cup \{\beta_1, \beta_2\}, \phi_d(\beta_3) = \beta_3 \cdot \beta_7 = b \cdot \beta_3 \cdot \beta_7 = b \cdot \phi_d(\beta_3)$
\[ \phi_d(\beta_4) = \phi_d(\beta_3) \] and, similarly, \[ \phi_d(\beta_4) = \phi_d(\beta_3). \] Therefore \( \phi_d \) is a bijection of \( Q_4 \) since \( \phi_d \) is a bijection of \( D_4 \).

(2) If \( \phi_d(\beta_3) = b \cdot \phi_d(\beta_3) \), then \( \theta_d \), defined by \( \theta_d(x) = \theta_d(x), \forall x \in A \cup \{ \beta_1, \beta_2 \}, \theta_d(\beta_3) = \beta_3, \theta_d(\beta_4) = \beta_4 \), is a canonical form complete mapping of \( Q_4 \). Since \( \theta_d(x) = \theta_d(x), \forall x \in A \cup \{ \beta_1, \beta_2 \} \), it is sufficient to show that \( \langle \phi_d(\beta_3), \phi_d(\beta_4) \rangle = \langle \phi_d(\beta_3), \phi_d(\beta_4) \rangle \), where \( \phi_d(\beta_3) = \beta_3 \beta_8 \) and \( \phi_d(\beta_4) = \beta_4 \beta_4 \). Now \( \beta_3 \beta_8 = b \cdot \beta_3 \beta_8 = b \cdot \phi_d(\beta_3) \neq \phi_d(\beta_4) \), similarly \( \beta_4 \beta_4 = \phi_d(\beta_4) \), hence \( \langle \phi_d(\beta_3), \phi_d(\beta_4) \rangle = \langle \beta_3 \beta_8, \beta_4 \beta_4 \rangle \) but clearly \( \langle \beta_3 \beta_8, \beta_4 \beta_4 \rangle = \langle \beta_3 \beta_8, \beta_4 \beta_4 \rangle \) and so we must have that \( \beta_3 \beta_8, \beta_4 \beta_4 \rangle = \langle \phi_d(\beta_3), \phi_d(\beta_4) \rangle \). Thus \( \phi_d \) is a bijection on \( Q_4 \).

To complete the proof we observe that the above function from the canonical form complete mappings of \( D_4 \) into those of \( Q_4 \) is a bijection. \( \square \)

Table 6.5 shows that there are in fact 48 canonical form complete mappings for both \( D_4 \) and \( Q_4 \). Thus, by Theorem 1.5, there is a total of 384 complete mappings for each group and hence 384 transversals of the Cayley tables of each group.

**Theorem 9.2.** There exists a natural bijection between the complete mappings of \( C_2 \times C_4 \) and \( C_2 \times C_2 \times C_2 \).

**Proof.** The proof is exactly analogous to that of Theorem 9.1, where for \((D_4, \cdot)\) and \((Q_4, \cdot)\) we substitute \((C_2 \times C_2, \circ)\) and \((C_2 \times C_4, \circ)\) respectively. \( \square \)

Table 6.5 shows that there are again 48 canonical form complete mappings of both \( C_2 \times C_2 \times C_2 \) and \( C_2 \times C_4 \). This would seem to suggest that there might be a further natural bijection between the complete mappings of \( D_4 \) and \( Q_4 \) and those of \( C_2 \times C_2 \times C_2 \) and \( C_2 \times C_4 \), but such a bijection has yet to be found.

Finally, we show that a similar natural bijection exists between the near complete mappings of \( D_4 \) and \( Q_4 \). We shall need the following two Lemmas.
Lemma 9.1 (Paige [44]). If \((G, \cdot)\) is a group of order \(n\) which has a complete mapping, then there exits an ordering, \(a_1, a_2, \ldots, a_n\) of \(G\), such that \(a_1a_2\cdots a_n = 1\).

Proof. Let \(\theta\) be a complete mapping of the group \((G, \cdot)\), where 
\[
\phi = (g_{11} g_{12} \cdots g_{1k_1}) \cdots (g_{1s} g_{2s} \cdots g_{sk_s})
\]
is the corresponding orthomorphism. Then
\[
\prod_{l=1}^{s} \prod_{j=1}^{k_l} \theta(g_{ij}) = \prod_{l=1}^{s} (g_{1l}^{-1}g_{2l})(g_{2l}^{-1}g_{3l})\cdots (g_{kl}^{-1}g_{1l}) = 1.
\]

Lemma 9.2 (Keedwell [33]). If \(\eta\) is the exdomain element of a near complete mapping \(\theta\) of a group \((G, \cdot)\), then there exists an ordering, \(a_1, a_2, \ldots, a_n\) of \(G\), such that \(a_1a_2\cdots a_n = \eta\).

Proof. Let \(\theta\) be a near complete mapping of the group \((G, \cdot)\), where 
\[
\phi = [g_1^1 g_2^1 \cdots g_h^1] \cdots (g_{11} g_{12} \cdots g_{1k_1}) \cdots (g_{1s} g_{2s} \cdots g_{sk_s})
\]
is the corresponding near orthomorphism. Then
\[
\left[ \prod_{j=1}^{h} \theta(g_j) \right] \left[ \prod_{j=1}^{s} \prod_{i=1}^{k_i} \theta(g_{ij}) \right] = \eta,
\]
since \(\prod_{j=1}^{h} \theta(g_j) = (g_{11}^{-1}g_{2l})(g_{2l}^{-1}g_{3l})\cdots (g_{kl}^{-1}g_{1l}) = 1\) and \(\prod_{j=1}^{k_i} \theta(g_{ij}) = (g_{1l}^{-1}g_{2l})(g_{2l}^{-1}g_{3l})\cdots (g_{kl}^{-1}g_{1l})\)
\(= g_{1l}^l g_{hl} = \eta\), since \(g_{1l}^l = 1\) and \(g_{hl}^l = \eta\). \qed

Theorem 9.3. There exists a natural bijection between the near complete mappings of \(D_4\) and \(Q_4\).

Proof. For both \(D_4\) and \(Q_4\) the set of elements in the commutator subgroup is \(\{1, b\}\).
It is well known that the product of all the elements of a group, in any order, is always in the same coset of its commutator subgroup. Since both \(D_4\) and \(Q_4\) possess complete mappings the product of all the elements in either of these groups is 1 or \(b\) (using Lemma 9.1). Thus, by Lemma 9.2, we have that, in any canonical form near complete mapping \(\theta\) of \(D_4\) or \(Q_4\), \(\eta = b\). Therefore,
\[ \theta_d = \begin{pmatrix} 1 & \alpha_2 & \alpha_3 & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \alpha_5 & \beta_5 & \beta_6 & \alpha_7 & \alpha_8 & \beta_7 & \beta_8 \end{pmatrix} \]

where \( \{1, \alpha_2, \alpha_3\} = A \setminus \{\beta\}; \{\alpha_5, \alpha_7, \alpha_8\} = A \setminus \{1\} \) and \( \{\beta_1, \beta_2, \beta_3, \beta_4\} = \{\beta_5, \beta_6, \beta_7, \beta_8\} \equiv B \).

With the notation so chosen we can now establish a bijection between the canonical form near complete mappings of \( D_4 \) and \( Q_4 \), similar to that which exists between the canonical form complete mappings. □

Table 6.5 shows that there are in fact 16 canonical form near complete mappings for both \( D_4 \) and \( Q_4 \).

### 9.2. The \( r \)-set sequenceability of abelian groups

The following question was raised by R.L. Graham [20].

"Given a group \((G, \cdot)\), of order \( n \), for which integers \( 0 < r \leq n \), does every \( r \)-set of \( G \) have an ordering such that all partial products are different?"

For our discussion of this question, we shall find it convenient to make the following two definitions.

**Definition 9.1.** An ordering of the elements of a subset \( S \) of \( G \), in which all the partial products are different, is called a sequencing of \( S \) in \((G, \cdot)\).

**Definition 9.2.** A group \((G, \cdot)\) with the property that, for a particular positive integer \( r \), every \( r \)-set of \( G \) possesses a sequencing, is called an \( r \)-set-sequenceable group.

In terms of these definitions Graham's question is equivalent to asking: "For which values of \( r \) is a given group \( r \)-set-sequenceable?"

In this chapter we solve this question for abelian groups, for all \( r \), except that for \( r = n - 1 \), the question remains partly unsolved for some groups, namely those groups for which it is unknown whether the group is \( R \)-sequenceable. In particular, all groups are both 1-set and 2-set-sequenceable. The only abelian groups which are 3-set-sequenceable are the generalised Klein groups. For
3 < r < n−2, no abelian group is r-set sequenceable. The only abelian groups of
order n > 4 which are (n−2)-set-sequenceable are the generalised Klein. We can
see immediately from our definitions that a group is n-set-sequenceable if and only
if it is sequenceable and it is well known that an abelian group is sequenceable if
and only if it contains a unique element of order two. Similarly we will show that
a group is (n−1)-set-sequenceable if and only if it is R-sequenceable. Regarding
non-abelian groups we observe that, if (G, ·) is a non-abelian group which contains
a subgroup which is isomorphic to an abelian group (H, ·), then for those values of
r for which (H, ·) is not r-set-sequenceable neither is (G, ·).

We shall need the following lemmas.

Lemma 9.3 (Miller [39]). If (G, ·) is an abelian group of order n, then \( \prod_{i=1}^{n} g_i = 1 \),
unless (G, ·) possesses a unique element of order two, say g', in which case
\( \prod_{i=1}^{n} g_i = g' \).

Proof. If (G, ·) possesses no element of order two, then the total product of its
elements can be written in the form \( 1g_1g_1^{-1}g_2g_2^{-1}\cdots g_ng_n^{-1} \) which is clearly equal to 1.
Similarly, if (G, ·) has a unique element g' of order two, then the total product of
its elements is \( 1g_1g_1^{-1}g_2g_2^{-1}\cdots g_ng_n^{-1}g' = g' \). Thus we need now only to consider those
groups which contain more than one element of order two. Using an argument
similar to the above we can see that the total product of the elements in such a
group will be equal to the total product of the elements of order two in that group.
Now the elements of order two, together with the identity element, form a
subgroup (H, ·) of (G, ·) where |H| = 2^r, r > 1. Let \( c_1, c_2, \ldots, c_r \) be a minimal set of
generators for (H, ·), then each element of H can be represented in the form
\( c_1^{\alpha_1}c_2^{\alpha_2}\cdots c_r^{\alpha_r} \), where the \( \alpha_i's \) either take the value 0 or 1. Now each generator \( c_i \) will
be present in the representation of exactly half of the elements of H and so we
have that, in the total product of the elements of H, each generator will occur \( 2^{r-1} \)
times. Since \( r > 1 \) each generator occurs an even number of times and, since they
are all of order two, the total product of the elements of \((H, \cdot)\) is 1. □

[Lemma 9.3 has been rediscovered on several occasions. For an historical note, see [13].]

**Lemma 9.4.** If \(1 \in S\) and \(S\) possesses a sequencing \(s_1, s_2, \ldots, s_n\), then \(s_i = 1\).

**Proof.** If \(s_i = 1\) and \(i \neq 1\), then \(s_1s_2\cdots s_{i-1}s_i = s_1s_2\cdots s_i\) and so the partial products are not all distinct. □

**Lemma 9.5.** If \(S\) is an \(r\)-set of \(G\) such that \(1 \in S\) and \(\prod_{i=1}^{r}s_i = 1\), then, in any ordering of \(S\), there must be a repeated partial product.

**Proof.** By Lemma 9.4 if \(S\) possesses a sequencing \(s_1, s_2, \ldots, s_n\), then \(s_1 = 1\) but \(s_1s_2\cdots s_r = 1\) and so the partial products are not all distinct. □

**Lemma 9.6.** An abelian group \((G, \cdot)\) of order \(n\) is \(n\)-set-sequenceable if and only if it possesses a unique element of order two.

**Proof.** By definition, \((G, \cdot)\) is \(n\)-set-sequenceable if and only if \((G, \cdot)\) is sequenceable. By Gordon [19], an abelian group is sequenceable if and only if it possesses a unique element of order two. □

**Theorem 9.4.** An abelian group \((G, \cdot)\) of order \(n\) is \((n-1)\)-set-sequenceable if and only if \((G, \cdot)\) is \(R\)-sequenceable.

**Proof.** If \((G, \cdot)\) possesses a unique element \(g'\) of order two, then, by Lemmas 9.3 and 9.5, the \((n-1)\)-set \(G\setminus\{g'\}\) possesses no sequencing. Thus, using Lemma 9.6, if \((G, \cdot)\) is sequenceable, then it is not \((n-1)\)-set-sequenceable. Hence, if \((G, \cdot)\) is \((n-1)\)-set-sequenceable, then \((G, \cdot)\) does not possess a unique element of order two and so \(\prod_{i=1}^{n}g_i = 1\), by Lemma 9.3.
Now suppose \((G, \cdot)\) is \((n-1)\)-set-sequenceable, then \(\forall (n-1)\) sets \(S \subseteq \) an ordering, say \(s_1, s_2, \ldots, s_{n-1}\), which forms a sequencing of \(S\). If the omitted element is the identity, then the ordering \(1, s_1, s_2, \ldots, s_{n-1}\) is an R-sequencing of \((G, \cdot)\). If, however, the omitted element \(s_n\) is not the identity, then the ordering \(s_1, s_2, \ldots, s_{n-1}, s_n\) is an R-sequencing of \((G, \cdot)\).

Conversely, suppose \((G, \cdot)\) is R-sequenceable, we saw in the proof of part (i) of Theorem 5.8 that the cyclic sequence \((c_2, c_3, \ldots, c_n)\) defines an \((n-1),1)\) orthomorphism of \((G, \cdot)\) if and only if the sequence \(c_1, c_1^{-1}c_2, c_2^{-1}c_3, \ldots, c_{n-1}^{-1}c_n\) is an R-sequencing of \((G, \cdot)\). But if \((c_2, c_3, \ldots, c_n)\) defines an \((n-1),1)\) orthomorphism of \((G, \cdot)\), then so does \((c_{n+1}, c_n, c_2, \ldots, c_1)\) and hence \(c_1, c_1^{-1}c_{n+1}, \ldots, c_{n-1}^{-1}c_n, c_n^{-1}c_{n-1}, \ldots, c_1^{-1}c_2\) is also an R-sequencing of \((G, \cdot)\). The first \((n-1)\) elements of this R-sequencing forms a sequencing of the \((n-1)\)-set \(G\setminus \{c_i^{-1}c_i\}\). Since the elements \(c_i^{-1}c_1, 2 \leq i \leq n\) exhaust the set \(G\setminus \{1\}\) we require only the further observation that \(c_1^{-1}c_2, c_2^{-1}c_3, \ldots, c_{n-1}^{-1}c_n\) is a sequencing of the \((n-1)\)-set \(G\setminus \{1\}\) to complete the proof. □

Theorem 9.4 raises the question: which finite abelian groups are R-sequenceable? We know that a necessary condition for R-sequenceability is that the group does not possess a unique element of order two. It has been conjectured that this condition is also sufficient. In [18], Friedlander, Gordon and Miller showed that the following types of abelian group are R-sequenceable:

(i) Cyclic groups of odd order;

(ii) Abelian groups of odd order whose Sylow 3-subgroup is cyclic;

(iii) Abelian groups of orders which are relatively prime to six;

(iv) Elementary abelian \(p\)-groups, except \(C_2^3\);

(v) Abelian groups of type \(C_2 \times C_{4k}\);

(vi) Abelian groups whose Sylow 2-subgroup \(S\) is one of the following
kinds:

(a) \( S = (C_2)^m, m > 1 \) but \( m \neq 3 \).

(b) \( S = C_2 \times C_h \), where \( h = 2^k \) and either \( k \) is odd or else \( k \geq 2 \) is even and \( G/S \) has a direct cyclic factor of order congruent to 2 modulo 3.

Also Ringel [49] has claimed that abelian groups of type \( C_2 \times C_{6k+2} \) are R-sequenceable.

It is easy to see that all groups are both 1-set and 2-set-sequenceable. To consider \( r \)-set-sequenceability of abelian groups for \( 2 < r < n - 1 \), we examine several cases.

**Theorem 9.5.** If \((G, \cdot)\) is an abelian group of order \( n \), where either \( n \) is odd or \((G, \cdot)\) has a unique element \( \eta \) of order two, then it is not \( r \)-set-sequenceable for \( 2 < r < n - 1 \).

**Proof.** For \( r \) odd, \( 2 < r < n - 1 \), the \( r \)-set \( S = \{1, g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_{(n-1)/2}, g_{(n-1)/2}^{-1}\} \) (where if \( n \) is even, then \( \eta \notin S \)) possesses no sequencing, by Lemma 9.5.

For \( r \) even, \( 2 < r < n - 1 \), the \( r \)-set \( S = \{1, g_1, g_2, (g_1g_2)^{-1}, g_3, g_3^{-1}, \ldots, g_{r/2}, g_{r/2}^{-1}\} \), where if \( n \) is odd, then \( S \cap \{g_1^{-1}, g_2^{-1}, g_1g_2\} = \emptyset \) and if \( n \) is even, then \( g_1 = \eta \) and \( S \cap \{g_2^{-1}, \eta g_2\} = \emptyset \), possesses no sequencing, by Lemma 9.5. [Note that for this construction when \( n \) is odd we require \( r \leq n - 3 \) but, since \( n - 2 \) is odd, this is sufficient for all even values of \( r < n - 1 \).] \( \square \)

**Theorem 9.6.** If \((G, \cdot)\) is an abelian group of order \( n \) which possesses more than one element of order two and at least one non-identity element not of order two, then \((G, \cdot)\) is not \( r \)-set-sequenceable for \( 2 < r < n - 1 \).

**Proof.** \((G, \cdot)\) must possess at least \( n/2 \) non-identity elements not of order two since the elements of order two, together with the identity, form a subgroup of index at
least two in \((G, \cdot)\).

For \(r\) odd, \(2 < r \leq (n/2) + 1\), the \(r\)-set \(S = \{1, g_1, g_1^{-1}, g_2, g_2^{-1}, \ldots, g_{(r-1)/2}, g_{(r-1)/2}^{-1}\}\) possesses no sequencing, by Lemma 9.5, where none of the elements of \(S\) has order two.

For \(r\) even, \(2 < r \leq (n/2) + 1\), the \(r\)-set \(S = \{1, g_1, g_2g_2, g_2, g_2^{-1}, \ldots, g_{r/2}, g_{r/2}^{-1}\}\), possesses no sequencing, by Lemma 9.5, where \(g_1, g_2\) and hence \(g_1g_2\) are of order two whilst the remaining elements of \(S\) are not.

For \(r\), when \(n/2 < r < n - 1\), the \(r\)-set \(S = (G \setminus S') \cup \{1\}\), where \(S'\) is an \((n-r+1)\)-set of the appropriate one of the two types constructed above, possesses no sequencing, by Lemmas 9.3 and 9.5. □

**Theorem 9.7.** If \((G, \cdot)\) is an abelian group of order \(n \geq 4\) in which every non-identity element has order two, then \((G, \cdot)\) is 3-set-sequenceable.

**Proof.** Any 3-set \(S\) must possess a sequencing since, if we consider the ordering \(s_1, s_2, s_3\), we obtain the partial products \(s_1, s_1s_2, s_1s_2s_3\). These partial products must all be distinct since \(s_1 = s_1s_2 \iff s_2 = 1\) and \(s_1s_2 = s_1s_2s_3 \iff s_3 = 1\), but, by Lemma 9.4, \(s_1 = 1\) when \(1 \in S\). The remaining possibility is \(s_1 = s_1s_2s_3\), but \(s_1 = s_1s_2s_3 \iff s_2s_3 = 1\), contrary to the hypothesis that every element has order two. □

**Theorem 9.8.** If \((G, \cdot)\) is an abelian group of order \(n \geq 8\) in which every non-identity element has order two, then \((G, \cdot)\) is not \(r\)-set-sequenceable for \(3 < r < n - 2\) and for \(r = n\).

**Proof.** The proof is by induction on the size of a minimal generating set of \((G, \cdot)\). We first note that, since every element has order 2, \((G, \cdot)\) must be the generalised Klein group of order \(n = 2^m\), for some \(m\). We denote a minimal set of generators of \((G, \cdot)\) by \(\{c_1, c_2, \ldots, c_m\}\).

As our starting point for the induction argument we take the generalised
Klein group of order eight. Now, for $r = 4$, the set $S = \langle 1, e_1, e_2, e_1e_2 \rangle$ has no sequencing and, for $r = 5$, the set $S = \langle 1, e_1, e_2, e_3, e_1e_2e_3 \rangle$ has no sequencing, also, for $r = 8$, the group has no sequencing, by Lemma 9.6. Thus for $3 < r < 6$ and $r = 8$, $\exists$ $r$-sets $S$ which possess no sequencing.

We now consider $(G, \cdot)$ to be an arbitrary generalised Klein group of order $2^m$, $m > 3$, and assume that, for the generalised Klein group of order $2^{m-1}$, the theorem is true. That is, $\exists$ $r$-sets $S$ for which no sequencing is possible when $3 < r < 2^{m-1} - 2$ and $r = 2^{m-1}$. Since the set $\{e_1, e_2, \ldots, e_{m-1}\}$ generates a subgroup $(H, \cdot)$ of $(G, \cdot)$ isomorphic to the generalised Klein group of order $2^{m-1}$, $\exists$, by assumption, $r$-sets $S$ of $G$ for which no sequencing exists $\forall r$ when $3 < r < 2^{m-1} - 2$ and $r = 2^{m-1}$. Furthermore, the product of all the elements in $H$ is the identity element, by Lemma 9.3. It follows that:

for $r = 2^{m-1} - 1$, the set $S = H \setminus \{c_1, c_3, c_1c_2c_3\} \cup \{c_2c_m, c_1c_2c_m\}$ possesses no sequencing, by Lemma 9.5;

for $r = 2^{m-1} - 2$, the set $S = H \setminus \{c_1, c_1c_2, c_1c_3, c_2c_3\} \cup \{c_2c_m, c_1c_2c_m\}$ possesses no sequencing, by Lemma 9.5.

Thus $\exists$ $r$-sets $S$ of $G$ which possess no sequencing for $3 < r < 2^{m-1}$. For $2^{m-1} < r < 2^m$, the set $S = (G \setminus S') \cup \{1\}$ possesses no sequencing, where $S'$ is an $(n-r+1)$-set of the appropriate one of the two types constructed above.

We have shown that the generalised Klein group $(G, \cdot)$ of order $n = 2^m$, $m \geq 3$, is not $r$-set-sequenceable for $r$, when $3 < r < 2^m - 2$. Furthermore, since $(G, \cdot)$ is not sequenceable, by Lemma 9.3, it is not $n$-set-sequenceable. $\square$

In [18], Friedlander, Gordon and Miller give the following construction for an $R$-sequencing of the additive group of $GF(p^m) \cong Z_2$, where $t = p^m - 2$ and $\alpha$ is a generator of the (cyclic) multiplicative group.
Here the top row contains the sequencing whilst the bottom row contains the partial 'products'. Since we are dealing with the additive group of a field the 'products' are in fact sums in this case. We make use of this result in the following theorem.

**Theorem 9.9.** If \((G, \cdot)\) is an abelian group of order \(n \geq 8\) in which every non-identity element has order two, then \((G, \cdot)\) is \((n-2)\)-set-sequenceable.

**Proof.** For any given pair of non-identity elements \((x, y)\) \exists a minimal set of generators \(C\) such that \((x, y) \subseteq C\). Hence, given any R-sequencing \(a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\) of \((G, \cdot)\), we can always find an isomorphism \(\theta\) of \((G, \cdot)\) such that \(\theta(a_{n-1}) = x\) and \(\theta(a_n) = y\). Then, since the ordering \(\theta(a_1), \theta(a_2), \ldots, \theta(a_{n-2}), \theta(a_{n-1}), \theta(a_n)\) forms an R-sequencing of \((G, \cdot)\), the ordering \(\theta(a_1), \theta(a_2), \ldots, \theta(a_{n-2})\) forms a sequencing of the set \(G \setminus \{x, y\}\). To complete the proof we note that \(\theta(a_2), \theta(a_3), \ldots, \theta(a_{n-2}), \theta(a_{n-1})\) is a sequencing of \(G \setminus \{1, y\}\). □

The question of \(r\)-set-sequenceability of the Klein group itself is trivial, since, for \(r = 1, 2, 3\), we have that all \(r\)-sets possess a sequencing whilst for \(r = 4\) no such sequencing is possible, by Lemma 9.3.
Chapter 10 Conclusions

One of the stated aims of this thesis was to describe the constructions used in obtaining the greatest known lower bounds of $N(n)$ for $n \leq 32$ and to show how several of these constructions are closely related.

In Chapter 2 we described how Bose proved that the existence of a finite projective plane of order $n$ is equivalent to the existence of a complete set of m.o.l.s. of order $n$. In particular, the existence of a Desarguesian plane for all prime power orders ensures that $N(p^r) = p^r - 1$. The construction implied by this fact (which we called the Bose construction) may be viewed in two different ways. Firstly, the complete set of m.o.l.s. which defines the Desarguesian plane is based on the Cayley table of an abelian $p$-group and as such can be thought of as being the result of an application of the orthomorphism method (as discussed in Chapter 4). In Chapter 4 we showed how the orthomorphism method itself has been used directly to show that $N(12) \geq 5$, $N(15) \geq 4$, $N(21) \geq 4$ and $N(24) \geq 4$. Furthermore, it was shown that the construction implied by MacNeish's theorem (which provides the greatest known lower bound for $N(28)$, namely $N(28) \geq 3$) can also be viewed as an application of the orthomorphism method. Secondly, the Bose construction may be thought of in the following way. The Galois field, from which we obtain a Desarguesian plane, is a particular type of cyclic neofield. When thought of as such the Bose construction is similar to Todorov's constructions for $N(14) \geq 3$ and $N(20) \geq 4$ as well as all known constructions for self-orthogonal latin squares of order ten, which were discussed in Chapter 8. In Chapter 5 we saw that a cyclic neofield of order $n + 1$ is equivalent to the existence of either an orthomorphism or near orthomorphism of the cyclic group of order $n$. Thus, the greatest known lower bounds for $N(n)$, $n \in \{2, 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 27, 28, 29, 31, 32\}$ can all be attained using constructions which depend on the existence of orthomorphisms or near orthomorphisms of groups.
In the above discussion the result \( N(10) \geq 2 \) was attained using a self-orthogonal latin square. This was not the first example of a pair of orthogonal latin squares of order ten. In Chapter 3 we described Parker's method which proved that \( N(12s + 10) \geq 2 \) for all \( s \geq 0 \). We also described how Parker's method and Yamamoto's method are closely related in the sense that the orthogonal latin squares which can be obtained by an application of Parker's method are isotopic to latin squares which can be obtained by an application of Yamamoto's generating principle. It was further shown that Yamamoto's method and Parker's method are equivalent for certain orders.

As for the remaining orders, the result \( N(1) = \infty \) is trivial and \( N(6) = 1 \) does not provide any construction for consideration. The remaining greatest known lower bounds for \( N(n) \), \( n \leq 32 \), are \( N(n) \geq 3 \), \( n \in \{18, 22, 26, 30\} \) all of which were attained by Wang's method. Although the latin squares obtained by Wang's method cannot themselves be obtained as a result of applying Yamamoto's generating principle similarities do exist between the two methods which were discussed in Chapter 3.

Finally, Yamamoto's generating principle may be thought of in terms of the generalised (or repeated) prolongation of a latin square. In Chapter 8 (Theorem 8.1) we established a strong connection between prolongation and a certain type of left neofield namely a left neofield which is defined by an orthomorphism of its multiplicative group. When Yamamoto's generating principle involves the repeated prolongation of a Cayley table of a group, as is the case with Parker's method and the results of Theorem 3.4 for example, then these methods can also be seen to depend on the existence of group orthomorphisms.
References


