On the existence and enumeration of sets of two or three mutually orthogonal Latin squares with application to sports tournament scheduling

Martin Philip Kidd

Dissertation presented for the degree of
Doctor of Philosophy
in the Faculty of Science at Stellenbosch University

Promoter: Prof JH van Vuuren
Co-promoter: Dr AP Burger

March 2012

Declaration

By submitting this dissertation electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: March 1, 2012

Abstract

A Latin square of order n is an $n \times n$ array containing an arrangement of n distinct symbols with the property that every row and every column of the array contains each symbol exactly once. It is well known that Latin squares may be used for the purpose of constructing designs which require a balanced arrangement of a set of elements subject to a number of strict constraints. An important application of Latin squares arises in the scheduling of various types of balanced sports tournaments, the simplest example of which is a so-called *round-robin tournament* — a tournament in which each team opposes each other team exactly once.

Among the various applications of Latin squares to sports tournament scheduling, the problem of scheduling special types of mixed doubles tennis and table tennis tournaments using special sets of three mutually orthogonal Latin squares is of particular interest in this dissertation. A so-called *mixed doubles table tennis (MDTT) tournament* comprises two teams, both consisting of men and women, competing in a mixed doubles round-robin fashion, and it is known that any set of three mutually orthogonal Latin squares may be used to obtain a schedule for such a tournament. A more interesting sports tournament design, however, and one that has been sought by sports clubs in at least two reported cases, is known as a *spouse-avoiding mixed doubles round-robin (SAMDRR) tournament*, and it is known that such a tournament may be scheduled using a *self-orthogonal Latin square with a symmetric orthogonal mate (SOLSSOM).*

These applications have given rise to a number of important unsolved problems in the theory of Latin squares, the most celebrated of which is the question of whether or not a set of three mutually orthogonal Latin squares of order 10 exists. Another open question is whether or not SOLSSOMs of orders 10 and 14 exist. A further problem in the theory of Latin squares that has received considerable attention in the literature is the problem of counting the number of (essentially) different ways in which a set of elements may be arranged to form a Latin square, *i.e.* the problem of enumerating Latin squares and equivalence classes of Latin squares of a given order. This problem quickly becomes extremely difficult as the order of the Latin square grows, and considerable computational power is often required for this purpose. In the literature on Latin squares only a small number of equivalence classes of *self-orthogonal Latin squares* (SOLS) have been enumerated, namely the number of distinct SOLS, the number of idempotent SOLS and the number of isomorphism classes generated by idempotent SOLS of orders $4 \leq n \leq 9$. Furthermore, only a small number of equivalence classes of ordered sets of k *mutually orthogonal Latin squares (k-MOLS)* of order n have been enumerated in the literature, namely main classes of 2-MOLS of order n for $3 \leq n \leq 8$ and isotopy classes of 8-MOLS of order 9. No enumeration work on SOLSSOMs appears in the literature.

In this dissertation a methodology is presented for enumerating equivalence classes of Latin squares using a recursive, backtracking tree-search approach which attempts to eliminate redundancy in the search by only considering structures which have the potential to be completed to well-defined class representatives. This approach ensures that the enumeration algorithm

only generates one Latin square from each of the classes to be enumerated, thus also generating a repository of class representatives of these classes. These class representatives may be used in conjunction with various well-known enumeration results from the theory of groups and group actions in order to determine the number of Latin squares in each class as well as the numbers of various kinds of subclasses of each class.

This methodology is applied in order to enumerate various equivalence classes of SOLS and SOLSSOMs of orders up to and including order 10 and various equivalence classes of k-MOLS of orders up to and including order 8. The known numbers of distinct SOLS, idempotent SOLS and isomorphism classes generated by idempotent SOLS are verified for orders $4 \leq n \leq 9$, and in addition the number of isomorphism classes, transpose-isomorphism classes and RC-paratopism classes of SOLS of these orders are enumerated. The search is further extended to determine the numbers of these classes for SOLS of order 10 via a large parallelisation of the backtracking tree-search algorithm on a number of processors. The RC-paratopism class representatives of SOLS thus generated are then utilised for the purpose of enumerating SOLSSOMs, while existing repositories of symmetric Latin squares are also used for this purpose as a means of validating the enumeration results. In this way distinct SOLSSOMs, standard SOLSSOMs, transpose-isomorphism classes of SOLSSOMs and RC-paratopism classes of SOLSSOMs are enumerated, and a repository of RC-paratopism class representatives of SOLSSOMs is also produced. The known number of main classes of 2-MOLS of orders $3 \leq n \leq 8$ are verified in this dissertation, and in addition the number of main classes of k-MOLS of orders $3 \leq n \leq 8$ are also determined for $3 \leq k \leq n-1$. Other equivalence classes of k-MOLS of order n that are enumerated include distinct k-MOLS and reduced k-MOLS of orders $3 \leq n \leq 8$ for $2 \leq k \leq n-1$.

Finally, a filtering method is employed to verify whether any SOLS of order 10 satisfies two basic necessary conditions for admitting a common orthogonal mate with its transpose, and it is found via a computer search that only four of the 121 642 class representatives of RC-paratopism classes of SOLS satisfy these conditions. It is further verified that none of these four SOLS admits a common orthogonal mate with its transpose. By this method the spectrum of resolved orders in terms of the existence of SOLSSOMs is improved in that the non-existence of such designs of order 10 is established, thereby resolving a longstanding open existence question in the theory of Latin squares. Furthermore, this result establishes a new necessary condition for the existence of a set of three mutually orthogonal Latin squares of order 10, namely that such a set cannot contain a SOLS and its transpose.

Uittreksel

'n Latynse vierkant van orde n is 'n $n \times n$ skikking van n simbole met die eienskap dat elke ry en elke kolom van die skikking elke element presies een keer bevat. Dit is welbekend dat Latynse vierkante gebruik kan word in die konstruksie van ontwerpe wat vra na 'n gebalanseerde rangskikking van 'n versameling elemente onderhewig aan 'n aantal streng beperkings. 'n Belangrike toepassing van Latynse vierkante kom in die skedulering van verskeie spesiale tipes gebalanseerde sporttoernooie voor, waarvan die eenvoudigste voorbeeld 'n sogenaamde *rondomtalietoernooi* is — 'n toernooi waarin elke span elke ander span presies een keer teenstaan.

Onder die verskeie toepassings van Latynse vierkante in sporttoernooi-skedulering, is die probleem van die skedulering van spesiale tipes gemengde dubbels tennis- en tafeltennistoernooie deur gebruikmaking van spesiale versamelings van drie paarsgewys-ortogonale Latynse vierkante in hierdie proefskrif van besondere belang. In sogenaamde *gemengde dubbels tafeltennis (GDTT) toernooi* ding twee spanne, elk bestaande uit mans en vrouens, op 'n gemengde-dubbels rondomtalie wyse mee, en dit is bekend dat enige versameling van drie paarsgewys-ortogonale Latynse vierkante gebruik kan word om 'n skedule vir só 'n toernooi op te stel. 'n Meer interessante sporttoernooi-ontwerp, en een wat al vantevore in minstens twee gerapporteerde gevalle deur sportklubs benodig is, is egter 'n *gade-vermydende gemengde-dubbels rondomtalie (GVGDR) toernooi*, en dit is bekend dat só 'n toernooi geskeduleer kan word deur gebruik te maak van 'n *self-ortogonale Latynse vierkant met 'n simmetriese ortogonale maat (SOLVSOM)*.

Hierdie toepassings het tot 'n aantal belangrike onopgeloste probleme in die teorie van Latynse vierkante gelei, waarvan die mees beroemde die vraag na die bestaan van 'n versameling van drie paarsgewys ortogonale Latynse vierkante van orde 10 is. Nog 'n onopgeloste probleem is die vraag na die bestaan van SOLVSOMs van ordes 10 en 14. 'n Verdere probleem in die teorie van Latynse vierkante wat aansienlik aandag in die literatuur geniet, is die bepaling van die getal (essensieel) verskillende maniere waarop 'n versameling elemente in 'n Latynse vierkant gerangskik kan word, *m.a.w.* die probleem van die enumerasie van Latynse vierkante en ekwivalensieklasse van Latynse vierkante van 'n gegewe orde. Hierdie probleem raak vinnig baie moeilik soos die orde van die Latynse vierkant groei, en aansienlike berekeningskrag word dikwels hiervoor benodig. Sover is slegs 'n klein aantal ekwivalensieklasse van *self-ortogonale Latynse vierkante* (SOLVe) in die literatuur getel, naamlik die getal verskillende SOLVe, die getal idempotente SOLVe en die getal isomorfismeklasse voortgebring deur idempotente SOLVe van ordes $4 \leq n \leq 9$. Verder is slegs 'n klein aantal ekwivalensieklasse van geordende versamelings van k *onderling ortogonale Latynse vierkante* (k-OOLVs) in die literatuur getel, naamlik die getal hoofklasse voortgebring deur 2-OOLVs van orde n vir $3 \leq n \leq 8$ en die getal isotoopklasse voortgebring deur 8-OOLVs van orde 9. Daar is geen enumerasieresultate oor SOLVSOMs in die literatuur beskikbaar nie.

In hierdie proefskrif word ’n metodologie vir die enumerasie van ekwivalensieklasse van Latynse vierkante met behulp van ’n soekboomalgoritme met terugkering voorgestel. Hierdie algoritme poog om oorbodigheid in die soektog te minimeer deur net strukture te oorweeg wat die potensiaal het om tot goed-gedefinieerde klasleiers opgebou te word. Hierdie eienskap verseker dat die algoritme slegs een Latynse vierkant binne elk van die klasse wat getel word, genereer, en dus word ’n databasis van verteenwoordigers van hierdie klasse sodoende opgebou. Hierdie klasverteenwoordigers kan tesame met verskeie welbekende groepteoretiese telresultate gebruik word om die getal Latynse vierkante in elke klas te bepaal, asook die getal verskeie deelklasse van verskillende tipes binne elke klas.

Die bogenoemde metodologie word toegepas om verskeie SOLV- en SOLVSOM-klasse van ordes kleiner of gelyk aan 10 te tel, asook om k-OOLV-klasse van ordes kleiner of gelyk aan 8 te tel. Die getal verskillende SOLVe, idempotente SOLVe en isomorfismeklasse voortgebring deur SOLVe word vir ordes $4 \leq n \leq 9$ geverifieer, en daarbenewens word die getal isomorfismeklasse, transponent-isomorfismeklasse en RC-paratoopklasse voortgebring deur SOLVe van hierdie ordes ook bepaal. Die soektog word deur middel van ’n groot parallelisering van die soekboomalgoritme op ’n aantal rekenaars ook uitgebrei na die tel van hierdie klasse voortgebring deur SOLVe van orde 10. Die verteenwoordigers van RC-paratoopklasse voortgebring deur SOLVe wat deur middel van hierdie algoritme gegenereer word, word dan gebruik om SOLVSOMs te tel, terwyl bestaande databasisse van simmetriese Latynse vierkante as validasie van die resultate ook vir hierdie doel ingespan word. Op hierdie manier word die getal verskillende SOLVSOMs, standaardvorm SOLVSOMs, transponent-isomorfismeklasse voortgebring deur SOLVSOMs asook RC-paratoopklasse voortgebring deur SOLVSOMs bepaal, en word ’n databasis van verteenwoordigers van RC-paratoopklasse voortgebring deur SOLVSOMs ook opgebou. Die bekende getal hoofklasse voortgebring deur 2-OOLVs van ordes $3 \leq n \leq 8$ word in hierdie proefskrif geverifieer, en so ook word die getal hoofklasse voortgebring deur k-OOLVs van ordes $3 \leq n \leq 8$ bepaal, waar $3 \leq k \leq n-1$. Ander ekwivalensieklasse voortgebring deur k-OOLVs van orde n wat ook getel word, sluit in verskillende k-OOLVs en gereduseerde k-OOLVs van ordes $3 \leq n \leq 8$, waar $2 \leq k \leq n-1$.

Laastens word daar van ’n filtreer-metode gebruik gemaak om te bepaal of enige SOLV van orde 10 twee basiese nodige voorwaardes om ’n ortogonale maat met sy transponent te deel kan bevredig, en daar word gevind dat slegs vier van die 121 642 klasverteenwoordigers van RC-paratoopklasse voortgebring deur SOLVe van orde 10 aan hierdie voorwaardes voldoen. Dit word verder vasgestel dat geeneen van hierdie vier SOLVe ortogonale maats in gemeen met hul transponente het nie. Die spektrum van afgehandelde ordes in terme van die bestaan van SOLVSOMs word dus vergroot deur aan te toon dat geen sulke ontwerpe van orde 10 bestaan nie, en sodoende word ’n jarelange oop bestaansvraag in die teorie van Latynse vierkante beantwoord. Verder bevestig hierdie metode ’n nuwe noodsaaklike bestaansvoorwaarde vir ’n versameling van drie paarsgewys-ortogonale Latynse vierkante van orde 10, naamlik dat só ’n versameling nie ’n SOLV en sy transponent kan bevat nie.

Acknowledgements

The author wishes to acknowledge the following people for their various contributions towards the completion of this work:

- I wish to extend my deepest gratitude to my promoter, Prof Jan van Vuuren, for his excellent guidance throughout this project. I appreciate his time, patience and enthusiasm when listening to my ideas, as well as his dedication and hard work in ensuring that work of a high standard is delivered.
- I wish also to extend my deepest gratitude to my co-promoter, Dr Alewyn Burger, for his undying enthusiasm and accessibility, friendliness and his willingness to lend a helping hand (or two) whenever necessary.
- I wish to thank the Department of Logistics for the use of their excellent computing facilities, and I thank in particular every single one of the Operations Research staff members for their friendliness, accessibility and support during the past three years.
- I wish to thank the Harry Crossley Foundation and the National Research Foundation for much needed funding during the past three years.
- A big thanks also goes to the various masters and doctoral students with whom I shared a number of wonderful experiences throughout the past three years, and a special thanks to those whom I can now call friends.
- Finally, I extend my deepest thanks to my family, friends and girlfriend for their unwavering support during the past three years and their understanding during times of great unavailability on my part. Nothing would have been possible without those whom I love.

Table of Contents

List of Reserved Symbols

Symbols in this dissertation conform to the following font conventions:

A	Symbol denoting a **finite set**	(Roman capitals)
$\mathcal{A}$	Symbol denoting a **set of Latin squares**	(Calligraphic capitals)
$\boldsymbol{A}$	Symbol denoting a **matrix** or **Latin square**	(Boldface capitals)
α	Symbol denoting a general **mapping**	(Greek lower case letters)

Symbol	Meaning
$\times$	A binary operator symbol denoting the direct product between groups and Latin squares.
$\wr$	A binary operator symbol denoting the wreath product between permutation groups.
$\varnothing$	A symbol used to denote the empty set.
$C(\boldsymbol{L})$	The column indexing set of a Latin square $\boldsymbol{L}$.
γ	The operation of replacing each column of a Latin square by its inverse permutation.
δ	A symbol used to specify that any conjugate operation may be used in the transformation of a Latin object of order n.
D_3	The Dihedral group of order 6.
e	The identity permutation.
$E(G)$	The edge set of a graph G.
ι	The identity mapping.
K_n	The complete graph on n vertices.
$\boldsymbol{L}(i)$	The i-th row of a Latin square $\boldsymbol{L}$.
$\boldsymbol{L}(i,j)$	The entry in row i and column j of a Latin square $\boldsymbol{L}$.
$\boldsymbol{L}^T$	The transpose of a Latin square $\boldsymbol{L}$.
$\boldsymbol{L}^T(j)$	The j-th column of a Latin square $\boldsymbol{L}$.
$\mathbb{N}$	The set of all natural numbers, *i.e.* $\{1,2,3,\ldots\}$.
π	A symbol used to specify that a permutation of order n is used in the transformation of a Latin object of order n.
P_n	The set of all permutations of order n.
ρ	The operation of replacing each row of a Latin square by its inverse permutation.
$R(\boldsymbol{L})$	The row indexing set of a Latin square $\boldsymbol{L}$.
$\langle S\rangle$	The group generated by the set S.
$S(\boldsymbol{L})$	The symbol set of a Latin square $\boldsymbol{L}$.
S_n	The symmetric group of order n.
τ	The operation of transposing a Latin square.

$T(\boldsymbol{L})$	The set of triples $\{(i,j,\boldsymbol{L}(i,j)) \mid i,j \in \mathbb{Z}_n\}$ of a Latin square $\boldsymbol{L}$ of order n.
$T(\mathcal{M})$	The set of tuples $\{(i,j,\boldsymbol{L}_0(i,j),\boldsymbol{L}_1(i,j),\ldots,\boldsymbol{L}_{k-1}(i,j)) \mid i,j \in \mathbb{Z}_n\}$ of a k-MOLS $\mathcal{M}=(\boldsymbol{L}_0,\boldsymbol{L}_1,\ldots,\boldsymbol{L}_{k-1})$ of order n.
$U(\mathcal{M})$	The set of all universal permutations of the Latin squares in the k-MOLS $\mathcal{M}$.
$V(G)$	The vertex set of a graph G.
$z_i^{a_i}$	A symbol used to denote the fact that a permutation has a_i cycles of length i.
$\mathbb{Z}_n$	The set of residues modulo $n \in \mathbb{N}$, *i.e.* $\{0,1,\ldots,n-1\}$.
$\mathbb{Z}_n^{(2)}$	The set of all 2-subsets of $\mathbb{Z}_n$.
$(\mathbb{Z}_n,+)$	The group over $\mathbb{Z}_n$ induced by the binary operation of addition performed modulo n.
$(\mathbb{Z}_n,\times)$	The group over $\mathbb{Z}_n$ induced by the binary operation of multiplication performed modulo n.
$(\mathbb{Z}_n,\ominus)$	The quasigroup over $\mathbb{Z}_n$ induced by the binary operation $\ominus$, defined as $a \ominus b = a-b \pmod n$ for any $a,b \in \mathbb{Z}_n$.
$(\mathbb{Z}_{2m+1},\odot)$	The quasigroup over $\mathbb{Z}_{2m+1}$ induced by the binary operation of $\odot$, defined as $a \odot b = (m+1)(a+b) \pmod{2m+1}$, for $a,b \in \mathbb{Z}_{2m+1}$.
$(\mathbb{Z}_{2m},\circledast)$	The group over $\mathbb{Z}_{2m}$ induced by the binary operation $\circledast$, defined as $a \circledast b = a+b-2 \pmod{2m}$ if both a and b are odd, or $a+b \pmod{2m}$ otherwise.

List of Acronyms

DTS: Directed Triple System

GF: Galois Field

MDTT: Mixed Doubles Table Tennis

MOLS: Mutually Orthogonal Latin Squares

OA: Orthogonal Array

OEIS: Online Encyclopedia of Integer Sequences

SAMDRR: Spouse-Avoiding Mixed Doubles Round-Robin

SDR: System of Distinct Representatives

SOLS: Self-Orthogonal Latin Square

SOLSSOM: Self-Orthogonal Latin Square with a Symmetric Orthogonal Mate

List of Figures

List of Tables

List of Algorithms

CHAPTER 1

Introduction

Contents

1.1 Historical background

In 1782 the Swiss mathematician Leonhard Euler (1707–1783) posed the following problem in a research paper:

> *"A very curious question that has taxed the brains of many inspired me to undertake the following research that has seemed to open a new path in Analysis and in particular in the area of combinatorics. This question concerns a group of thirty-six officers of six different ranks, taken from six different regiments, and arranged in a square in a way such that in each row and column there are six officers, each of a different rank and regiment." [52]*

Euler used the Latin letters a, b, c, d, e and f to denote the six different regiments and the Greek letters α, β, γ, δ, ϵ and ζ to denote the six different ranks. The problem described by Euler has become known as the "36 officers problem" [9], and in mathematical terms consists of finding a 6×6 array in which each entry contains an ordered pair of elements, one in $\{a, b, c, d, e, f\}$ and one in $\{\alpha, \beta, \gamma, \delta, \epsilon, \zeta\}$, so that no pair appears more than once within the array and so that no symbol appears twice in any row or column of the array. Euler was unable to find a solution to this problem, but gave a partial solution in [52], shown in Table 1.1, where each symbol appears exactly once in each row and column, but where the pairs $b\zeta$ and $d\epsilon$ appear twice, while the pairs $b\epsilon$ and $d\zeta$ do not appear at all.

Even earlier than 1782 Euler had considered the problem in general, where there are n^2 officers from n different ranks and n different regiments for some natural number n. Euler called the associated $n \times n$ array a *Graeco-Latin square* of order n (derived from his usage of Latin and

$a\alpha$	$\underline{b\zeta}$	$c\delta$	$\underline{d\epsilon}$	$e\gamma$	$f\beta$
$b\beta$	$c\alpha$	$f\epsilon$	$e\delta$	$a\zeta$	$d\gamma$
$c\gamma$	$\underline{d\epsilon}$	$a\beta$	$\underline{b\zeta}$	$f\delta$	$e\alpha$
$d\delta$	$f\gamma$	$e\zeta$	$c\beta$	$b\alpha$	$a\epsilon$
$e\epsilon$	$a\delta$	$b\gamma$	$f\alpha$	$d\beta$	$c\zeta$
$f\zeta$	$e\beta$	$d\alpha$	$a\gamma$	$c\epsilon$	$b\delta$

TABLE 1.1: *A partial solution to the 36 officers problem given by Euler in [52]. The pairs $b\zeta$ and $d\epsilon$ appear twice (in the underlined positions), while the pairs $b\epsilon$ and $d\zeta$ are absent.*

Greek letters) and used them in the construction of *magic squares*[1] in [53] which, according to a statement on p. 593 of this paper, was presented to the St. Petersburg Academy in 1776. Euler also considered Graeco-Latin squares without the Greek letters, referring to them as Latin squares. He found many examples of Graeco-Latin squares, and in particular gave two general constructions of Graeco-Latin squares in [52], one for squares of odd order and another for squares of order a multiple of 4. Euler could not, however, find a Graeco-Latin square of any other order (*i.e.* even orders which are not multiples of 4, including the case of the 36 officers problem), and conjectured that Graeco-Latin squares of order n do not exist when $n = 4m + 2$, for some integer m:

> *"Thus, I have not hesitated to conclude from this that we cannot produce a complete square with thirty-six entries, and that the same impossibility extends to the cases of $n = 10$, $n = 14$ and in general to all the oddly even numbers." [52]*

It is easy to verify that a Graeco-Latin square of order 2 does not exist, but for orders 6 and upwards Euler's attempts at proving his conjecture were inconclusive, and remained so until his death in 1783.

Euler's conjecture remained unsolved for over a hundred years before a small step was taken towards confirming his predictions. In 1900 the French mathematician Gaston Tarry [136] proved that there is no solution to the 36 officers problem by an exhaustive elimination of all possible cases, thereby verifying Euler's conjecture for $n = 6$. This still left the orders $n = 10, 14, 18, \ldots$ unresolved, and it would only be 59 years later, when Indian mathematicians Raj Chandra Bose and Sharadchandra Shankar Shrikhande constructed a Graeco-Latin square of order 22 [22], that a special case of Euler's conjecture was disproven for the first time. By this time the term "Graeco-Latin square" was no longer in use; the concept of *orthogonality* between Latin squares had taken its place[2]. Soon thereafter, also in 1959, the American mathematician Ernest Tilden Parker constructed two orthogonal Latin squares of order 10 [115], and in 1960 Bose, Shrikhande and Parker finally disproved Euler's 177-year old conjecture for all other orders [23].

Although Euler does not cite any previous work on Latin squares, he was not the first to consider this type of design. According to Andersen [6] examples of Latin squares (as well as magic squares) were found on amulets and talismans belonging to Arab or Indian cultures dating back roughly 1 000 years. Possibly the oldest examples of Latin squares in print may be found in the book *Shams al-Maarif al-Kubra* (*The sun of great knowledge*) written by Ahmad ibn Ali ibn Yusuf al-Buni no later than the year 1 225. In the 13$^{\text{th}}$ century the Spanish philosopher

[1]See [88, §10] for a discussion on magic squares.

[2]Two Latin squares of order n are said to be *orthogonal* if their superimposition yields n^2 distinct ordered pairs, as was the requirement for $n = 6$ in Euler's 36 officers problem.

Ramón Lull also attempted to "explain the world" by using combinatorics and constructing Latin squares [6].

Another interesting occurrence of Latin squares (in fact, Graeco-Latin squares, possibly preceding Euler's work) appears in the form of a playing-card puzzle. The exact date of publication of the earliest work containing the puzzle is not known. According to Kendall [81], and Styan and Boyer [135], Henry Ernest Dudeney (1857–1930) believed that it is contained in a book dating back to 1624 by Claude Gaspar Bachet de Méziriac (1581–1638) entitled "Problèmes plaisants and délectables, qui se font par les nombres." The puzzle asks for the number of distinct ways in which the sixteen court cards (Jacks, Queens, Kings and Aces of all four suites) can be arranged in a square grid so that no royalty or suite is found more than once in any row, column or diagonal. Clearly such an arrangement gives rise to a Graeco-Latin square. Ball [12] gave a solution of 72, which was, according to Gardner [61], a mistake; Gardner gave the correct answer as 144 (in both cases rotations and reflections of designs are not counted as different designs).

Early occurrences of Latin squares may also be found in a subfield of statistics to which the application of Latin squares are well known, namely the field of experimental design. According to Andersen [6] and Ullrich [138], one of the earliest applications of Latin squares in experimental design was published by French agronomist Francois Cretté de Palluel (1741–1798) who (seemingly unaware of this fact) used a Latin square to design an experiment involving the effects of different diets on different breeds of sheep. He used sixteen sheep for his experiment, four sheep of each of four different breeds, namely the breed of the country (Île de France), the breed of Beauce, the breed of Champagne, and the breed of Picardy. He fed the sheep four different kinds of food, namely potatoes, turnips, beets and corn, and had four of them slaughtered each consecutive month for four months following the start of the experiment. When four sheep were slaughtered, he wanted all four to be of different breeds and on different diets, and so constructed the design shown in Table 1.2, which is a Latin square of order 4.

	Potatoes	Turnips	Beets	Corn
Île de France	1	2	3	4
Beauce	4	1	2	3
Champagne	3	4	1	2
Picardy	2	3	4	1

TABLE 1.2: *An experiment designed by agronomist Francois Cretté de Palluel for the feeding of sheep, where the entry in row i and column j gives the number of months after the experiment started on which a sheep of breed i on diet j was to be slaughtered.*

The statistician Sir Ronald Fisher also described the design of experiments using Latin squares as well as orthogonal Latin squares in his celebrated books "Statistical methods for research workers" [55] and "The design of experiments" [56], and together with Frank Yates published some of the first work on the enumeration of Latin squares in [57], namely the enumeration of Latin squares of order 6.

Orthogonal Latin squares indeed play an important part in the design of experiments, and especially so *self-orthogonal Latin squares*[3] *(SOLS)*, as discussed by Hedayat [72, 73]. SOLS were first systematically constructed by Mendelsohn [105] in 1971 and soon thereafter, in 1973, Brayton *et al.* [24] proved that a SOLS exists for any order except[4] orders 2, 3 and 6. In

[3]Latin squares which are orthogonal to their transposes

[4]The non-existence proof for $n = 6$ is considerably more complicated than for $n = 2$ and $n = 3$. This has led to a number of alternative proofs for the case $n = 6$ over the years. The author was involved in establishing a

the paper by Brayton *et al.* the authors describe how they came across another area in which Latin squares seem to have useful applications, namely in sports tournament scheduling. They noted that a SOLS may be used to schedule a *spouse-avoiding mixed doubles round-robin tennis tournament*[5]. A SOLS, however, can only give the matches for such a tournament, but cannot be used to group these matches into the minimum number of rounds so that each player plays exactly once in each round. In 1978 Wang [143] noted that if a symmetric Latin square is found which is orthogonal to a SOLS, then the matches given by the SOLS could be grouped into the minimum number of rounds so that each player plays exactly once in each round. Such a design is called a *self-orthogonal Latin square with a symmetric orthogonal mate (SOLSSOM)*, and it was a special case of the logically next step in design construction beyond Graeco-Latin squares, namely the study of *sets of mutually orthogonal Latin squares (MOLS)*, where a *k-MOLS* is defined as a set of k Latin squares, each two of which are orthogonal. Ever since the fall of Euler's conjecture, the search for larger sets of orthogonal Latin squares has become the breeding ground for new open questions in the theory of Latin squares. Order 10 has outlasted the other integers in the sense that it is currently the only order for which the existence of three mutually orthogonal Latin squares is undecided (see Colbourn *et al.* [38, Theorem 3.43]).

The search for SOLSSOMs has been as difficult as the search for MOLS; in fact, even more so since it is a special case of a 3-MOLS. SOLSSOMs trivially do not exist for orders 2, 3 and 6, and Wang found constructions for SOLSSOMs of an infinite number of orders, but could not construct SOLSSOMs of order

$$\begin{aligned} n \in \; & \{10, 14, 39, 46, 51, 54, 58, 62, 66, 70, 74, 82, 87, 98, 102, 118, 123, 142, 159, 174, 183, 194, 202, \\ & 214, 219, 230, 258, 267, 278, 282, 303, 394, 398, 402, 422, 1322\}. \end{aligned}$$

Only five years later, in 1983, this list of unresolved orders was reduced drastically by Lindner *et al.* [91] to $n \in \{10, 14, 39, 46, 54, 58, 62, 66, 70, 87, 102, 194, 230\}$, and in the following year Zhu [155] found SOLSSOMs of orders 39, 87, 102, 194 and 230. More than ten years elapsed before any further progress was made: In 1996 Bennet and Zhu constructed SOLSSOMs of orders 46, 54 and 58 in [16] and of order 62 in [17]. This left only orders 10, 14, 66 and 70 as unresolved cases, but the latter two were resolved when Abel *et al.* [1] constructed SOLSSOMs of these orders in the year 2000. Since 2000 no new results on the existence of SOLSSOMs have been published, and until now, 31 years after the first SOLSSOM was constructed, it was still not known whether SOLSSOMs of orders 10 and 14 exist[6].

Notable applications of Latin squares, other than in experimental designs and sports tournament scheduling, include applications to cryptography and coding theory [88], and the very interesting and difficult problem of the enumeration of Latin squares, which is (next to the existence of a 3-MOLS of order 10 and SOLSSOMs of orders 10 and 14) one of the great open problems in combinatorics, and has challenged mathematicians considerably during the past century. Although Euler was wrong in his conjecture that Graeco-Latin squares only exist for those orders for which he could construct them, he was more accurate in another, more subtle conjecture given in the last line of his crucial 1782 paper:

> *"Here, I bring mine to an end on a question that, although is of little use itself, has led us to some observations as important for the doctrine of combinatorics as for the general theory of magic squares." [52]*

very simple graph theoretic proof of the non-existence of a SOLS of order 6 [31].

[5] A mixed-doubles tennis tournament in which married couples take part, but may not oppose nor be partnered with their spouses.

[6] It is shown later in this dissertation that there is no SOLSSOM of order 10.

1.2 Problem statement

In the theory of combinatorics three important questions arise from the study of any combinatorial design, namely the question of existence (deciding whether a design can be found), the design methods of construction (determining how a design may be constructed) and the process of design enumeration (counting in how many different ways a design can be constructed). As may be expected, these questions do not always have trivial answers, and often remain unanswered for long periods of time.

In this dissertation these three questions are addressed in the context of three special classes of orthogonal Latin squares, namely SOLS, SOLSSOMs, and k-MOLS. Answers to the question of construction are reviewed for these designs from the literature, while the enumeration question for SOLS and k-MOLS of orders strictly less than 10 has only been partially resolved in the literature, and not at all for SOLSSOMs. A number of subclasses of SOLS that have previously not been enumerated are therefore enumerated in this dissertation, and enumeration results are also given for SOLS of order 10. Various subclasses of SOLSSOMs up to and including order 10 are enumerated as well, the numbers of which were previously unknown. Finally, various classes of k-MOLS up to and including order 8 are enumerated for $2 \leq k \leq 7$, of which $k = 2$ is the only case where the results have previously been established.

Finally, the question of existence has been resolved completely for SOLS, but not for SOLSSOMs and k-MOLS. It was previously still unknown whether SOLSSOMs of orders 10 and 14 exist, and in this dissertation one of these orders, namely order 10, is completely resolved in that it is established that no SOLSSOM of order 10 exists. This existence question is related to the celebrated question of whether a 3-MOLS of order 10 exists. A new necessary condition for this latter existence question is put forward, namely that such a set cannot contain a SOLS and its transpose.

1.3 Scope and objectives

The following objectives are pursued in this dissertation:

I To *illustrate* the importance and benefit of using Latin square designs in the scheduling of balanced sports tournaments.

II To *review* a selection of construction methods from the literature for special classes of orthogonal Latin squares.

III To *document* a number of transformations which may be applied to Latin squares without destroying their defining property.

IV To *propose* a general notation for describing any equivalence class of Latin squares induced by the group action of any transformation documented in Objective III.

V To *design* algorithms using the general notation mentioned in Objective IV for the purpose of enumerating equivalence classes of any type of Latin square.

VI To *implement* the algorithms mentioned in Objective V for the purpose of enumerating various subclasses of SOLS, SOLSSOMs and k-MOLS of small orders.

VII To *resolve* the question of the existence of a SOLSSOM of order 10.

VIII To *contribute* towards answering the celebrated question of whether a 3-MOLS of order 10 exists.

Combinatorial designs other than Latin squares are, for the most part, considered to fall beyond the scope of this dissertation. Except for a small number of special cases where certain designs may be used to better illustrate notions that are important in the study of Latin squares, structures such as block designs, triple systems, transversal designs and frame-type SOLSSOMs (although useful in the construction of Latin squares) are not considered. Furthermore, applications of Latin squares in areas other than sports tournament scheduling are not discussed in this dissertation, and the same holds for applications of other combinatorial designs to sports tournament scheduling.

1.4 Thesis organisation

The second chapter of this dissertation lays down fundamental groundwork from the theory of Latin squares. A number of basic definitions of various notions in the theory of Latin squares are provided in the first section, while the important notion of orthogonality between Latin squares is introduced in the second section. The notion of changing the structure of a Latin square or a set of orthogonal Latin squares via some operation is considered in the third section. In the fourth section a number of recursive constructions of Latin squares are given, and these recursive constructions are utilised for the purpose of reviewing constructions of sets of orthogonal Latin squares.

In the third chapter the importance of Latin squares in applications to sports tournament scheduling is highlighted. The first section of this chapter contains a brief overview of the application of Latin squares to the scheduling of sports tournaments, and the usefulness of utilising Latin squares for this purpose is illustrated. The second and third section each contains an application of special sets of two and three mutually orthogonal Latin squares to the scheduling of mixed doubles sports tournaments. These sections also contain a number of constructions of these designs for various orders.

In the fourth chapter a methodology is presented for the enumeration of subclasses of Latin squares in general. The first section of this chapter illustrates the use of operations on Latin squares to define group actions on Latin squares, which in turn give rise to equivalence classes of Latin squares. The second section contains a brief historical account of the problem of enumerating Latin squares, and in the third section a backtracking tree-search algorithm is presented for the purpose of enumerating Latin square subclasses. In the fourth section it is shown how graph theoretical methods may be utilised in order to determine the so-called autotransformation group of a Latin square, whereas in the fifth section it is illustrated how these groups may be used to provide theoretical counts of Latin squares and Latin square subclasses.

The results of an implementation of the enumeration methodology in Chapter 4, specifically for the purpose of enumerating self-orthogonal Latin squares, self-orthogonal Latin squares with symmetric orthogonal mates and ordered sets of mutually orthogonal Latin squares, are then presented in the fifth chapter. The numbers of the various classes enumerated are given, as well as additional information which may facilitate future validation of the results.

The dissertation closes, in Chapter 6, with a summary of the work contained therein, an appraisal of the contributions of the dissertation as well as a discussion on possibilities for future work in the area of Latin square equivalence class enumeration.

CHAPTER 2

Latin squares

Contents

In this chapter a basic introductory background to the design theoretic subfield of Latin squares is presented. In §2.1 a number of basic definitions of various aspects of Latin squares, such as subsquares, transversals and universals, are introduced and the connection between Latin squares and quasigroups is highlighted. In §2.2 the notion of orthogonal Latin squares is discussed. This notion is considered one of the most important and useful (in a practical application sense) notions in the theory of Latin squares, and some definitions and constructions of orthogonal Latin squares and sets of orthogonal Latin squares are given. In §2.3 transformations of Latin squares are considered, and a number of operations are presented which may be applied to a Latin square in order to obtain another Latin square as a result. The notions in this section play an important role in the classification of Latin squares, as will be discussed later in this dissertation. In §2.4 the possibility of building larger Latin squares from smaller ones is discussed together with a number of methods for achieving such constructions, and some applications to the construction of sets of orthogonal Latin squares are considered.

2.1 Basic definitions

A permutation may be viewed as a one-dimensional array in which no two symbols are equal (see §A.1). A natural extension of a permutation is to consider a two-dimensional array with a similar property; in other words, a two-dimensional array in which each row and column is a permutation. Laywine and Mullin [88, p. 3] noted that “a Latin square may be thought of as a two-dimensional analogue of a permutation.” A formal definition of a Latin square follows.

Definition 2.1.1 *Given a set S of cardinality n, a* Latin square *of order n is an $n \times n$ array in which each row and each column represents a permutation of the elements of S.* □

In simpler terms a Latin square of order n is an array or matrix containing as entries n symbols in such a way that each symbol is contained exactly once within each row and each column, a definition commonly found in the literature on Latin squares (see Colbourn *et al.* [38, p. 135] and Dénes and Keedwell [41, p. 15]). This defining property of a Latin square has been referred to as the *latinness* of the square (see Dénes and Keedwell [41, p. 439]). The 8×8 array

$$\boldsymbol{L}_{2.1} = \begin{bmatrix} 0&1&2&3&4&5&6&7\\ 1&2&3&4&5&6&7&0\\ 2&3&4&5&6&7&0&1\\ 3&4&5&6&7&0&1&2\\ 4&5&6&7&0&1&2&3\\ 5&6&7&0&1&2&3&4\\ 6&7&0&1&2&3&4&5\\ 7&0&1&2&3&4&5&6 \end{bmatrix}$$

is an example of a Latin square of order 8.

Let $S(\boldsymbol{L})$, $R(\boldsymbol{L})$ and $C(\boldsymbol{L})$ denote respectively the symbol set, row indexing set and column indexing set of a Latin square $\boldsymbol{L}$ such that, for any $i \in R(\boldsymbol{L})$ and $j \in C(\boldsymbol{L})$, the (i, j)-th element of $\boldsymbol{L}$ is denoted by $\boldsymbol{L}(i, j) \in S(\boldsymbol{L})$. The set of entries $\{(k + i, i) \mid i \in \mathbb{Z}_n\}$ in a Latin square $\boldsymbol{L}$ of order n is called the *k-th diagonal* of $\boldsymbol{L}$, and the 0-th diagonal is referred to as the *main diagonal*. The *transpose* of a Latin square $\boldsymbol{L}$ is again a Latin square, denoted by $\boldsymbol{L}^T$, for which $\boldsymbol{L}^T(i, j) = \boldsymbol{L}(j, i)$. Throughout this dissertation it is assumed that $R(\boldsymbol{L}) = C(\boldsymbol{L}) = S(\boldsymbol{L}) = \mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ for any Latin square $\boldsymbol{L}$ of order n. Whenever a sequence of n distinct entries in a Latin square contains its elements in the order $0, 1, \ldots, n - 1$, this sequence is said to be in *natural order*.

Any row i of a Latin square $\boldsymbol{L}$ of order n may be viewed as a permutation of the form

$$\begin{pmatrix} 0 & 1 & \ldots & n-1 \\ \boldsymbol{L}(i,0) & \boldsymbol{L}(i,1) & \ldots & \boldsymbol{L}(i,n-1) \end{pmatrix}.$$

The i-th row of a Latin square $\boldsymbol{L}$ is henceforth denoted by $\boldsymbol{L}(i)$. Therefore $\boldsymbol{L}(i, j)$ is the image of the element j under the permutation $\boldsymbol{L}(i)$. Similarly, the j-th column is denoted by $\boldsymbol{L}^T(j)$.

The following theorem establishes the close connection between Latin squares and quasigroups[1].

Theorem 2.1.1 ([41], Theorem 1.1.1) *The Cayley table of a quasigroup is a Latin square.*

Proof: Assume some element a appears twice in row i of the Cayley table of a quasigroup, say in columns j and k. Then $i \circ j = a$ and $i \circ k = a$, contradicting the fact that $i \circ x = a$ has a unique solution x for i and a known. Therefore each element appears only once in each row of the Cayley table of a quasigroup. A similar argument shows that each element appears only once in each column of the Cayley table of a quasigroup. ■

Any Latin square $\boldsymbol{L}$ may also be used to define a quasigroup, which is henceforth referred to as the *underlying quasigroup* of $\boldsymbol{L}$. Define on the set $\mathbb{Z}_n$ the operation '$\circ$' by writing $a \circ b = c$ if $\boldsymbol{L}(a, b) = c$. Since $\boldsymbol{L}$ is a Latin square, the equation $a \circ b = c$ always has a unique solution, given any two of a, b and c in $\mathbb{Z}_n$. Hence $(\mathbb{Z}_n, \circ)$ forms a quasigroup.

[1]This chapter contains references to a number of notions from group theory, including *quasigroups*, *loops*, the *Cayley table* of a group, *subgroups*, *permutations*, *symmetric groups*, *dihedral groups*, *generating sets* of groups and *group actions*. For the definitions of and further discussions on these notions, the reader is referred to §A.2.1.

It may readily be seen that each row of $\boldsymbol{L}_{2.1}$ is a shift to the left by one entry of the row preceding it. This gives a simple construction for a Latin square of any order, leading to the following existence result.

Theorem 2.1.2 *A Latin square of order n exists for any positive integer n.*

Proof: Let $\boldsymbol{L}$ be the Cayley table of the group $(\mathbb{Z}_n, +)$ as discussed in §A.2.1. Then, by Theorem 2.1.1, $\boldsymbol{L}$ is a Latin square. The group $(\mathbb{Z}_n, +)$ clearly exists for all $n \in \mathbb{N}$. ■

A similar proof of Theorem 2.1.2 may be found in [88, Theorem 1.1]. In the Cayley table of $(\mathbb{Z}_n, +)$ the first row is in natural order since it is the addition of 0 to all elements of $\mathbb{Z}_n$, and each row is a shift to the left by one position of the row preceding it. This is true since $\boldsymbol{L}(i+1, j) = i+1+j = \boldsymbol{L}(i, j)+1 \pmod{n}$. Hence $\boldsymbol{L}_{2.1}$ is the Cayley table of the group $(\mathbb{Z}_8, +)$. The Cayley table of $(\mathbb{Z}_n, +)$ has the special property that the element in row i and column j of the table is also found in row j and column i, and a formal definition of a Latin square with this property follows.

Definition 2.1.2 (Symmetric Latin square) *A Latin square $\boldsymbol{L}$ is* symmetric *if $\boldsymbol{L}(i, j) = \boldsymbol{L}(j, i)$ for all $i, j \in \mathbb{Z}_n$.* □

The Latin square $\boldsymbol{L}_{2.1}$ is therefore an example of a symmetric Latin square. The following theorem shows that a symmetric Latin square of any order exists.

Theorem 2.1.3 *A symmetric Latin square of order n exists for any positive integer n.*

Proof: Since $a+b = b+a \pmod{n}$ for any $a, b \in \mathbb{Z}_n$, the Cayley table of $(\mathbb{Z}_n, +)$ is a symmetric Latin square. ■

The fact that the first row of the Cayley table of the group $(\mathbb{Z}_n, +)$ is in natural order implies that the first column is also in natural order. A formal definition of this type of Latin square follows.

Definition 2.1.3 (Reduced Latin square) *A Latin square $\boldsymbol{L}$ of order n is* reduced *(or in* standard form*) if $\boldsymbol{L}(0, i) = i = \boldsymbol{L}(i, 0)$ for all $i \in \mathbb{Z}_n$. Equivalently, the first row and first column of a reduced Latin square is in natural order, or $\boldsymbol{L}(i) = \boldsymbol{L}^T(i) = e$ (where e is the identity permutation).* □

The notion of a reduced Latin square is commonly found in books on (or in chapters on) Latin squares (see, for instance, Colbourn *et al.* [38, p. 135] and Laywine and Mullin [88, p. 4]).

Since $\boldsymbol{L}(0, i) = i = \boldsymbol{L}(i, 0)$ for a reduced Latin square $\boldsymbol{L}$, the identities $0 \circ i = i = i \circ 0$ hold in the underlying quasigroup of $\boldsymbol{L}$, and 0 is consequently the identity element of the quasigroup. Hence the underlying quasigroup of a reduced Latin square is a loop, and is henceforth referred to as the *underlying loop* of the reduced Latin square. The existence of reduced Latin squares of all orders is guaranteed by the following corollary, which follows directly from Theorem 2.1.3.

Corollary 2.1.1 *A reduced Latin square of order n exists for any positive integer n.*

It may also occur that a Latin square contains smaller Latin squares among some of its entries. This is similar to the notion of a subgroup of a group, and the definition below may also be found in Dénes and Keedwell [42, p. 102].

Definition 2.1.4 (Subsquare) *If R and C are two subsets of $\mathbb{Z}_n$ both of cardinality m for any $n, m \in \mathbb{N}$, then the set of entries $R \times C$ forms an $m \times m$* subsquare *of a Latin square $\boldsymbol{L}$ if the set $\{\boldsymbol{L}(i,j) \mid (i,j) \in R \times C\}$ contains m distinct elements of $\mathbb{Z}_n$.* □

Since the rows and columns of an $m \times m$ subsquare are taken from a Latin square, and since the subsquare can only contain m distinct symbols, it is itself a Latin square. For example, the Latin square

$$\begin{bmatrix} 0 & 5 & 3 & 6 & 1 & 4 & 2 \\ 2 & 1 & \mathbf{6} & 3 & \mathbf{4} & 0 & \mathbf{5} \\ 1 & 2 & \mathbf{5} & 0 & \mathbf{6} & 3 & \mathbf{4} \\ 4 & 6 & 1 & 5 & 3 & 2 & 0 \\ 5 & 3 & 0 & 4 & 2 & 6 & 1 \\ 3 & 0 & \mathbf{4} & 2 & \mathbf{5} & 1 & \mathbf{6} \\ 6 & 4 & 2 & 1 & 0 & 5 & 3 \end{bmatrix}$$

of order 7 contains a subsquare of order 3 on the symbols $\{4, 5, 6\}$, as shown in boldface.

The following definition is also widely found in the literature on Latin squares. In particular, see Colbourn *et al.* [38, p. 143].

Definition 2.1.5 (Transversal) *A* transversal *V in a Latin square $\boldsymbol{L}$ is a set of n distinct ordered pairs $(i,j) \in \mathbb{Z}_n^2$, such that $(i,j) = (i,k)$ implies $j = k$, $(i,j) = (k,j)$ implies $i = k$ and $\boldsymbol{L}(i,j) \neq \boldsymbol{L}(k,\ell)$ for two distinct elements (i,j) and (k,ℓ) of V.* □

Hence a transversal consists of n entries in a Latin square, no two of which contain the same element and no two of which appear in the same row or column. Transversals in Latin squares are equivalent to *complete mappings* in quasigroups. A *complete mapping* of a quasigroup $(G, \circ)$ is a bijection α from G to itself such that the mapping β, where $\beta(g) = g \circ \alpha(g)$ for any $g \in G$, is also a bijection from G to itself. It is easy to verify that the set $\{(g, \alpha(g)) \mid g \in G\}$ of entries in the Cayley table of $(G, \circ)$ satisfies all the properties of a transversal.

An example of a transversal in the Latin square

$$\boldsymbol{L}_{2.2} = \begin{bmatrix} \mathbf{0} & 1 & 2 & 3 & 4 \\ 4 & 0 & \mathbf{1} & 2 & 3 \\ 3 & 4 & 0 & 1 & \mathbf{2} \\ 2 & \mathbf{3} & 4 & 0 & 1 \\ 1 & 2 & 3 & \mathbf{4} & 0 \end{bmatrix}$$

is $V = \{(0,0), (1,2), (2,4), (3,1), (4,3)\}$, as shown above in boldface.

Consider the set of entries $V' = \{(0,1), (1,2), (2,3), (3,4), (4,0)\}$ in $\boldsymbol{L}_{2.2}$. The set V' satisfies all the properties of a transversal, except for the fact that each entry contains the element 1. A formal definition of the notion of such a set follows.

Definition 2.1.6 (Universal) *A* universal *U in a Latin square $\boldsymbol{L}$ is a set of n distinct ordered pairs $(i,j) \in \mathbb{Z}_n^2$, such that $(i,j) = (i,k)$ implies $j = k$, $(i,j) = (k,j)$ implies $i = k$ and $\boldsymbol{L}(i,j) = \boldsymbol{L}(k,\ell)$ for all $(i,j), (k,\ell) \in U$.* □

Hence the universal of an element k in a Latin square $\boldsymbol{L}$ is simply all the entries in $\boldsymbol{L}$ that contain k. The notion of a universal is a novel contribution of this dissertation; for the best knowledge of the author no such notion exists in the literature on Latin squares. As will be shown later in this dissertation, the notion of a universal may be used very effectively in the enumeration of equivalence classes of Latin squares.

Transversals and universals may also be written in permutation form. The *transversal permutation* of a transversal V is a permutation v such that $v(i) = j$ if $(i, j) \in V$. Similarly, the *universal permutation* of an element k in a Latin square $\boldsymbol{L}$ is a permutation, denoted by u_k, for which $u_k(i) = j$ if $\boldsymbol{L}(i, j) = k$.

It may be noted that a Latin square of order n has exactly n distinct universals, all n of which are disjoint. A Latin square may, however, contain more than n distinct transversals, any number of which may intersect. Consider, for instance, the Latin squares

$$\boldsymbol{L}_{2.3} = \begin{bmatrix} \mathbf{0} & 1 & \mathbf{2} & 3 & 4 & \mathbf{5} & 6 & \mathbf{7} & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 \\ \mathbf{2} & 3 & 4 & 5 & 6 & \mathbf{7} & 8 & 9 & 0 & 1 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 \\ 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 \\ \mathbf{5} & 6 & \mathbf{7} & 8 & 9 & \mathbf{0} & 1 & \mathbf{2} & 3 & 4 \\ 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 \\ \mathbf{7} & 8 & 9 & 0 & 1 & \mathbf{2} & 3 & 4 & 5 & 6 \\ 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{2.4} = \begin{bmatrix} \mathbf{5} & 1 & \mathbf{7} & 3 & 4 & \mathbf{0} & 6 & \mathbf{2} & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 \\ \mathbf{7} & 3 & 4 & 5 & 6 & \mathbf{2} & 8 & 9 & 0 & 1 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 \\ 4 & 5 & 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 \\ \mathbf{0} & 6 & \mathbf{2} & 8 & 9 & \mathbf{5} & 1 & \mathbf{7} & 3 & 4 \\ 6 & 7 & 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 \\ \mathbf{2} & 8 & 9 & 0 & 1 & \mathbf{7} & 3 & 4 & 5 & 6 \\ 8 & 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 9 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{bmatrix}$$

of order 10. Euler [52] gave a simple proof of the fact that $\boldsymbol{L}_{2.3}$ (and, in fact, any Latin square which is the Cayley table of the group $(\mathbb{Z}_{2n}, +)$ for any $n \in \mathbb{N}$) does not contain any transversals, while Parker [116] showed that by simply rotating the elements of a number of 2×2 subsquares of $\boldsymbol{L}_{2.3}$ (namely a subsquare containing 0 and 5 and two subsquares containing 2 and 7, as shown in boldface), the Latin square $\boldsymbol{L}_{2.4}$ may be produced which contains 5 504 transversals. Transversals play an important part in *orthogonality* between Latin squares, as will be explained later in this dissertation.

A quasigroup satisfying the identity $a \circ a = a$ has the property that, if its Cayley table is bordered in natural order, the main diagonal of its Cayley table is in natural order. A formal definition of the notion of a Latin square with such an underlying quasigroup is given below and is also commonly found in literature on Latin squares (see, for instance, Colbourn *et al.* [38, p. 136]).

Definition 2.1.7 (Idempotent Latin square) *A Latin square $\boldsymbol{L}$ is* idempotent *if $\boldsymbol{L}(i, i) = i$ for all $i \in \mathbb{Z}_n$, or equivalently if the main diagonal of the Latin square is a transversal in natural order.* □

For example, the Latin square

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

is idempotent. In fact, let $(\mathbb{Z}_{2m+1}, \odot)$ be a quasigroup where $\odot$ is defined as

$$a \odot b = (m + 1)(a + b) \pmod{2m + 1},$$

for $a, b \in \mathbb{Z}_{2m+1}$ and $m \in \mathbb{N}$. Then, for any $a \in \mathbb{Z}_{2m+1}$,

$$a \odot a = (m+1)2a = (2m+1+1)a = a \pmod{2m+1},$$

and hence the Cayley table of $(\mathbb{Z}_{2m+1}, \odot)$ is an idempotent Latin square (the idempotent Latin square above is the Cayley table of $(\mathbb{Z}_7, \odot)$). If the Cayley table of a quasigroup is an idempotent Latin square, then the quasigroup is also said to be *idempotent*. It will be shown later in this chapter that an idempotent Latin square exists for any order $n \neq 2$.

2.2 Orthogonality between Latin squares

A notion in the theory of Latin squares which has given rise to extremely challenging problems, as well as a number of useful applications in various fields, is that of *orthogonality* between Latin squares. In fact, as noted in §1.1, Latin squares were first studied by Euler with the notion of orthogonality in mind. The following definition may be found in Colbourn *et al.* [38, p. 160] and Dénes and Keedwell [41, p. 154].

Definition 2.2.1 (Orthogonality) *Two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are* orthogonal *if $\boldsymbol{L}(i,j) = \boldsymbol{L}(k,\ell)$ and $\boldsymbol{L}'(i,j) = \boldsymbol{L}'(k,\ell)$ imply that $i = k$ and $j = \ell$ for all $i, j, k, \ell \in \mathbb{Z}_n$, in which case $\boldsymbol{L}$ and $\boldsymbol{L}'$ are called* orthogonal mates *of one another.* □

In other words, two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are orthogonal if the ordered pair $(\boldsymbol{L}(i,j), \boldsymbol{L}'(i,j))$ is unique as i and j vary over $\mathbb{Z}_n$. Furthermore, if U is a universal in $\boldsymbol{L}$ and $(i,j), (k,\ell) \in U$, then $\boldsymbol{L}'(i,j) = \boldsymbol{L}'(k,\ell)$ implies that $i = k$ and $j = \ell$ (by definition), and therefore U represents a transversal in $\boldsymbol{L}'$. Each universal in $\boldsymbol{L}$ is therefore associated with a transversal in $\boldsymbol{L}'$, and it follows that a Latin square has an orthogonal mate if and only if it consists of n transversals that are pairwise disjoint. The Latin squares

$$\boldsymbol{L}_{2.5} = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{2.6} = \begin{bmatrix} 0 & 3 & 2 & 1 \\ 3 & 0 & 1 & 2 \\ 1 & 2 & 3 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix},$$

are, for example, orthogonal. Notice that the set of entries $\{(0,0), (1,2), (2,1), (3,3)\}$ is a universal (of the element 0) in $\boldsymbol{L}_{2.5}$ and a transversal in $\boldsymbol{L}_{2.6}$, and the same is true for the other three universals of $\boldsymbol{L}_{2.5}$. The Latin square

$$\boldsymbol{L}_{2.7} = \begin{bmatrix} 0 & 3 & 2 & 1 \\ 3 & 0 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \end{bmatrix}$$

is, however, not orthogonal to $\boldsymbol{L}_{2.5}$ since, whereas $\{(0,0), (1,2), (2,1), (3,3)\}$ is a universal in $\boldsymbol{L}_{2.5}$, it is not a transversal in $\boldsymbol{L}_{2.7}$.

It is also often useful to consider a set $\{\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1}\}$ of k Latin squares of order n in which $\boldsymbol{L}_i$ and $\boldsymbol{L}_j$ are orthogonal for all $i, j \in \mathbb{Z}_k$, which is referred to as a set of k *mutually orthogonal Latin squares (MOLS)* of order n (see, for instance, Colbourn *et al.* [38, Definition 3.3]). For reasons that will be made clear later in this dissertation, it will be more convenient to define a set of MOLS to be ordered. In other words, an ordered k-tuple $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of mutually orthogonal Latin squares of order n will henceforth be considered instead of an unordered set, and such a tuple will be referred to as a k-MOLS of order n.

The next theorem provides an upper bound on the cardinality of a k-MOLS of order n.

Theorem 2.2.1 (Theorem 5.1.5, [41]) *A k-MOLS of order n can contain no more than $n-1$ Latin squares.*

Proof: Assume, to the contrary, that $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{n-1})$ is an n-MOLS of order n. Note, for any $\boldsymbol{L}_i$ and $\boldsymbol{L}_j$ where $i, j \in \mathbb{Z}_n$ and $i \neq j$, that $\boldsymbol{L}_i(1,0) = \boldsymbol{L}_i(0,k)$ and $\boldsymbol{L}_j(1,0) = \boldsymbol{L}_j(0,\ell)$ necessarily imply that $k \neq \ell$, since otherwise $(\boldsymbol{L}_i(1,0), \boldsymbol{L}_j(1,0)) = (\boldsymbol{L}_i(0,k), \boldsymbol{L}_j(0,k))$, which contradicts the orthogonality of $\boldsymbol{L}_i$ and $\boldsymbol{L}_j$. Since there are n Latin squares in this set, $\boldsymbol{L}_i(1,0) = \boldsymbol{L}_i(0,0)$ must follow for some $i \in \mathbb{Z}_n$, which contradicts the latinness of $\boldsymbol{L}_i$. ■

The following theorem (which utilises the notion of a *finite field*[2]) states that the upper bound given in Theorem 2.2.1 is attainable for certain orders, in which case the set of MOLS is called a *complete set* of MOLS. This well-known theorem was originally established by Bose [21] in 1938, and may be found in most textbooks on the subjects of combinatorics, combinatorial designs and Latin squares (see, for instance, Grimaldi [67, Theorem 17.16], Wallis [142, Corollary 10.3.1] and Dénes and Keedwell [41, Theorem 5.2.3]).

Theorem 2.2.2 *An $(n-1)$-MOLS of order n exists if $n = p^r$, where p is prime and $r \in \mathbb{N}$.*

Proof: Let $(G, +, \times) = GF(p^r)$ denote the finite field of order p^r where p is prime and $r \in \mathbb{N}$. For any $\lambda \in G \backslash \{0\}$ (where 0 is the additive identity), it is easy to see that the equation $a + \lambda b = c$ always has a unique solution, given any two of a, b and c, and that a Latin square $\boldsymbol{L}_\lambda$ may be defined such that $\boldsymbol{L}_\lambda(i,j) = i + \lambda j$ for each $i, j \in G$. Furthermore, let

$$(\boldsymbol{L}_\lambda(i,j), \boldsymbol{L}_\mu(i,j)) = (\boldsymbol{L}_\lambda(k,\ell), \boldsymbol{L}_\mu(k,\ell)),$$

where $\lambda, \mu, i, j, k, \ell \in G$ and $\lambda \neq \mu$. Then $i + \lambda j = k + \lambda \ell$ and $(i-k) + \lambda(j-\ell) = 0$, and similarly $(i-k) + \mu(j-\ell) = 0$. Hence

$$\lambda(j-\ell) = \mu(j-\ell),$$

and since $\lambda \neq \mu$, it must hold that $j = \ell$. Since $(i-k) + \lambda(j-\ell) = 0$, it follows that $i = k$, and therefore that $\boldsymbol{L}_\lambda$ and $\boldsymbol{L}_\mu$ are orthogonal. Hence the $p^r - 1$ elements of $G \backslash \{0\}$ give $p^r - 1$ Latin squares, any two of which are orthogonal. ■

For example, in [67, pp. 846–847] it is shown that $\mathbb{Z}_2[x]/(1 + x + x^2) = \{0, 1, x, 1 + x\}$ forms the finite field $GF(4)$. The three Latin squares of order 4 obtained by the method of Theorem 2.2.2 are

$$\begin{bmatrix} 0 & 1 & x & 1+x \\ 1 & 0 & 1+x & x \\ x & 1+x & 0 & 1 \\ 1+x & x & 1 & 0 \end{bmatrix},$$

[2]It is well known that *finite fields* (also known as *Galois fields*) are extremely useful in the construction of various types of combinatorial designs, as discussed in most books on (or containing chapters on) combinatorial designs. This notion is not discussed in detail in this dissertation; detailed discussions on the construction and application of finite fields (which includes the notions of *irreducible polynomials* and the division algorithm for polynomials) may, however, be found in Grimaldi [67, §17] and Wallis [142].

where the entry (i,j) contains $i+j$,

$$\begin{bmatrix} 0 & x & 1+x & 1 \\ 1 & 1+x & x & 0 \\ x & 0 & 1 & 1+x \\ 1+x & 1 & 0 & x \end{bmatrix},$$

where the entry (i,j) contains $i+xj$, and

$$\begin{bmatrix} 0 & 1+x & 1 & x \\ 1 & x & 0 & 1+x \\ x & 1 & 1+x & 0 \\ 1+x & 0 & x & 1 \end{bmatrix},$$

where the entry (i,j) contains $i+(1+x)j$. It may be verified that these three Latin squares form a 3-MOLS of order 4. In what follows the Latin square containing $i+\lambda j$ in row i and column j for $i,j,\lambda \in GF(n)$ is referred to as the *λ-Latin square of $GF(n)$*.

2.3 Operations on Latin squares

An aspect of Latin squares that has to be addressed before embarking on a search for Latin squares exhibiting certain properties is the question of when two Latin squares are different, and in what sense they are different. First of all, two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are *equal*, denoted by $\boldsymbol{L}=\boldsymbol{L}'$, if and only if, for every $i,j \in \mathbb{Z}_n$, $\boldsymbol{L}(i,j)=\boldsymbol{L}'(i,j)$; otherwise they are *distinct*. Consider, however, the distinct Latin squares

$$\boldsymbol{L}_{2.8} = \begin{bmatrix} a & b & c \\ b & c & a \\ c & a & b \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{2.9} = \begin{bmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \\ \gamma & \alpha & \beta \end{bmatrix}.$$

Upon inspection it may immediately be seen that these Latin squares essentially have the same structures; they are only represented by different symbol sets. It follows that any symbol change leaves the structure or some underlying properties of a Latin square unchanged. The Latin square

$$\boldsymbol{L}_{2.10} = \begin{bmatrix} b & a & c \\ a & c & b \\ c & b & a \end{bmatrix}$$

is also essentially the same as $\boldsymbol{L}_{2.8}$ and $\boldsymbol{L}_{2.9}$; a may be replaced by b and *vice versa* to transform $\boldsymbol{L}_{2.10}$ to $\boldsymbol{L}_{2.8}$. Thus a symbol change may also imply a permutation on the symbol set.

Since Latin squares of order n in this dissertation are represented by a single symbol set, namely $\mathbb{Z}_n$, the only symbol changes that are considered are permutations on the symbol set, and the symmetric group S_n represents all $n!$ possible permutations that may be performed on the symbol set of a Latin square of order n. Similar operations may be performed on the indexing sets of a Latin square as well. The rows or columns of a Latin square may be rearranged in any order according to any of the $n!$ elements of the symmetric group S_n. It is easy to see that none of these operations destroys the defining property of a Latin square.

Consider applying a permutation p to the columns of a Latin square $\boldsymbol{L}$ of order n in order to obtain a Latin square $\boldsymbol{L}'$. Hence, in the underlying quasigroup of $\boldsymbol{L}$ the operation $i \circ j = k$ becomes $i \circ p(j) = k$. This permutation implies that the column in position i of $\boldsymbol{L}$ moves to position $p(i)$. Equivalently, since $\boldsymbol{L}'(i,p(j)) = \boldsymbol{L}(i,j)$ for all $i,j \in \mathbb{Z}_n$, $\boldsymbol{L}'(i) \circ p = \boldsymbol{L}(i)$ for all $i \in \mathbb{Z}_n$. Hence if a permutation p is applied to the columns of a Latin square $\boldsymbol{L}$, then $\boldsymbol{L}(i)$ is replaced by $\boldsymbol{L}(i) \circ p^{-1}$ for all $i \in \mathbb{Z}_n$. Similary, applying p to the rows of $\boldsymbol{L}$ replaces $\boldsymbol{L}^T(i)$ by $\boldsymbol{L}^T(i) \circ p^{-1}$. If p is applied to the symbol set of $\boldsymbol{L}$, the operation $i \circ j = k$ becomes $i \circ j = p(k)$. Hence the symbol k is replaced by the symbol $p(k)$ in $\boldsymbol{L}$. Also, since $p(\boldsymbol{L}(i,j)) = \boldsymbol{L}''(i,j)$ for all $i, j \in \mathbb{Z}_n$ (where $\boldsymbol{L}''$ is the resulting Latin square after p has been applied to the symbols of $\boldsymbol{L}$), $p \circ \boldsymbol{L}(i) = \boldsymbol{L}''(i)$ for all $i \in \mathbb{Z}_n$. Hence row $\boldsymbol{L}(i)$ is replaced by $p \circ \boldsymbol{L}(i)$ in this case.

For example, consider the Latin square

$$\boldsymbol{L}_{2.11} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}$$

and consider a permutation $p_r = \binom{0\,1\,2\,3}{1\,2\,3\,0}$ applied to the rows of $\boldsymbol{L}_{2.11}$, a permutation $p_c = \binom{0\,1\,2\,3}{2\,3\,0\,1}$ applied to the columns of $\boldsymbol{L}_{2.11}$ and finally a permutation $p_s = \binom{0\,1\,2\,3}{1\,0\,3\,2}$ applied to the symbol set of $\boldsymbol{L}_{2.11}$. The resulting Latin square is

$$\boldsymbol{L}_{2.12} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 2 & 3 & 0 & 1 \\ 1 & 0 & 3 & 2 \end{bmatrix}.$$

Since p_r moves the row in position 3 in $\boldsymbol{L}$ to position 0, $\boldsymbol{L}_{2.12}(0) = p_s \circ \boldsymbol{L}_{2.11}(3) \circ p_c^{-1}$. Indeed,

$$\begin{pmatrix} 0\,1\,2\,3 \\ 1\,0\,3\,2 \end{pmatrix} \circ \begin{pmatrix} 0\,1\,2\,3 \\ 3\,2\,1\,0 \end{pmatrix} \circ \begin{pmatrix} 0\,1\,2\,3 \\ 2\,3\,0\,1 \end{pmatrix} = \begin{pmatrix} 0\,1\,2\,3 \\ 0\,1\,2\,3 \end{pmatrix}.$$

The three permutations applied above may be applied in any order without altering the final outcome of the sequence of operations. This is true since these three permutations replace the triple $(i, j, \boldsymbol{L}_{2.11}(i,j))$ with the triple $(p_r(i), p_c(j), p_s(\boldsymbol{L}_{2.11}))$, from which it is clear that they may be applied in any order. Since these three permutations produce a Latin square of order n when applied to a Latin square of the same order, they are collectively an element of the group S_n^3 acting on the set of all Latin squares of order n.

Let two permutations, p and q, be applied consecutively to the rows of a Latin square $\boldsymbol{L}$. Since the row in position i of $\boldsymbol{L}$ moves to position $p(i)$ and thereafter to position $q(p(i))$, applying p and q to $\boldsymbol{L}$ (in that order) is equivalent to applying $q \circ p$ to $\boldsymbol{L}$. A similar argument shows that the composition of permutations may also be applied to the rows and symbol set of a Latin square instead of applying the permutations individually. Furthermore, consider applying the two permutations p and p^{-1} to a Latin square $\boldsymbol{L}$. This is equivalent to applying $p \circ p^{-1} = e$, the identity permutation, to $\boldsymbol{L}$, leaving $\boldsymbol{L}$ unchanged. Hence each rearrangement of the rows is reversible. Similar arguments deliver the same result for the columns and symbol set of a Latin square.

Row, column and symbol permutations may also be defined for MOLS. For the purpose of defining these operations it is convenient to consider the so-called *orthogonal array* representation [99] of a Latin square. The following definition may be found in Colbourn *et al.* [38, Definition 3.5].

Definition 2.3.1 (Orthogonal array) *An* orthogonal array *of strength 2, index 1, degree k and order n, denoted by $OA(k,n)$, is a $k \times n^2$ array $\boldsymbol{A}$ containing elements from the set $\mathbb{Z}_n$ in such a way that any $2 \times n^2$ sub-array of $\boldsymbol{A}$ contains no repeated columns.* □

In what follows, the row and column indices of an $OA(k,n)$ are denoted by $\mathbb{Z}_k$ and $\mathbb{Z}_{n^2}$ respectively, and the notation $\boldsymbol{A}(i,j)$ is used to denote the entry in row i and column j of an $OA(k,n)$ $\boldsymbol{A}$. An example of an $OA(5,4)$ is

$$\boldsymbol{A}_{2.1} = \begin{bmatrix} 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \\ 0&1&2&3&0&1&2&3&0&1&2&3&0&1&2&3 \\ 0&1&2&3&1&0&3&2&2&3&0&1&3&2&1&0 \\ 0&1&2&3&2&3&0&1&3&2&1&0&1&0&3&2 \\ 0&1&2&3&3&2&1&0&1&0&3&2&2&3&0&1 \end{bmatrix}.$$

Since an $OA(k,n)$ has n^2 columns, and since no two columns of any $2 \times n^2$ sub-array are equal, it follows that for every ordered pair $(i,j) \in \mathbb{Z}_n^2$ and any two rows $a, b \in \mathbb{Z}_k$ there exists exactly one column $c \in \mathbb{Z}_{n^2}$ such that $\boldsymbol{A}(a,c) = i$ and $\boldsymbol{A}(b,c) = j$. This fact gives rise to the following theorem which establishes the connection between orthogonal Latin squares and orthogonal arrays.

Theorem 2.3.1 *An $OA(k+2,n)$ is equivalent to a k-MOLS of order n.*

Proof: Let $\boldsymbol{A}$ be an $OA(k+2,n)$, and let $\boldsymbol{L}_\ell$ be an $n \times n$ array such that $\boldsymbol{L}_\ell(\boldsymbol{A}(0,c), \boldsymbol{A}(1,c)) = \boldsymbol{A}(\ell+2,c)$ for all $c \in \mathbb{Z}_{n^2}$ and $0 \leq \ell \leq k-1$. Since, for any $i,j \in \mathbb{Z}_n$, there is only one element $c \in \mathbb{Z}_{n^2}$ with the properties that $\boldsymbol{A}(0,c) = i$ and $\boldsymbol{A}(\ell+2,c) = \boldsymbol{L}_\ell(i,j)$, the ordered pair $(i, \boldsymbol{L}_\ell(i,j))$ is unique as i and j vary over $\mathbb{Z}_n$. Each element of $\mathbb{Z}_n$ therefore appears exactly once in each row of $\boldsymbol{L}_\ell$, and it may similarly be shown that each element of $\mathbb{Z}_n$ appears exactly once in each column of $\boldsymbol{L}_\ell$. Hence $\boldsymbol{L}_\ell$ is a Latin square for all $0 \leq \ell \leq k-1$. Furthermore, for any $i,j \in \mathbb{Z}_n$ and any $\ell \neq m$, there is only one element $c \in \mathbb{Z}_{n^2}$ with the properties that $\boldsymbol{A}(\ell+2,c) = \boldsymbol{L}_\ell(i,j)$ and $\boldsymbol{A}(m+2,c) = \boldsymbol{L}_m(i,j)$, and hence the ordered pair $(\boldsymbol{L}_\ell(i,j), \boldsymbol{L}_m(i,j))$ is unique as i and j vary over $\mathbb{Z}_n$. It therefore follows that $\boldsymbol{L}_\ell$ and $\boldsymbol{L}_m$ are orthogonal for any $\ell \neq m$, and $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ therefore forms a k-MOLS of order n. ■

Given a k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n, let $T(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ henceforth denote the set of tuples $(i, j, \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, \boldsymbol{L}_{k-1}(i,j))$ for all $i,j \in \mathbb{Z}_n$. From the proof of Theorem 2.3.1 it is therefore clear that the elements of $T(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ represent the columns of an $OA(k+2,n)$. In the case of a single Latin square $\boldsymbol{L}$, $T(\boldsymbol{L})$ contains the triples $(i,j,\boldsymbol{L}(i,j))$ for all $i,j \in \mathbb{Z}_n$ which represent the columns of an $OA(3,n)$. The $OA(5,4)$ $\boldsymbol{A}_{2.1}$, for example, is equivalent in this way to the 3-MOLS

$$\mathcal{M}_{2.1} = \left(\begin{bmatrix} 0&1&2&3 \\ 1&0&3&2 \\ 2&3&0&1 \\ 3&2&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&2&3 \\ 2&3&0&1 \\ 3&2&1&0 \\ 1&0&3&2 \end{bmatrix}, \begin{bmatrix} 0&1&2&3 \\ 3&2&1&0 \\ 1&0&3&2 \\ 2&3&0&1 \end{bmatrix} \right)$$

of order 4.

It is easy to verify that if a permutation of the elements of $\mathbb{Z}_n$ is applied to all the entries in any row of an $OA(k,n)$, then the resulting array is still an orthogonal array. This implies that any k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n may be transformed into another k-MOLS of order n by applying $k+2$ permutations, namely one to the rows of $\boldsymbol{L}_i$ for all $i \in \mathbb{Z}_k$, one to the columns of $\boldsymbol{L}_i$ for all $i \in \mathbb{Z}_k$, and one to the symbols of each of the k Latin squares individually. Hence the permutations applied to the rows and columns of all Latin squares in a k-MOLS of order n must be equal in order to preserve orthogonality between them, while independent permutations may be applied to the symbol sets of the Latin squares without destroying the orthogonality between them.

Consider, for example, applying the permutation $\binom{0\,1\,2\,3}{3\,0\,1\,2}$ to the rows of the Latin squares in $\mathcal{M}_{2.1}$, the permutation $\binom{0\,1\,2\,3}{0\,2\,1\,3}$ to the columns, and the permutation $\binom{0\,1\,2\,3}{3\,1\,2\,0}$ to the symbol set of the last Latin square in the set (in the order in which they are presented in $\mathcal{M}_{2.1}$). The resulting 3-MOLS of order 4 is

$$\left(\begin{bmatrix} 1&3&0&2\\ 2&0&3&1\\ 3&1&2&0\\ 0&2&1&3 \end{bmatrix}, \begin{bmatrix} 2&0&3&1\\ 3&1&2&0\\ 1&3&0&2\\ 0&2&1&3 \end{bmatrix}, \begin{bmatrix} 0&1&2&3\\ 1&0&3&2\\ 2&3&0&1\\ 3&2&1&0 \end{bmatrix}\right).$$

The fact that independent permutations may be applied to the symbol sets of the Latin squares of a k-MOLS provides a useful tool in proving certain basic properties of MOLS, as illustrated by the following result.

Lemma 2.3.1 ([14]) *If a k-MOLS of order n exists, then a $(k-1)$-MOLS of order n exists in which each Latin square is idempotent.*

Proof: Let $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ be a k-MOLS of order n, and let the rows of all these Latin squares be permuted using one permutation in such a way that $\boldsymbol{L}_{k-1}$ is unipotent[3]. By the property of orthogonality it follows that $\boldsymbol{L}_i$ contains a transversal on its main diagonal for all $0 \leq i \leq k-2$, and the desired result follows by applying $k-1$ independent permutations to the symbol sets of $\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-2}$ in such a way that the resulting Latin squares are all idempotent. ■

Another operation that may be applied to an orthogonal array is to rearrange the rows of the array. It is easy to verify that this does not destroy the defining property of the array, and it corresponds to uniformly applying a single permutation of $\mathbb{Z}_{k+2}$ to each tuple in $T(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ for a k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n. This operation delivers a new set of tuples, $T(\boldsymbol{L}'_0, \boldsymbol{L}'_1, \ldots, \boldsymbol{L}'_{k-1})$ say, which defines a new k-MOLS $(\boldsymbol{L}'_0, \boldsymbol{L}'_1, \ldots, \boldsymbol{L}'_{k-1})$ of order n. In the case where $k = 1$ (*i.e.* in the case of a single Latin square), the resulting Latin square is known in the literature as a *conjugate* of the original Latin square (see, for instance, Colbourn *et al.* [38, p. 135]). The following definition, however, also includes the cases where $1 < k < n$.

Definition 2.3.2 (Conjugate) *Given a k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n, the resulting k-MOLS of order n obtained by uniformly permuting the elements of the tuples $(i, j, \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, \boldsymbol{L}_{k-1}(i,j))$ for all $i, j \in \mathbb{Z}_n$ is a* conjugate *of $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$.* □

The underlying quasigroup of a conjugate of a Latin square $\boldsymbol{L}$ is a *conjugate* or *parastrophic* quasigroup of the underlying quasigroup of $\boldsymbol{L}$ [41, p. 65]. The notion of a conjugate of a Latin square has also been referred to as an *adjugate* or *parastrophe* of the Latin square [99].

It is clear, by definition, that a k-MOLS of order n has $(k+2)!$ (not necessarily distinct) conjugates. In what follows, each of the six conjugates of a single Latin square $\boldsymbol{L}$ (*i.e.* where $k = 1$) and their relationships with $\boldsymbol{L}$ are treated in detail. Naturally, the identity permutation of S_3 leaves $T(\boldsymbol{L})$ unchanged, and this conjugate, simply denoted by $\boldsymbol{L}$, is the identity conjugate of $\boldsymbol{L}$.

Consider the permutation $\binom{0\,1\,2}{1\,0\,2}$ applied to $T(\boldsymbol{L})$. Here the roles of the rows and columns in $\boldsymbol{L}$ are swapped, and hence this conjugate is the transpose of $\boldsymbol{L}$, *i.e.* $\boldsymbol{L}^T$. To see this more

[3] A Latin square $\boldsymbol{L}$ of order n is *unipotent* if $\boldsymbol{L}(i,i) = k$ for all $i \in \mathbb{Z}_n$ and some $k \in \mathbb{Z}_n$.

clearly, note that, since the permutation $\binom{012}{102}$ interchanges the first two elements of the triple $(i, j, \boldsymbol{L}(i,j))$, the conjugate has the property that if $\boldsymbol{L}(i,j) = k$, then $\boldsymbol{L}^T(j,i) = k$.

Next consider the permutation $\binom{012}{021}$ applied to $T(\boldsymbol{L})$. The resulting conjugate of $\boldsymbol{L}$, denoted by $\boldsymbol{L}^{-1}$ (see Dénes and Keedwell [41, p. 125]), has the property that if $\boldsymbol{L}(i,j) = k$, then $\boldsymbol{L}^{-1}(i,k) = j$. Hence if the image of j under the permutation $\boldsymbol{L}(i)$ is k, then the image of k under the permutation $\boldsymbol{L}^{-1}(i)$ is j, and $\boldsymbol{L}^{-1}(i) = (\boldsymbol{L}(i))^{-1}$ for all $i \in \mathbb{Z}_n$. In other words each row in $\boldsymbol{L}^{-1}$ represents the inverse permutation of each row in $\boldsymbol{L}$.

Let τ henceforth denote the operation of replacing a Latin square by its transpose and let ι henceforth denote an identity operation leaving a Latin square unchanged. Furthermore, let ρ denote the operation of replacing each row in $\boldsymbol{L}$ by its inverse permutation.

Let the composition $\rho\tau$ denote the operation of first applying τ and then ρ to a Latin square. It is easy to see that if the operation $\gamma = \tau\rho\tau$ is applied to a Latin square $\boldsymbol{L}$, each column of $\boldsymbol{L}$ is replaced by its inverse permutation. This is equivalent to applying the permutation

$$\begin{pmatrix}012\\102\end{pmatrix} \circ \begin{pmatrix}012\\021\end{pmatrix} \circ \begin{pmatrix}012\\102\end{pmatrix} = \begin{pmatrix}012\\210\end{pmatrix}$$

to $T(\boldsymbol{L})$, and it delivers a conjugate, denoted by ${}^{-1}\boldsymbol{L}$. Hence, $({}^{-1}\boldsymbol{L})^T(i) = (\boldsymbol{L}^T(i))^{-1}$, and the operation γ therefore replaces each coloumn of a Latin square by its inverse. Note that this is also equivalent to applying the permutation

$$\begin{pmatrix}012\\021\end{pmatrix} \circ \begin{pmatrix}012\\102\end{pmatrix} \circ \begin{pmatrix}012\\021\end{pmatrix} = \begin{pmatrix}012\\210\end{pmatrix}$$

to $T(\boldsymbol{L})$, hence $\gamma = \tau\rho\tau = \rho\tau\rho$. Furthermore, consider application of the operation $\tau\rho$ to $\boldsymbol{L}$, which is equivalent to applying the permutation

$$\begin{pmatrix}012\\102\end{pmatrix} \circ \begin{pmatrix}012\\021\end{pmatrix} = \begin{pmatrix}012\\120\end{pmatrix}$$

to $T(\boldsymbol{L})$. It may easily be verified that $\tau\rho = \rho\gamma$. The conjugate arising from applying $\tau\rho$ to $\boldsymbol{L}$ is simply the transpose of $\boldsymbol{L}^{-1}$, denoted by $(\boldsymbol{L}^{-1})^T$. Finally, consider application of the operation $\tau\gamma = \rho\tau$ to $\boldsymbol{L}$, which is equivalent to applying the permutation

$$\begin{pmatrix}012\\021\end{pmatrix} \circ \begin{pmatrix}012\\102\end{pmatrix} = \begin{pmatrix}012\\201\end{pmatrix}$$

to $T(\boldsymbol{L})$. The resulting conjugate is simply the transpose of ${}^{-1}\boldsymbol{L}$, denoted by $({}^{-1}\boldsymbol{L})^T$. In summary, the six conjugates of a Latin square are listed in Table 2.1 together with the corresponding operations (henceforth referred to as the *conjugate operations*) applied to $\boldsymbol{L}$ and permutations applied to $T(\boldsymbol{L})$ in order to obtain each conjugate.

Conjugate	$\boldsymbol{L}$	$\boldsymbol{L}^T$	$\boldsymbol{L}^{-1}$	$(\boldsymbol{L}^{-1})^T$	${}^{-1}\boldsymbol{L}$	$({}^{-1}\boldsymbol{L})^T$
Operation	ι	τ	ρ	$\tau\rho$	γ	$\tau\gamma$
Permutation	$\binom{012}{012}$	$\binom{012}{102}$	$\binom{012}{021}$	$\binom{012}{120}$	$\binom{012}{210}$	$\binom{012}{201}$

TABLE 2.1: *The six conjugates of a Latin square $\boldsymbol{L}$ together with the operations applied to $\boldsymbol{L}$ and the permutations applied to $T(\boldsymbol{L})$ by which they are formed.*

Consider, for example, the six conjugates of the Latin square

$$\boldsymbol{L}_{2.13} = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{bmatrix},$$

which are given by

$$\boldsymbol{L}_{2.13} = \begin{bmatrix} 0&3&1&2\\1&2&0&3\\3&0&2&1\\2&1&3&0 \end{bmatrix}, \qquad \boldsymbol{L}_{2.13}^T = \begin{bmatrix} 0&1&3&2\\3&2&0&1\\1&0&2&3\\2&3&1&0 \end{bmatrix},$$

$$\boldsymbol{L}_{2.13}^{-1} = \begin{bmatrix} 0&2&3&1\\2&0&1&3\\1&3&2&0\\3&1&0&2 \end{bmatrix}, \qquad (\boldsymbol{L}_{2.13}^{-1})^T = \begin{bmatrix} 0&2&1&3\\2&0&3&1\\3&1&2&0\\1&3&0&2 \end{bmatrix},$$

$$^{-1}\boldsymbol{L}_{2.13} = \begin{bmatrix} 0&1&3&2\\2&3&1&0\\1&0&2&3\\3&2&0&1 \end{bmatrix}, \qquad (^{-1}\boldsymbol{L}_{2.13})^T = \begin{bmatrix} 0&2&1&3\\1&3&0&2\\3&1&2&0\\2&0&3&1 \end{bmatrix}.$$

It is clear from Table 2.1 and the discussion above that the set $\{\iota, \tau, \rho, \tau\rho, \gamma, \tau\gamma\}$ forms a group isomorphic[4] to the symmetric group S_3, and hence to the dihedral group D_3. The Cayley-table of D_3, as represented by the set of conjugate operations, is given in Table 2.2.

	ι	τ	ρ	$\tau\rho$	γ	$\tau\gamma$
ι	ι	τ	ρ	$\tau\rho$	γ	$\tau\gamma$
τ	τ	ι	$\tau\rho$	ρ	$\tau\gamma$	γ
ρ	ρ	$\tau\gamma$	ι	γ	$\tau\rho$	τ
$\tau\rho$	$\tau\rho$	γ	τ	$\tau\gamma$	ρ	ι
γ	γ	$\tau\rho$	$\tau\gamma$	τ	ι	ρ
$\tau\gamma$	$\tau\gamma$	ρ	γ	ι	τ	$\tau\rho$

TABLE 2.2: *The Cayley table of D_3 as represented by the set $\{\iota, \tau, \rho, \tau\rho, \gamma, \tau\gamma\}$.*

It is easy to verify that the non-trivial subgroups of D_3 are $\{\iota, \rho\}$, $\{\iota, \gamma\}$, $\{\iota, \tau\}$ and $\{\iota, \tau\rho, \tau\gamma\}$ when represented by the set $\{\iota, \tau, \rho, \tau\rho, \gamma, \tau\gamma\}$. As discussed in §A.2.2, any single element of this set generates one of these subgroups and by Corollary A.2.1 any two elements from two different subsets generate the entire group D_3. For instance, if the transformation $\tau\rho$ is used to transform $\boldsymbol{L}$ into $(\boldsymbol{L}^{-1})^T$, then $\boldsymbol{L}$ may also be transformed either into $(^{-1}\boldsymbol{L})^T$ or into itself, since $\tau\rho$ generates the subgroup $\{\iota, \tau\rho, \tau\gamma\}$. It is also clear by this argument that any collection of the conjugate operations of a Latin square of order n are actions of some subgroup of D_3 on the set of all Latin squares of order n.

Consider applying a permutation $p_r \in S_n$ to $R(\boldsymbol{L})$ (where $\boldsymbol{L}$ is a Latin square of order n), a permutation $p_c \in S_n$ to $C(\boldsymbol{L})$, a permutation $p_s \in S_n$ to $S(\boldsymbol{L})$ and a permutation $\alpha \in S_3$ to $T(\boldsymbol{L})$. Since α actually maps the sets $R(\boldsymbol{L})$, $C(\boldsymbol{L})$ and $S(\boldsymbol{L})$ to one another and since p_r, p_c and p_c are permutations of these sets respectively, these transformations together form the element (p_r, p_c, p_s, α) of a group known as the *wreath product*[5] of S_n and S_3, denoted by $S_n \wr S_3$. If the case is considered where α is restricted to be an element the subgroup of D_3 generated by τ, namely $\langle\tau\rangle = \{\iota, \tau\} \cong S_2$, then the transformations p_r, p_c, p_s and α form an element of the group $S_n \times S_n \wr S_2$ since τ only permutes the sets $R(\boldsymbol{L})$ and $C(\boldsymbol{L})$. It is clear that any collection

[4] Two groups $(G, \circ)$ and $(H, \bullet)$ are isomorphic if $|G| = |H|$ and there exists a one-to-one mapping α from G to H such that $\alpha(a \circ b) = \alpha(a) \bullet \alpha(b)$ for $a, b \in G$. Table 2.1 gives the isomorphism between $\{\iota, \tau, \rho, \tau\rho, \gamma, \tau\gamma\}$ and D_3, where the image of each conjugate operation is the corresponding permutation given below it.

[5] See, for instance, Hall [69, p. 81] and Rotman [124, p. 142] for a definition of this product of groups.

of operations applied to a Latin square of order n is a group action on the set of all Latin squares of order n.

A similar study can be made of the conjugate operations that may be applied to a k-MOLS of order n where $k > 1$. For a 2-MOLS of order n, however, there are already $(2+2)! = 24$ conjugate operations, and it would be too lengthy to consider each one in detail.

Some interesting observations may still be made in general without considering each conjugate separately. First of all it may be noted that a permutation which interchanges the first two elements of each tuple $(i, j, \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, \boldsymbol{L}_{k-1}(i,j))$ for all $i, j \in \mathbb{Z}_n$ for some k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n simply transposes $\boldsymbol{L}_i$ for all $i \in \mathbb{Z}_k$. Furthermore, a permutation which fixes the first two elements while permuting the last k elements of each tuple $(i, j, \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, \boldsymbol{L}_{k-1}(i,j))$ is equivalent to permuting the order of the Latin squares within the tuple $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$.

Consider a permutation $p \in S_{k+2}$ which interchanges the second element with an element within the last k positions of the tuple, while fixing the remaining elements in the tuple. Hence $(i, j, \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, \boldsymbol{L}_{k-1}(i,j))$ will be mapped to, say, $(i, \boldsymbol{L}_\ell(i,j), \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, j, \ldots, \boldsymbol{L}_{k-1}(i,j))$ for all $i, j \in \mathbb{Z}_n$ and some $\ell \in \mathbb{Z}_k$. It may be noted from the discussion above relating to the conjugates of a single Latin square that this operation replaces $\boldsymbol{L}_\ell$ by one of its conjugates, namely $\boldsymbol{L}_\ell^{-1}$. Furthermore, for any $\boldsymbol{L}_m$ (where $m \neq \ell$) this operation maps the entry $\boldsymbol{L}_m(i,j)$ to $\boldsymbol{L}_m(i, \boldsymbol{L}_\ell(i,j))$ for all $i, j \in \mathbb{Z}_n$. Hence each row $\boldsymbol{L}_m(i)$ is replaced by $\boldsymbol{L}_m(i) \circ \boldsymbol{L}_\ell(i)$ for all $i \in \mathbb{Z}_n$ and all $m \in \mathbb{Z}_k \backslash \{\ell\}$.

Similarly, interchanging the first element with the element in position $\ell > 2$ in the tuple, while fixing the remaining elements, is equivalent to replacing each column $\boldsymbol{L}_m^T(i)$ by $\boldsymbol{L}_m^T(i) \circ \boldsymbol{L}_\ell^T(i)$ for all $i \in \mathbb{Z}_n$ and all $m \in \mathbb{Z}_k \backslash \{\ell\}$, while $\boldsymbol{L}_\ell$ is mapped to ${}^{-1}\boldsymbol{L}_\ell$.

2.4 Recursive constructions of Latin squares

Recursive constructions of Latin squares refer to methods by which a collection of Latin squares may be combined in some sense, or by which a single Latin square may be extended in some sense, in order to produce a new Latin square of larger order (see, for instance, Dénes and Keedwell [42, §5]). Recursive constructions play an important role in the construction of orthogonal Latin squares, mainly due to the fact that these methods often carry over the property of orthogonality from the smaller to the larger Latin squares. In the past this has, for instance, enabled Euler to construct pairs of orthogonal Latin squares of orders which are multiples of four. Recursive constructions were also used by both Parker [115] and Zhu [154] in their disproofs of the Euler conjecture.

The notion of a transversal in a Latin square $\boldsymbol{L}$ of order n may be used to extend $\boldsymbol{L}$ to a Latin square of order $n + k$ by a process known as *prolongation*[6], which requires that $\boldsymbol{L}$ should have k disjoint transversals. Let $\boldsymbol{L}$ be a Latin square of order n with a transversal V, and let the entries of V be denoted in two different ways, namely as (i, v_i) or as (v_i', i) for all $i \in \mathbb{Z}_n$. The *row-projection* of V is defined as an ordered list of elements of $\mathbb{Z}_n$ such that the i-th position contains $\boldsymbol{L}(v_i', i)$, while the *column-projection* of V is defined as an ordered list of elements of $\mathbb{Z}_n$ such that the i-th position contains $\boldsymbol{L}(i, v_i)$. If a Latin square $\boldsymbol{L}$ has k disjoint transversals

[6] Dénes and Keedwell describe the method of prolongation for $k = 1$ in [41, p. 39] and the more general version in [42, p. 103–104]. For $k = 1$ this process has been called a *1-extension* by Yamamoto [153] and a *bordering procedure* by Colbourn and Rosa [39, p. 16].

$V_0, V_1, \ldots, V_{k-1}$, then *prolongation* may be performed by (i) replacing the entries of V_i in $\boldsymbol{L}$ by the element $n+i$ (so that V_i becomes a universal of an element not in $\boldsymbol{L}$) for all $0 \le i \le k-1$, (ii) by appending the row-projections (in any order) of V_i for all $0 \le i \le k-1$ to the rows of $\boldsymbol{L}$ and the column-projections (in any order) of V_i for all $0 \le i \le k-1$ to the columns of $\boldsymbol{L}$, and (iii) by filling the resulting $k \times k$ empty square in the bottom right corner of the resulting array using any Latin square of order k containing the symbols $n, n+1, \ldots, n+k-1$.

Consider, for instance, prolongation of the Latin square

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

using the three disjoint transversals

$$V_0 = \{(0,0),(1,3),(2,6),(3,2),(4,5),(5,1),(6,4)\},$$

$$V_1 = \{(0,4),(1,0),(2,3),(3,6),(4,2),(5,5),(6,1)\},$$

and

$$V_2 = \{(0,1),(1,4),(2,0),(3,3),(4,6),(5,2),(6,5)\},$$

as well as the Latin square

$$\begin{bmatrix} 7&8&9\\ 8&9&7\\ 9&7&8 \end{bmatrix}.$$

Furthermore, consider appending the row-projection of V_0 first, then appending the row-projection of V_1, followed by the row-projection of V_2, and appending the column-projections in the same order. The resulting Latin square after the three steps of prolongation is

$$\begin{bmatrix} \mathbf{7}&\mathbf{9}&1&5&\mathbf{8}&6&3&0&2&4\\ \mathbf{8}&5&2&\mathbf{7}&\mathbf{9}&0&4&6&1&3\\ \mathbf{9}&6&3&\mathbf{8}&4&1&\mathbf{7}&5&0&2\\ 3&0&\mathbf{7}&\mathbf{9}&5&2&\mathbf{8}&4&6&1\\ 4&1&\mathbf{8}&2&6&\mathbf{7}&\mathbf{9}&3&5&0\\ 5&\mathbf{7}&\mathbf{9}&3&0&\mathbf{8}&1&2&4&6\\ 6&\mathbf{8}&0&4&\mathbf{7}&\mathbf{9}&2&1&3&5\\ 0&2&4&6&1&3&5&\mathbf{7}&\mathbf{8}&\mathbf{9}\\ 1&3&5&0&2&4&6&\mathbf{8}&\mathbf{9}&\mathbf{7}\\ 2&4&6&1&3&5&0&\mathbf{9}&\mathbf{7}&\mathbf{8} \end{bmatrix},$$

where the entries containing the new symbols 7, 8 and 9 (including the entries of V_0, V_1 and V_2) are shown in boldface. An interesting application of prolongation arises in the proof of the existence of idempotent Latin squares for all orders $n > 2$, as illustrated by the following theorem.

Theorem 2.4.1 ([39], Lemma 1.2) *An idempotent Latin square of order n exists if and only if $n \neq 2$.*

Proof: Let $\boldsymbol{L}$ be the Cayley table of $(\mathbb{Z}_{2m+1}, \odot)$, where $m > 0$. In §2.1 it was shown that this quasigroup is idempotent, and therefore an idempotent Latin square exists for any odd order.

Let V be the set of distinct ordered pairs $(i, i+1)$ for all $i \in \mathbb{Z}_{2m+1}$. By the definition of the operator $\odot$ it is easy to see that $\boldsymbol{L}(i, i+1) = \boldsymbol{L}(j, j+1)$ if and only if $i = j$. Hence V is a transversal of $\boldsymbol{L}$. Let $\boldsymbol{L}'$ be the resulting Latin square of order $2m+2$ if $\boldsymbol{L}$ is extended via prolongation by V. Since $m \neq 0$, no entry on the diagonal of $\boldsymbol{L}$ is in V and since $\boldsymbol{L}'(2m+1, 2m+1) = 2m+1$ (there is only one Latin square of order 1), $\boldsymbol{L}'$ is an idempotent Latin square. Hence an idempotent Latin square exists for any even order greater than 2. Finally, it is easy to verify that there exists no idempotent Latin square of order 2. ■

Another way to extend a Latin square is to use the *direct product* of quasigroups, which, given two quasigroups $(G, \circ)$ and $(H, \bullet)$, is the quasigroup $(G \times H, \star)$ where $\star$ is defined by

$$(g_1, h_1) \star (g_2, h_2) = (g_1 \circ g_2, h_1 \bullet h_2)$$

for all $(g_1, h_1), (g_2, h_2) \in G \times H$ (see, for example, Allenby [4, Definition 6.3.1]). Let the *direct product* between two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$, denoted by $\boldsymbol{L} \times \boldsymbol{L}'$, be the Latin square represented by the Cayley-table of the direct product of the underlying quasigroups of $\boldsymbol{L}$ and $\boldsymbol{L}'$. Since $R(\boldsymbol{L}) = C(\boldsymbol{L}) = S(\boldsymbol{L}) = \mathbb{Z}_n$ and $R'(\boldsymbol{L}) = C'(\boldsymbol{L}) = S'(\boldsymbol{L}) = \mathbb{Z}_m$ (if $\boldsymbol{L}$ and $\boldsymbol{L}'$ are of orders n and m, respectively), it follows by definition of the direct product of quasigroups that $R(\boldsymbol{L} \times \boldsymbol{L}') = C(\boldsymbol{L} \times \boldsymbol{L}') = S(\boldsymbol{L} \times \boldsymbol{L}') = \mathbb{Z}_n \times \mathbb{Z}_m$. In order to conform to the convention of representing the elements of a Latin square of order n by the elements of $\mathbb{Z}_n$, the elements of $\boldsymbol{L} \times \boldsymbol{L}'$ are replaced by their images under some bijection from $\mathbb{Z}_n \times \mathbb{Z}_m$ to $\mathbb{Z}_{nm}$.

For example,

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) \\ (0,1) & (0,2) & (0,0) & (1,1) & (1,2) & (1,0) \\ (0,2) & (0,0) & (0,1) & (1,2) & (1,0) & (1,1) \\ (1,0) & (1,1) & (1,2) & (0,0) & (0,1) & (0,2) \\ (1,1) & (1,2) & (1,0) & (0,1) & (0,2) & (0,0) \\ (1,2) & (1,0) & (1,1) & (0,2) & (0,0) & (0,1) \end{bmatrix},$$

and using the bijection α where $\alpha(0) = (0,0)$, $\alpha(1) = (0,1)$, $\alpha(2) = (0,2)$, $\alpha(3) = (1,0)$, $\alpha(4) = (1,1)$ and $\alpha(5) = (1,2)$, the resulting Latin square

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

of order 6 is found. The following result, utilising the direct product, is also useful when recursively constructing Latin squares.

Lemma 2.4.1 *For any two Latin squares $\boldsymbol{L}$ and $\boldsymbol{M}$ of orders n and m respectively, $\boldsymbol{L}^T \times \boldsymbol{M}^T = (\boldsymbol{L} \times \boldsymbol{M})^T$.*

Proof: Let the elements of $\boldsymbol{L}^T \times \boldsymbol{M}^T$ be replaced by their images under a bijection α from $\mathbb{Z}_n \times \mathbb{Z}_m$ to $\mathbb{Z}_{nm}$, and let $i = \alpha((i_1, i_2))$ and $j = \alpha((j_1, j_2))$ for any $i, j \in \mathbb{Z}_{nm}$. Then

$$\begin{aligned} \boldsymbol{L}^T \times \boldsymbol{M}^T(i,j) &= (\boldsymbol{L}^T(i_1, j_1), \boldsymbol{M}^T(i_2, j_2)) \\ &= (\boldsymbol{L}(j_1, i_1), \boldsymbol{M}(j_2, i_2)) \\ &= \boldsymbol{L} \times \boldsymbol{M}(j, i) = (\boldsymbol{L} \times \boldsymbol{M})^T(i,j) \end{aligned}$$

for any $i, j \in \mathbb{Z}_{nm}$. ■

A product of quasigroups and Latin squares similar to the direct product was proposed by Sade [127], and the definition of this product and a proof that the product delivers a quasigroup is given by the following theorem.

Theorem 2.4.2 (Theorem 12.1.2, [41]) *Let $(Q, \circ)$ be a quasigroup of order n with a sub-quasigroup $(S, \circ)$ of order $m < n$, let $(Q \backslash S, \bullet)$ be a quasigroup of order $\ell = n - m$ and let $(R, \star)$ be an idempotent quasigroup of order k. Then the* singular direct product $(Q \cup ((Q\backslash S) \times R), *)$, *defined by*

$$a * b = \begin{cases} a \circ b, & \textit{if } a, b \in S, \\ (a \circ b_1, b_2), & \textit{if } a \in S \textit{ and } b = (b_1, b_2) \in ((Q\backslash S) \times R), \\ (a_1 \circ b, a_2), & \textit{if } b \in S \textit{ and } a = (a_1, a_2) \in ((Q\backslash S) \times R), \\ (a_1 \bullet b_1, a_2 \star b_2), & \textit{if } a = (a_1, a_2), b = (b_1, b_2) \in ((Q\backslash S) \times R) \textit{ and } a_2 \neq b_2, \\ (a_1 \circ b_1, c), & \textit{if } a = (a_1, c), b = (b_1, c) \in ((Q\backslash S) \times R) \textit{ and } a_1 \circ b_1 \in (Q\backslash S), \\ a_1 \circ b_1, & \textit{if } a = (a_1, c), b = (b_1, c) \in ((Q\backslash S) \times R) \textit{ and } a_1 \circ b_1 \in S, \end{cases}$$

is also a quasigroup.

The proof of this theorem is not difficult, but requires verification of the quasigroup property for a large number of cases, and it is therefore omitted here. The fact that the singular direct product delivers a quasigroup will be made clear, however, by means of an example. A proof of the theorem may be found in Dénes and Keedwell [41, Theorem 12.1.2].

The *singular direct product* of a Latin square $\boldsymbol{L}$ of order n which contains a subsquare $\boldsymbol{S}$ of order m, a Latin square $\boldsymbol{M}$ of order $\ell = n - m$ and an idempotent Latin square $\boldsymbol{N}$ of order k, denoted by $\boldsymbol{L} \otimes (\boldsymbol{M} \times \boldsymbol{N})$, is defined as the Latin square representing the Cayley table of the singular direct product of their underlying quasigroups.

Consider, for example, the Latin square

$$\boldsymbol{L}_{2.14} = \left[\begin{array}{ccc|cccc} 5 & 6 & 4 & 1 & 2 & 0 & 3 \\ 6 & 4 & 5 & 2 & 1 & 3 & 0 \\ 4 & 5 & 6 & 3 & 0 & 2 & 1 \\ \hline 3 & 1 & 2 & 0 & 5 & 6 & 4 \\ 1 & 3 & 0 & 4 & 6 & 5 & 2 \\ 0 & 2 & 1 & 5 & 3 & 4 & 6 \\ 2 & 0 & 3 & 6 & 4 & 1 & 5 \end{array}\right],$$

which contains the Latin square

$$\boldsymbol{L}_{2.15} = \begin{bmatrix} 5 & 6 & 4 \\ 6 & 4 & 5 \\ 4 & 5 & 6 \end{bmatrix}$$

as a subsquare in its upper right-hand corner. Furthermore, let

$$\boldsymbol{L}_{2.16} = \begin{bmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{2.17} = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

The structure of the Latin square $\boldsymbol{L}_{2.14} \otimes (\boldsymbol{L}_{2.16} \times \boldsymbol{L}_{2.17})$ is best explained by using the schematic representation in Figure 2.1 of this Latin square, where each of the labelled regions denotes a part of the Latin square. In Figure 2.1 Region A contains $\boldsymbol{L}_{2.15}$, which corresponds to the first case (where $a, b \in S$) in Theorem 2.4.2. Region B_i for $i = 0, 1, 2$ contains the array

$$\begin{array}{cccc}
(1,i) & (2,i) & (0,i) & (3,i) \\
(2,i) & (1,i) & (3,i) & (0,i) \\
(3,i) & (0,i) & (2,i) & (1,i)\,,
\end{array}$$

where the first elements of these ordered pairs give the upper right-hand part of $\boldsymbol{L}_{2.14}$. This corresponds to the second case in Theorem 2.4.2. Similarly, Region C_i for $i = 0, 1, 2$ contains the array

$$\begin{array}{ccc}
(3,i) & (1,i) & (2,i) \\
(1,i) & (3,i) & (0,i) \\
(0,i) & (2,i) & (1,i) \\
(2,i) & (0,i) & (3,i)\,,
\end{array}$$

where the first elements of these ordered pairs give the lower left-hand part of $\boldsymbol{L}_{2.14}$. This corresponds to the third case in Theorem 2.4.2. Region E_i for $i = 0, 1, 2$ contains the array

$$\begin{array}{cccc}
(0,i) & (3,i) & (1,i) & (2,i) \\
(1,i) & (2,i) & (0,i) & (3,i) \\
(2,i) & (1,i) & (3,i) & (0,i) \\
(3,i) & (0,i) & (1,i) & (2,i)\,,
\end{array}$$

where the first elements of these ordered pairs give $\boldsymbol{L}_{2.16}$. It may be noted that these arrays form part of the direct product $\boldsymbol{L}_{2.16} \times \boldsymbol{L}_{2.17}$. These regions correspond to the fourth case in Theorem 2.4.2. Finally, Region D_i for $i = 0, 1, 2$ contains the array

$$\begin{array}{cccc}
(0,i) & 5 & 6 & 4 \\
4 & 6 & 5 & (2,i) \\
5 & (3,i) & 4 & 6 \\
6 & 4 & (1,i) & 5\,,
\end{array}$$

where the elements (if pairs occur, the first elements) give the lower right-hand corner of $\boldsymbol{L}_{2.14}$. This corresponds to the final two cases in Theorem 2.4.2.

A	B_0	B_1	B_2
C_0	D_0	E_2	E_1
C_1	E_2	D_1	E_0
C_2	E_1	E_0	D_2

FIGURE 2.1: *A schematic representation of the layout of the singular direct product* $\boldsymbol{L}_{2.14} \otimes (\boldsymbol{L}_{2.16} \times \boldsymbol{L}_{2.17})$.

The Latin square $\boldsymbol{L}_{2.14} \otimes (\boldsymbol{L}_{2.16} \times \boldsymbol{L}_{2.17})$ is given by

$$\left[\begin{array}{ccccccccccccccc}
5 & 6 & 4 & (1,0) & (2,0) & (0,0) & (3,0) & (1,1) & (2,1) & (0,1) & (3,1) & (1,2) & (2,2) & (0,2) & (3,2) \\
6 & 4 & 5 & (2,0) & (1,0) & (3,0) & (0,0) & (2,1) & (1,1) & (3,1) & (0,1) & (2,2) & (1,2) & (3,2) & (0,2) \\
4 & 5 & 6 & (3,0) & (0,0) & (2,0) & (1,0) & (3,1) & (0,1) & (2,1) & (1,1) & (3,2) & (0,2) & (2,2) & (1,2) \\
(3,0) & (1,0) & (2,0) & (0,0) & 5 & 6 & 4 & (0,2) & (3,2) & (1,2) & (2,2) & (0,1) & (3,1) & (1,1) & (2,1) \\
(1,0) & (3,0) & (0,0) & 4 & 6 & 5 & (2,0) & (1,2) & (2,2) & (0,2) & (3,2) & (1,1) & (2,1) & (0,1) & (3,1) \\
(0,0) & (2,0) & (1,0) & 5 & (3,0) & 4 & 6 & (2,2) & (1,2) & (3,2) & (0,2) & (2,1) & (1,1) & (3,1) & (0,1) \\
(2,0) & (0,0) & (3,0) & 6 & 4 & (1,0) & 5 & (3,2) & (0,2) & (2,2) & (1,2) & (3,1) & (0,1) & (2,1) & (1,1) \\
(3,1) & (1,1) & (2,1) & (0,2) & (3,2) & (1,2) & (2,2) & (0,1) & 5 & 6 & 4 & (0,0) & (3,0) & (1,0) & (2,0) \\
(1,1) & (3,1) & (0,1) & (1,2) & (2,2) & (0,2) & (3,2) & 4 & 6 & 5 & (2,1) & (1,0) & (2,0) & (0,0) & (3,0) \\
(0,1) & (2,1) & (1,1) & (2,2) & (1,2) & (3,2) & (0,2) & 5 & (3,1) & 4 & 6 & (2,0) & (1,0) & (3,0) & (0,0) \\
(2,1) & (0,1) & (3,1) & (3,2) & (0,2) & (2,2) & (1,2) & 6 & 4 & (1,1) & 5 & (3,0) & (0,0) & (2,0) & (1,0) \\
(3,2) & (1,2) & (2,2) & (0,1) & (3,1) & (1,1) & (2,1) & (0,0) & (3,0) & (1,0) & (2,0) & (0,2) & 5 & 6 & 4 \\
(1,2) & (3,2) & (0,2) & (1,1) & (2,1) & (0,1) & (3,1) & (1,0) & (2,0) & (0,0) & (3,0) & 4 & 6 & 5 & (2,2) \\
(0,2) & (2,2) & (1,2) & (2,1) & (1,1) & (3,1) & (0,1) & (2,0) & (1,0) & (3,0) & (0,0) & 5 & (3,2) & 4 & 6 \\
(2,2) & (0,2) & (3,2) & (3,1) & (0,1) & (2,1) & (1,1) & (3,0) & (0,0) & (2,0) & (1,0) & 6 & 4 & (1,2) & 5
\end{array}\right].$$

Lindner [90] suggested a generalisation of this product, namely the *generalised singular direct product*, where (using the notation of Theorem 2.4.2) $|R|^2 - |R|$ quasigroups $(Q\backslash S, \bullet_{a,b})$ for each $(a,b) \in R^2\backslash\{(r,r) \mid r \in R\}$ are required instead of simply the quasigroup $(Q\backslash S, \bullet)$, and where $a * b = (a_1 \bullet_{a_2,b_2} b_1, a_2 \star b_2)$ if $a = (a_1, a_2), b = (b_1, b_2) \in ((Q\backslash S) \times R)$ and $a_2 \neq b_2$. In the example above, for instance, the generalised singular direct product states that the $3^2 - 3 = 6$ regions denoted by E_i for $i = 0, 1, 2$ in Figure 2.1 may be populated using any six distinct Latin squares of order 4, instead of six copies of the Latin square $\boldsymbol{L}_{2.16}$.

A well-known application of recursive constructions of Latin squares was given by MacNeish [94], and it uses the direct product of Latin squares in order to construct MOLS of larger order from MOLS of smaller order. The following theorem forms the basis of the construction.

Theorem 2.4.3 (Theorem 12.1.1, [41]) *If $(\boldsymbol{L}_1, \boldsymbol{L}_2, \ldots, \boldsymbol{L}_k)$ and $(\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_k)$ are k-MOLS of order n and m respectively, then $(\boldsymbol{L}_1 \times \boldsymbol{M}_1, \boldsymbol{L}_2 \times \boldsymbol{M}_2, \ldots, \boldsymbol{L}_k \times \boldsymbol{M}_k)$ is a k-MOLS of order nm.*

Proof: Replace the elements of $\boldsymbol{L}_t \times \boldsymbol{M}_t$ and $\boldsymbol{L}_s \times \boldsymbol{M}_s$ for any $t, s \in \{1, 2, \ldots, k\}$ by their images under a bijection α from $\mathbb{Z}_n \times \mathbb{Z}_m$ to $\mathbb{Z}_{nm}$, and let

$$(\boldsymbol{L}_t \times \boldsymbol{M}_t(i,j), \boldsymbol{L}_s \times \boldsymbol{M}_s(i,j)) = (\boldsymbol{L}_t \times \boldsymbol{M}_t(k,\ell), \boldsymbol{L}_s \times \boldsymbol{M}_s(k,\ell)),$$

for some $i, j, k, \ell \in \mathbb{Z}_{nm}$. If $i = \alpha((i_1, i_2))$, $j = \alpha((j_1, j_2))$, $k = \alpha((k_1, k_2))$ and $\ell = \alpha((\ell_1, \ell_2))$, then

$$\begin{aligned}
(\boldsymbol{L}_t(i_1, j_1), \boldsymbol{M}_t(i_2, j_2)) &= \boldsymbol{L}_t \times \boldsymbol{M}_t(i,j) \\
&= \boldsymbol{L}_t \times \boldsymbol{M}_t(k,\ell) \\
&= (\boldsymbol{L}_t(k_1, \ell_1), \boldsymbol{M}_t(k_2, \ell_2)),
\end{aligned}$$

and $\boldsymbol{L}_t(i_1, j_1) = \boldsymbol{L}_t(k_1, \ell_1)$, while $\boldsymbol{M}_t(i_2, j_2) = \boldsymbol{M}_t(k_2, \ell_2)$. Similarly, it may be shown that $\boldsymbol{L}_s(i_1, j_1) = \boldsymbol{L}_s(k_1, \ell_1)$ and $\boldsymbol{M}_s(i_2, j_2) = \boldsymbol{M}_s(k_2, \ell_2)$. By the orthogonality between $\boldsymbol{L}_t$ and $\boldsymbol{L}_s$ it follows that $i_1 = k_1$ and $j_1 = \ell_1$, and by the orthogonality between $\boldsymbol{M}_t$ and $\boldsymbol{M}_s$ it follows that $i_2 = k_2$ and $j_2 = \ell_2$. Hence $i = k$ and $j = \ell$, and so $\boldsymbol{L}_t \times \boldsymbol{M}_t$ and $\boldsymbol{L}_s \times \boldsymbol{M}_s$ are by definition orthogonal for any $t, s \in \{1, 2, \ldots, k\}$. ■

The next corollary follows naturally from Theorems 2.2.2 and 2.4.3.

Corollary 2.4.1 *If* $n = \prod_{i=1}^{q} p_i^{r_i}$ *is the unique factorisation of* $n \in \mathbb{N}$ *into powers of distinct primes where* $r_1, \ldots, r_q > 0$*, then there exists a* k*-MOLS of order* n *where* $k = \min\{p_i^{r_i} \mid 1 \leq i \leq q\} - 1$.

MacNeish [94] conjectured that for any $n = \prod_{i=1}^{q} p_i^{r_i}$ the largest set of MOLS of order n is one containing $\min\{p_i^{r_i} \mid 1 \leq i \leq q\} - 1$ Latin squares, which is indeed the case if $n = p^r$ for p prime and $r \in \mathbb{N}$. His conjecture was, however, disproven by Parker [114] who showed that a 4-MOLS of order $21 = 3^1 7^1$ exists, while MacNeish's conjecture states that a MOLS of order 21 can only contain $\min\{3^1, 7^1\} - 1 = 2$ Latin squares.

The next theorem states that the singular direct product may also be used to construct orthogonal Latin squares recursively.

Theorem 2.4.4 *If* $\boldsymbol{L}_1$ *and* $\boldsymbol{L}_2$ *are orthogonal Latin squares of order* n *which contain the orthogonal subsquares* $\boldsymbol{S}_1$ *and* $\boldsymbol{S}_2$ *of order* m *respectively, and if* $\boldsymbol{M}_1$ *and* $\boldsymbol{M}_2$ *are orthogonal Latin squares of order* $n - m$ *while* $\boldsymbol{N}_1$ *and* $\boldsymbol{N}_2$ *are orthogonal idempotent Latin squares of order* k*, then the singular direct products* $\boldsymbol{L}_1 \otimes (\boldsymbol{M}_1 \times \boldsymbol{N}_1)$ *and* $\boldsymbol{L}_2 \otimes (\boldsymbol{M}_2 \times \boldsymbol{N}_2)$ *are orthogonal.*

The proof of this theorem is lengthy in that it requires the verification of the orthogonality property for a large number of cases, and it is therefore omitted here. The proof may, however, be found in [41, Theorem 12.1.3]. The next corollary, originally due to Sade [127], follows naturally from Lemma 2.3.1 and Theorem 2.4.4.

Corollary 2.4.2 (Theorem 12.1.4, [41]) *If each Latin square in an* r*-MOLS of order* n *contains a subsquare of order* m *such that these* r *subsquares form an* r*-MOLS of order* m*, and if there exists an* s*-MOLS of order* $\ell = n - m$ *and a* t*-MOLS of order* k*, then there exists a* $\min(r, s, t-1)$*-MOLS of order* $m + \ell k$.

2.5 Chapter summary

In this chapter the basic theory behind Latin squares was introduced, and definitions and constructions were reviewed that will be utilised in the remainder of the dissertation. The definition of a Latin square, as well as of special types of Latin squares, such as reduced and idempotent Latin squares, was given in §2.1. This section also contains a description of the notions of transversals and universals, both of which play an important role in the enumeration of special types of orthogonal Latin squares as will be demonstrated later in this dissertation. The connection between Latin squares and quasigroups was also highlighted in this section.

In §2.2 the important notion of orthogonality between Latin squares was discussed, a notion which Euler had in mind when he gave the very first constructions of Latin squares. This section also contains the definition of an ordered set of mutually orthogonal Latin squares (MOLS), and an upper bound on the cardinality of such a set is given. The usefulness of Galois fields in the construction of orthogonal Latin squares was illustrated by a construction of a set of MOLS that attains the upper bound.

The classification of Latin squares according to similarities in structure may be achieved by using various operations that transform a Latin square into other Latin squares, as described in §2.3. In particular, it was noted that permutations may be used to rearrange the rows or columns or rename the symbols of a Latin square or a set of orthogonal Latin squares without destroying the defining property of the Latin square, while the roles of rows, columns and symbols are interchangeable. This leads to the important notion of group actions on the set of all Latin squares of a certain order, and some interesting connections between these operations and group theory were also highlighted.

A number of recursive constructions of Latin squares were reviewed in §2.4. Three such constructions were described, namely the method of prolongation, the direct product of Latin squares and the singular direct product of Latin squares. These construction methods have been used to settle some of the most important existence questions in the theory of orthogonal Latin squares, as will be explained in the next chapter, and it was shown in this section how these methods may be used to extend a set of MOLS to a set containing larger MOLS.

CHAPTER 3

Applications of Latin squares to sports tournament scheduling

Contents

In this chapter the use of Latin squares in the scheduling of sports tournaments is illustrated using two important practical examples. In §3.1 a brief review is given of the application of Latin squares to sports tournament scheduling, followed in §3.2 and §3.3 by two applications of specifically sets of two and three orthogonal Latin squares to mixed doubles sports tournament scheduling. In §3.2.1 a tournament called a *mixed doubles table tennis tournament* is considered, and it is shown how such a tournament may be scheduled using a set of three mutually orthogonal Latin squares. A review of past attempts by researchers to construct sets of two and three mutually orthogonal Latin squares is thereafter presented in §3.2.2. In §3.3.1 a similar tournament is considered, namely a *spouse-avoiding mixed doubles round-robin tennis tournament*, and it is shown that such a tournament is equivalent to a special kind of set of three mutually orthogonal Latin squares. Previous attempts at constructing these sets are reviewed in §3.3.2.

3.1 Scheduling sports tournaments using Latin squares

Latin squares have been applied successfully to the problem of scheduling various types of sports tournaments for which a strict requirement is that the tournament should be balanced and fair with respect to the players or teams involved. The reason for this is that the defining property of a Latin square asks for a balanced arrangement of the elements of $\mathbb{Z}_n$; the design of a Latin square may be seen as "fair" in the sense that each element of $\mathbb{Z}_n$ has the opportunity to appear in each row and column exactly once. Similarly, orthogonal Latin squares give rise to designs in which each element of $\mathbb{Z}_n^2$ has the opportunity of appearing exactly once in the superimposition of two Latin squares. In this chapter it is explained how these properties of Latin squares lead to interesting applications in sports tournament design, and they enable the scheduler of a sports tournament to construct schedules which may be extremely difficult to achieve by intuition.

The simplest and most common example of a balanced and fair sports tournament is a so-called *round-robin tournament of order* $2n$, in which $2n$ players[1] (for some $n \in \mathbb{N}$) take part in a tournament consisting of $2n - 1$ rounds, each of which consists of n matches. Each match consists of two players opposing one another, and the tournament has the property that each player opposes each other player exactly once, and that each player plays in exactly one match per round. An example of a schedule for a round-robin tournament of order 6 is given in Table 3.1, where the elements of the set $\mathbb{Z}_6$ are used to represent the names of the players.

Round 1	Round 2	Round 3	Round 4	Round 5
0 vs 1	0 vs 2	0 vs 3	0 vs 4	0 vs 5
2 vs 5	1 vs 3	1 vs 5	1 vs 2	1 vs 4
3 vs 4	4 vs 5	2 vs 4	3 vs 5	2 vs 3

Table 3.1: *A schedule for a round-robin tournament of order 6, where the names of the six players are represented by the set* $\mathbb{Z}_6$.

A round-robin tournament of order $2n - 1$, for some $n \in \mathbb{N}$, is equivalent to a round-robin tournament of order $2n$. Since in each round of a tournament of odd order some player has to sit out (*i.e.* receive a bye), a schedule for an even number of players may be used, where opposing some fixed player is equivalent to receiving a bye. For example, a round-robin tournament in which five players take part is also given by Table 3.1, where $\mathbb{Z}_6 \backslash \{0\}$ may be used, for example, to represent the names of the players and where a player receives a bye if he/she is scheduled to oppose 0.

It may be noted that a round-robin tournament for $2n$ players is equivalent to a 1-factorisation of the complete graph K_{2n}, in which the vertices labelled by the elements of $\mathbb{Z}_n$ model the players, where each factor represents a round of the tournament, and where each edge corresponds to a match between two players. For example, Figure 3.1 shows the corresponding 1-factorisation for the round-robin tournament in Table 3.1.

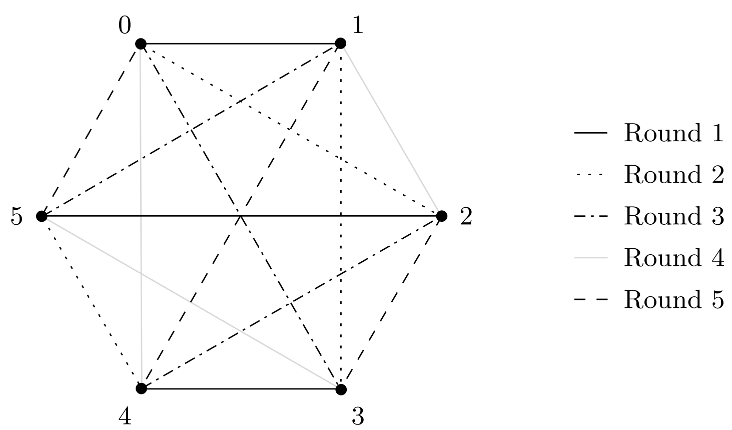

Figure 3.1: *A 1-factorisation of* K_6 *corresponding to the round-robin tournament in Table 3.1.*

[1] Participants of a round-robin tournament may in general also be referred to as *teams*.

More importantly, however, a round-robin tournament may be represented by a special type of Latin square. Let $\{F_1, F_2, \ldots, F_{2n-1}\}$ be a 1-factorisation of K_{2n}, and let $\boldsymbol{L}$ be a $2n \times 2n$ array such that $\boldsymbol{L}(i,j) = \boldsymbol{L}(j,i) = k$ for each $\{i,j\} \in F_k$ where $1 \leq k \leq 2n-1$, and such that $\boldsymbol{L}(i,i) = 0$ for $0 \leq i \leq 2n-1$. Then $\boldsymbol{L}$ is symmetric and unipotent, and since the 1-factors are all pairwise disjoint, each entry in $\boldsymbol{L}$ contains exactly one symbol. Furthermore, if $\boldsymbol{L}(i,j) = \boldsymbol{L}(i,j') = k$, then $\{i,j\}$ and $\{i,j'\}$ are both in F_k, contradicting the fact that F_k forms part of a partition of $\mathbb{Z}_n$. Each element of $\mathbb{Z}_n$ therefore appears exactly once in each row of $\boldsymbol{L}$, and a similar argument shows that each element also appears exactly once in each column of $\boldsymbol{L}$. Hence $\boldsymbol{L}$ is a symmetric unipotent Latin square. It may similarly also be shown that a symmetric unipotent Latin square of order $2n$ may be used to obtain a 1-factorisation of K_{2n}, and therefore that the two designs are equivalent. For example, the round-robin tournament in Table 3.1 may also be represented by the symmetric Latin square

$$\boldsymbol{L}_{3.1} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 4 & 2 & 5 & 3 \\ 2 & 4 & 0 & 5 & 3 & 1 \\ 3 & 2 & 5 & 0 & 1 & 4 \\ 4 & 5 & 3 & 1 & 0 & 2 \\ 5 & 3 & 1 & 4 & 2 & 0 \end{bmatrix},$$

where the entry in row i and column j gives the round in which i opposes j. Such a table must be a Latin square in order to ensure that each player plays exactly once in each round, while it must be symmetric in order to ensure that each player opposes each other player exactly once. Furthermore, the diagonal of this Latin square may be ignored as it corresponds to a round where players oppose themselves.

It may also be noted that a symmetric unipotent Latin square of order $2n$ is equivalent to a symmetric idempotent Latin square of order $2n-1$, which is an especially useful representation if there are an odd number of players participating in a round-robin tournament. A symmetric idempotent Latin square may obtained from a symmetric unipotent Latin square $\boldsymbol{L}$ by reversing the process of prolongation discussed in §2.4, where the last $2n-1$ entries of the first row and first column of $\boldsymbol{L}$ may be projected back to the diagonal (which is a universal in $\boldsymbol{L}$). For instance, the symmetric idempotent Latin square obtained in this way from $\boldsymbol{L}_{3.1}$ is

$$\boldsymbol{L}_{3.2} = \begin{bmatrix} 1 & 4 & 2 & 5 & 3 \\ 4 & 2 & 5 & 3 & 1 \\ 2 & 5 & 3 & 1 & 4 \\ 5 & 3 & 1 & 4 & 2 \\ 3 & 1 & 4 & 2 & 5 \end{bmatrix}.$$

As will be shown in the following sections, special types of round-robin tournaments may be scheduled by utilising Latin squares which are orthogonal to symmetric Latin squares. In such applications it is therefore more beneficial to consider a round-robin tournament in the form of a Latin square than in the form of a 1-factorisation.

Another benefit of considering the Latin square representation of round-robin tournaments arises from a very interesting problem in round-robin tournament scheduling, namely the problem of balancing so-called *carry-over effects* in round-robin tournaments. Let $\boldsymbol{L}$ be a symmetric unipotent Latin square representing a round-robin tournament schedule. A player $i \in \mathbb{Z}_n$ is said to receive a *carry-over effect* from player $j \in \mathbb{Z}_n$ if $\boldsymbol{L}(\ell,j) = k$ and $\boldsymbol{L}(\ell,i) = k+1$. The assumption is made in this case that the performance of player ℓ has been affected by the match between ℓ and j in round k, and that this effect is "carried over" to the next round. For example, if j is an extremely strong player, then ℓ might be both physically and psychologically exhausted after opposing j, and i might benefit from this since he/she is opposing a tired player in the next round.

The advantage of considering the Latin square representation of a round-robin tournament in this case is that, since $\boldsymbol{L}(\ell, j) = k$ and $\boldsymbol{L}(\ell, i) = k + 1$, it follows that $\boldsymbol{L}^{-1}(\ell, k) = j$ and $\boldsymbol{L}^{-1}(\ell, k + 1) = i$, and the carry-over effects are therefore given by consecutive elements in the rows of $\boldsymbol{L}^{-1}$. For example,

$$\boldsymbol{L}_{3.1}^{-1} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 5 & 2 & 4 \\ 2 & 5 & 0 & 4 & 1 & 3 \\ 3 & 4 & 1 & 0 & 5 & 2 \\ 4 & 3 & 5 & 2 & 0 & 1 \\ 5 & 2 & 4 & 1 & 3 & 0 \end{bmatrix},$$

and from the consecutive pairs $\boldsymbol{L}_{3.1}^{-1}(1, 1) = 0$ and $\boldsymbol{L}_{3.1}^{-1}(1, 2) = 3$ in row 1, it may be seen that 0 gives a carry-over effect to 3. Hence this representation using a Latin square provides a much easier way of observing the various carry-over effects throughout the tournament, whereas it is difficult to see the carry-over effects when considering the corresponding 1-factorisation representation of a round-robin tournament. Furthermore, the problem under consideration is to balance the carry-over effects, *i.e.* to find a round-robin schedule where each player receives a carry-over effect from each other player at most once. Hence a symmetric unipotent Latin square $\boldsymbol{L}$ may be used, where $\boldsymbol{L}^{-1}$ has the property that each element of $\mathbb{Z}_n^2 \backslash \{(a, a) \mid a \in \mathbb{Z}_n\}$ appears at most once as consecutive elements in its rows[2].

For more detail on the problem of balancing the carry-over effects of a round-robin tournament, see, for instance, Anderson [7], Keedwell [80], Kidd [83] and Russel [125], all of which contain references to a number of other authors who have also considered the problem. Keedwell [80], in particular, not only considers the application of Latin squares to the problem of balancing carry-over effects, but also to a number of other special types of tournaments, such as tennis on unequal courts, home and away football, mixed doubles tennis tournaments and bridge tournaments.

An application of orthogonal Latin squares to the scheduling of a special type of golf tournament is considered (among others) by Robinson [122] and Wallis [140]. The tournament they consider consists of $2n + 1$ players taking part in $2n - 1$ round-robin tournaments, where each round-robin tournament is scheduled in such a way that the round in which a player receives a bye takes place on that player's home ground. Such a tournament is simple to schedule by means of $2n - 1$ symmetric idempotent Latin squares of order $2n + 1$, but an additional requirement that each pair of players oppose one another exactly once on each of the other $2n - 1$ players' home grounds is imposed, which requires that the $2n - 1$ symmetric idempotent Latin squares form a $(2n - 1)$-MOLS of order $2n + 1$. Such a set of MOLS is known as a *golf-design*, and a detailed review of the constructions and uses of these designs may be found in Dinitz *et al.* [45, §VI.51.7].

A large number of other applications of various combinatorial designs (including Latin squares) to the scheduling of sports tournaments are reviewed by Dinitz *et al.* [45]. Examples include the application of Latin squares to mixed doubles tennis tournaments [45, §51.11] and whist[3] tournaments [45, §51.9], where the former is of particular interest in this dissertation. Although whist tournaments have Latin square representations (see Bennet and Zhu [15]), they are usually

[2] Such a Latin square is known as a *row-complete Latin square* (see, for instance, Dénes and Keedwell [41, §2.3]).

[3] Whist is a so-called trick-taking playing card game similar to bridge [147].

considered in the guise of various other combinatorial designs, such as Mendelsohn designs and balanced incomplete block designs (see, for example, Anderson and Finizio [8]).

3.2 An application of sets of orthogonal Latin squares

In this section an application to mixed doubles sports tournament scheduling (which arises in tennis and table tennis tournaments) is presented, where a mixed doubles tournament refers to a tournament with the requirement that two teams consisting of two players each oppose one another in each match, and where a team consists of a man and a woman. Such a match will henceforth be given in the tabular form

$$\begin{array}{|c||c|}\hline M & M' \\ \hline W & W' \\ \hline\end{array},$$

where M and M' are men and W and W' women, and where $\{M, W\}$ forms the first team and $\{M', W'\}$ the second. In §3.2.1 it is shown how such a tournament for $4n$ players satisfying a number of additional properties is equivalent to a 3-MOLS of order n, and a number of constructions of such designs are also presented.

3.2.1 Mixed doubles table tennis (MDTT) tournaments

In 1975 Pulleyblank [119] considered a special type of mixed doubles tournament in which two opposing teams participate, each of which consists of n men and n women for some $n \in \mathbb{N}$. The requirement to be satisfied by the tournament is similar to the requirement for a round-robin tournament, namely that each player opposes each player from the opposite team exactly once. However, it is also required that each man is in partnership with each woman from the same team exactly once. Hence there are $4n$ players in total, each of whom participates in a total of n matches throughout the tournament. The matches of the tournament may also be partitioned into a number of rounds in such a way that each player participates in exactly one match per round, and the tournament can therefore not consist of fewer than n rounds. Pulleyblank simply referred to such a tournament for $4n$ players as a *mixed doubles table tennis (MDTT) tournament of order* n, due to the fact that such a tournament was scheduled for table tennis by a local social club. Furthermore, an MDTT tournament of order n is *resolvable* if it can be scheduled into n rounds, each consisting of n matches.

Consider, for example, a team consisting of four men, denoted by M_0, M_1, M_2 and M_3, and four women, denoted by W_0, W_1, W_2 and W_3, opposing another team consisting of four men, denoted by M'_0, M'_1, M'_2 and M'_3, and four women, denoted by W'_0, W'_1, W'_2 and W'_3. A schedule for a resolvable MDTT tournament consisting of four rounds is given in Table 3.2.

It may be noted that an MDTT tournament of order n is equivalent to an orthogonal array (see §2.2). If the entry in row i and column j of an $OA(4, n)$ $\boldsymbol{A}$ is denoted by $\boldsymbol{A}(i, j)$ for all $i \in \mathbb{Z}_4$ and $j \in \mathbb{Z}_{n^2}$, then it is easy to see that the matches

$$\begin{array}{|c||c|}\hline \boldsymbol{A}(0,i) & \boldsymbol{A}(1,i) \\ \hline \boldsymbol{A}(2,i) & \boldsymbol{A}(3,i) \\ \hline\end{array}, \quad i \in \mathbb{Z}_{n^2}$$

Round 0		Round 1		Round 2		Round 3	
M_0	M_0'	M_0	M_1'	M_0	M_2'	M_0	M_3'
W_0	W_0'	W_1	W_1'	W_2	W_2'	W_3	W_3'
M_1	M_3'	M_1	M_2'	M_1	M_1'	M_1	M_0'
W_2	W_1'	W_3	W_0'	W_0	W_3'	W_1	W_2'
M_2	M_1'	M_2	M_0'	M_2	M_3'	M_2	M_2'
W_3	W_2'	W_2	W_3'	W_1	W_0'	W_0	W_1'
M_3	M_2'	M_3	M_3'	M_3	M_0'	M_3	M_1'
W_1	W_3'	W_0	W_2'	W_3	W_1'	W_2	W_0'

TABLE 3.2: *A schedule for an MDTT tournament of order 4.*

satisfy all the requirements of an MDTT tournament. For instance, the orthogonal array

$$\boldsymbol{A}_{3.1} = \begin{bmatrix} 0&0&0&0&1&1&1&1&2&2&2&2&3&3&3&3 \\ 0&1&2&3&3&2&1&0&1&0&3&2&2&3&0&1 \\ 0&1&2&3&2&3&0&1&3&2&1&0&1&0&3&2 \\ 0&1&2&3&1&0&3&2&2&3&0&1&3&2&1&0 \end{bmatrix}$$

gives the MDTT in Table 3.2 under four bijections α_0, α_1, α_2 and α_3, where α_i is applied to the elements of row i of $\boldsymbol{A}_{3.1}$, and where $\alpha_0(i) = M_i$, $\alpha_1(i) = M_i'$, $\alpha_2(i) = W_i$ and $\alpha_3(i) = W_i'$.

Hence an MDTT tournament of order n in which a team of n men, denoted by $M_0, M_1, \ldots, M_{n-1}$, and n women, denoted by $W_0, W_1, \ldots, W_{n-1}$, oppose another team of n men, denoted by $M_0', M_1', \ldots, M_{n-1}'$, and n women, denoted by $W_0', W_1', \ldots, W_{n-1}'$, is equivalent to two orthogonal Latin squares $\boldsymbol{L}$ and $\boldsymbol{M}$ where $\boldsymbol{L}(M_i, M_j') = W_k$ and $\boldsymbol{M}(M_i, M_j') = W_k'$ for each match of the form

$$\begin{array}{|c||c|} \hline M_i & M_j' \\ \hline W_k & W_\ell' \\ \hline \end{array}.$$

For example, the corresponding pair of orthogonal Latin squares for the MDTT tournament in Table 3.2 is given in Table 3.3.

	M_0'	M_1'	M_2'	M_3'
M_0	W_0	W_1	W_2	W_3
M_1	W_1	W_0	W_3	W_2
M_2	W_2	W_3	W_0	W_1
M_3	W_3	W_2	W_1	W_0

	M_0'	M_1'	M_2'	M_3'
M_0	W_0'	W_1'	W_2'	W_3'
M_1	W_2'	W_3'	W_0'	W_1'
M_2	W_3'	W_2'	W_1'	W_0'
M_3	W_1'	W_0'	W_3'	W_2'

TABLE 3.3: *The matches of the MDTT tournament of order 4 in Table 3.2, represented here by a pair of orthogonal Latin squares of order 4.*

It therefore follows that if a pair of orthogonal Latin squares of order n may be constructed, then an MDTT tournament schedule of order n may be obtained. However, a pair of orthogonal Latin squares do not provide any means of scheduling the tournament into n rounds, and for this purpose it follows that another Latin square is required which is orthogonal to the pair used to construct the matches.

Consider a resolvable MDTT tournament of order n, namely where the matches are partitioned into n rounds so that no player plays twice in any round. Let $\boldsymbol{L}$ and $\boldsymbol{M}$ be two orthogonal

Latin squares such that $\boldsymbol{L}(i,j) = k$ if M_i (using the same notation as above) is in partnership with W_k when opposing M'_j and $\boldsymbol{M}(i,j) = k$ if M'_j is in partnership with W'_k when opposing M_i, and let $\boldsymbol{N}$ be an $n \times n$ array such that $\boldsymbol{N}(i,j)$ gives the round in which M_i opposes M'_j for all $i, j \in \mathbb{Z}_n$. Since each player participates in exactly one match per round, the ordered pairs $(M_i, \boldsymbol{N}(i,j))$, *i.e.* the ordered pairs $(i, \boldsymbol{N}(i,j))$, are unique as i and j vary over $\mathbb{Z}_n$. For the same reason the ordered pairs $(j, \boldsymbol{N}(i,j))$, $(\boldsymbol{L}(i,j), \boldsymbol{N}(i,j))$ and $(\boldsymbol{M}(i,j), \boldsymbol{N}(i,j))$ are unique as i and j vary over $\mathbb{Z}_n$ (since the women $W_{\boldsymbol{L}(i,j)}$ and $W_{\boldsymbol{M}(i,j)}$ both play in round $\boldsymbol{N}(i,j)$). It therefore follows that $\boldsymbol{N}$ is a Latin square which is orthogonal to both $\boldsymbol{L}$ and $\boldsymbol{M}$.

It therefore follows that a resolvable MDTT tournament schedule for $4n$ players may be obtained by constructing a 3-MOLS of order n. For example, Table 3.4 shows the MDTT tournament given in Table 3.2 as represented by three mutually orthogonal Latin squares, the first two of which give the matches and the third of which gives the rounds of the MDTT tournament.

	M'_0	M'_1	M'_2	M'_3
M_0	W_0	W_1	W_2	W_3
M_1	W_1	W_0	W_3	W_2
M_2	W_2	W_3	W_0	W_1
M_3	W_3	W_2	W_1	W_0

	M'_0	M'_1	M'_2	M'_3
M_0	W'_0	W'_1	W'_2	W'_3
M_1	W'_2	W'_3	W'_0	W'_1
M_2	W'_3	W'_2	W'_1	W'_0
M_3	W'_1	W'_0	W'_3	W'_2

	M'_0	M'_1	M'_2	M'_3
M_0	0	1	2	3
M_1	3	2	1	0
M_2	1	0	3	2
M_3	2	3	0	1

TABLE 3.4: *The schedule of the resolvable MDTT tournament of order 4 in Table 3.2, represented here by a triple of orthogonal Latin squares of order 4.*

3.2.2 Constructions of pairs and triples of orthogonal Latin squares

It is easy to verify that a Latin square of order 2 cannot have an orthogonal mate, but the question of existence of Latin squares of orders larger than 2 admitting orthogonal mates is not trivial to resolve. The following theorem is, however, useful in the construction of pairs of orthogonal Latin squares.

Theorem 3.2.1 (Theorem 1.4.2, [41]) *If a Latin square of order n represents the Cayley-table of a group and exhibits at least one transversal, then it exhibits n disjoint transversals.*

Proof: Let $\boldsymbol{L}$ be the Cayley table of a group $(G, \circ)$ of order n, and let

$$\{(g_0, h_0), (g_1, h_1), \ldots, (g_{n-1}, h_{n-1})\}$$

be a transversal in $\boldsymbol{L}$ where $g_i, h_i \in G$. If $a \in G$, then the set of entries

$$\{(a \circ g_0, h_0), (a \circ g_1, h_1), \ldots, (a \circ g_{n-1}, h_{n-1})\}$$

also forms a transversal in $\boldsymbol{L}$. If it did not, then $a \circ g_i \circ h_i = a \circ g_j \circ h_j$ for some $i, j \in \mathbb{Z}_n$ would imply that $g_i \circ h_i = g_j \circ h_j$, contradicting the fact that

$$\{(g_0, h_0), (g_1, h_1), \ldots, (g_{n-1}, h_{n-1})\}$$

is a transversal. Furthermore, let $a, b \in G$ and $a \neq b$. Then the transversals

$$\{(a \circ g_0, h_0), (a \circ g_1, h_1), \ldots, (a \circ g_{n-1}, h_{n-1})\}$$

and

$$\{(b \circ g_0, h_0), (b \circ g_1, h_1), \ldots, (b \circ g_{n-1}, h_{n-1})\}$$

in $\boldsymbol{L}$ are disjoint, since $(a \circ g_i, h_i) = (b \circ g_i, h_i)$ for any $i \in \mathbb{Z}_n$ implies that $a = b$. Therefore, letting a vary over the elements of G, it follows that $\boldsymbol{L}$ has n disjoint transversals. ■

The *order* of an element a in a group $(G, \circ)$ is the smallest positive integer m such that a^m is the identity element of the group, and it is equal to the order of the subgroup generated by a. The following theorem provides a means of obtaining a pair of orthogonal Latin squares of any odd order.

Theorem 3.2.2 (Theorem 1.4.3, [41]) *The Cayley-table of a group of odd order exhibits a transversal.*

Proof: It is shown that the main diagonal of the Cayley-table of a group $(G, \circ)$ of odd order is a transversal. Assume that $a^2 = b^2$ for some $a, b \in G$. The element a^2 must have odd order, since otherwise it generates a subgroup of even order which contradicts Lagrange's theorem [67, Theorem 16.9] (since $(G, \circ)$ has odd order). Therefore, let $(a^2)^{2m-1} = e$ for some integer m (where e is the identity element of $(G, \circ)$). Then $a^{4m-2} = e$, and since a also has odd order, $a^{2m-1} = e$. Furthermore, since $a^2 = b^2$, it similarly follows that $b^{2m-1} = e$. Hence, $a = a^{2m} = b^{2m} = b$, and therefore no element repeats on the diagonal of the Cayley-table of $(G, \circ)$. ■

It follows by Theorems 3.2.1 and 3.2.2 and from the fact that a group exists for any odd order, that a pair of orthogonal Latin squares exists for any odd order, as summarised in the following corollary.

Corollary 3.2.1 *A pair of orthogonal Latin squares of order n exists for any odd $n \in \mathbb{N}$.*

For example, the Latin square

$$\boldsymbol{L}_{3.3} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

represents the Cayley-table of the group $(\mathbb{Z}_5, +)$, and the Latin square

$$\boldsymbol{L}_{3.4} = \begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{bmatrix}$$

is orthogonal to it by the construction given in Theorem 3.2.1. Euler [52] also gave a special case of this construction. He called a Latin square in which each row is a shift to the right of the row preceding it a *single-step Latin square*, and established a number of ways of obtaining a transversal in such a Latin square of odd order. Upon finding a transversal, Euler also noted that it could be used to obtain n disjoint transversals as described in Theorem 3.2.1.

In addition to a construction of pairs of orthogonal Latin squares of odd order, Euler also gave constructions for pairs of orthogonal Latin squares of order $4m$ for any $m \in \mathbb{N}$. He introduced a *two-step Latin square*, which is equivalent to a Latin square of order $2m$ obtained by taking the direct product of a Latin square square of order 2 and the Latin square representing the Cayley-table of the group $(\mathbb{Z}_m, +)$. Since a Latin square of order 2 represents the Cayley-table of the group $(\mathbb{Z}_2, +)$, a two-step Latin square represents the Cayley-table of the group $(\mathbb{Z}_2, +) \times (\mathbb{Z}_m, +)$. The following lemma provides a simple way of constructing such a Latin square, and is similar to the construction given by Euler [52].

Lemma 3.2.1 *The group $(\mathbb{Z}_{2m}, \circledast)$ where*

$$a \circledast b = \begin{cases} a + b - 2 \,(\text{mod } 2m), & \text{if both } a \text{ and } b \text{ are odd,} \\ a + b \,(\text{mod } 2m), & \text{otherwise,} \end{cases}$$

for $a, b \in \mathbb{Z}_{2m}$ is isomorphic to the group $(\mathbb{Z}_2 \times \mathbb{Z}_m, \oplus) = (\mathbb{Z}_2, +) \times (\mathbb{Z}_m, +)$.

Proof: Let α be a bijection from $\mathbb{Z}_{2m}$ to $\mathbb{Z}_2 \times \mathbb{Z}_m$ such that

$$\alpha(a) = \begin{cases} \left(0, \frac{a}{2}\right), & \text{if } a \text{ is even,} \\ \left(1, \frac{a-1}{2}\right), & \text{if } a \text{ is odd.} \end{cases}$$

Three cases are considered in what follows. Let $a, b \in \mathbb{Z}_{2m}$.

<u>*Case 1*</u>: Both a and b are even.

Then

$$\alpha(a) \oplus \alpha(b) = \left(0, \frac{a+b}{2}\right) = \alpha(a+b) = \alpha(a \circledast b).$$

<u>*Case 2*</u>: Only one of a or b is even.

Then

$$\alpha(a) \oplus \alpha(b) = \left(1, \frac{a+b-1}{2}\right) = \alpha(a+b) = \alpha(a \circledast b).$$

<u>*Case 3*</u>: Both a and b are odd.

Then

$$\alpha(a) \oplus \alpha(b) = \left(0, \frac{a+b-2}{2}\right) = \alpha(a+b-2) = \alpha(a \circledast b).$$

Hence $\alpha(a) \oplus \alpha(b) = \alpha(a \circledast b)$ for any $a, b \in \mathbb{Z}_{2m}$, and α is therefore an isomorphism from $(\mathbb{Z}_{2m}, \circledast)$ to $(\mathbb{Z}_2 \times \mathbb{Z}_m, \oplus)$. ■

Euler [52] also established a number of methods for obtaining a transversal in a two-step Latin square of order a multiple of 4. The following theorem illustrates one of these methods.

Theorem 3.2.3 *The Cayley-table of $(\mathbb{Z}_{4m}, \circledast)$ exhibits a transversal.*

Proof: A transversal may be obtained as follows. For all $i \in \{2, 4, 6, \ldots, 2m-2\}$ let $(i, i+2)$ form part of the transversal. Among these pairs the transversal intersects column j for all $j \in \{4, 6, 8, \ldots, 2m\}$ and contains the symbol $i \circledast (i+2) = 2i + 2$ for all i, which are all the elements in the set $\{6, 10, 14, \ldots, 4m-2\}$; in other words all distinct symbols which are odd multiples of two (since i is even), except 2.

For all $i \in \{1, 3, 5, \ldots, 2m-3\}$ let (i, i) form part of the transversal. Among these pairs the transversal intersects column j for all $j \in \{1, 3, 5, \ldots, 2m-3\}$ and contains the symbol $i \circledast i = 2i - 2$ for all i, which are all the elements in the set $\{0, 4, 8, \ldots, 4m-8\}$; in other words all distinct symbols which are even multiples of two (since i is odd), except $4m-4$.

For all $i \in \{2m, 2m+2, 2m+4, \ldots, 4m-2\}$ let $(i, i-1)$ form part of the transversal. Among these pairs the transversal intersects column j for all $j \in \{2m-1, 2m+1, 2m+3, \ldots, 4m-3\}$ and contains the symbol $i \circledast (i-1) = 2i - 1$ for all i, which are all the elements in the set $\{4m-1, 4m+3, 4m+7, \ldots, 8m-5\}$; in other words all distinct symbols which are one less than a multiple of four.

Finally, for all $i \in \{2m-1, 2m+1, 2m+3, \ldots, 4m-3\}$ let $(i, i+3)$ form part of the transversal. Among these pairs the transversal intersects column j for all $j \in \{2m+2, 2m+4, 2m+6, \ldots, 4m-2, 0\}$ and contains the symbol $i \circledast (i+3) = 2i+3$ for all i, which are all the elements in the set $\{4m+1, 4m+5, 4m+9, \ldots, 8m-3\}$; in other words all distinct symbols which are one more than a multiple of four.

Hence these four cases together provide a list of entries with the property that no row, column or symbol is repeated. Rows 0 and $4m-1$, columns 2 and $4m-1$, and symbols 2 and $4m-4$ are, however, not yet part of this list. Since $0 \circledast 2 = 2$ and $(4m-1) \circledast (4m-1) = 4m-4$, this list forms a transversal with the addition of $(0, 2)$ and $(4m-1, 4m-1)$ to it. ■

The next result provides a method for constructing a pair of orthogonal Latin squares of any order which is a multiple of four.

Corollary 3.2.2 *A pair of orthogonal Latin squares of order n exists if n is a multiple of four.*

Proof: By Theorems 3.2.1 and 3.2.3 it follows that the Cayley table of the group $(\mathbb{Z}_{4m}, \circledast)$ of order $4m$ exhibits $4m$ disjoint transversals. ■

For example, consider the Cayley-table of $(\mathbb{Z}_8, \circledast)$, which is represented by the Latin square

$$\boldsymbol{L}_{3.5} = \begin{bmatrix} 0 & 1 & \mathbf{2} & 3 & 4 & 5 & 6 & 7 \\ 1 & \mathbf{0} & 3 & 2 & 5 & 4 & 7 & 6 \\ 2 & 3 & 4 & 5 & \mathbf{6} & 7 & 0 & 1 \\ 3 & 2 & 5 & 4 & 7 & 6 & \mathbf{1} & 0 \\ 4 & 5 & 6 & \mathbf{7} & 0 & 1 & 2 & 3 \\ \mathbf{5} & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\ 6 & 7 & 0 & 1 & 2 & \mathbf{3} & 4 & 5 \\ 7 & 6 & 1 & 0 & 3 & 2 & 5 & \mathbf{4} \end{bmatrix}.$$

The transversal obtained by the method described in Theorem 3.2.3 is

$$\{(0,2), (1,1), (2,4), (3,6), (4,3), (5,0), (6,5), (7,7)\},$$

as shown in boldface in $\boldsymbol{L}_{3.5}$. Using the method described in Theorem 3.2.1, another transversal is

$$\{(1,2), (0,1), (3,4), (2,6), (5,3), (4,0), (7,5), (6,7)\},$$

which is obtained by replacing each pair (a, b) in the first transversal by $(1 \circledast a, b)$. It is interesting to note that if (a, b) and $(a+1, c)$ are consecutive pairs in the original transversal, and if a is even, then (a, b) is replaced by $(a+1, b)$ while $(a+1, c)$ is replaced by (a, c). The remaining six transversals may be found in the same manner, resulting in the Latin square

$$\boldsymbol{L}_{3.6} = \begin{bmatrix} 5 & 1 & 0 & 4 & 6 & 2 & 7 & 3 \\ 4 & 0 & 1 & 5 & 7 & 3 & 6 & 2 \\ 7 & 3 & 2 & 6 & 0 & 4 & 1 & 5 \\ 6 & 2 & 3 & 7 & 1 & 5 & 0 & 4 \\ 1 & 5 & 4 & 0 & 2 & 6 & 3 & 7 \\ 0 & 4 & 5 & 1 & 3 & 7 & 2 & 6 \\ 3 & 7 & 6 & 2 & 4 & 0 & 5 & 1 \\ 2 & 6 & 7 & 3 & 5 & 1 & 4 & 0 \end{bmatrix},$$

which is orthogonal to $\boldsymbol{L}_{3.5}$.

Corollaries 3.2.1 and 3.2.2 together state that a pair of orthogonal Latin squares of order n exists for any $n \neq 2 \pmod 4$. Although Euler found constructions for these orders, he could not find a pair of orthogonal Latin squares of order $n = 2 \pmod 4$, and conjectured[4] that they do not exist (as mentioned in §1.1).

A special case of the conjecture, namely that two orthogonal Latin squares of order 6 do not exist, was proven correct by Tarry [136] in 1900 via an exhaustive elimination of a large number of cases. Tarry found that there are 9 408 reduced Latin squares of order six, and he grouped these into 17 distinct classes such that if a Latin square has an orthogonal mate, then any Latin square in its class also has an orthogonal mate. It therefore sufficed to show that among 17 Latin squares, one taken from each class, there does not exist one with an orthogonal mate. This proof of the non-existence of orthogonal Latin squares of order 6 was verified by Fisher and Yates [57], who also counted 9 408 reduced Latin squares and 17 classes of Latin squares of order six. According to Norton [112] the same exhaustive enumeration proof was allegedly given even before 1900, but was left unpublished. Non-exhaustive proofs of this result were given by Yamamoto [152] and Stinson [133], while Appa *et al.* [10] used integer programming to show that no orthogonal Latin squares of order 6 exists.

Although Euler's conjecture was verified for the special case of $n = 6$, it was disproven for the special case of $n = 10$ in 1959 by Bose and Shrikhande [22] and Parker [115], who produced the pair

$$\left(\begin{bmatrix} 0 & 4 & 1 & 7 & 2 & 9 & 8 & 3 & 6 & 5 \\ 8 & 1 & 5 & 2 & 7 & 3 & 9 & 4 & 0 & 6 \\ 9 & 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 & 0 \\ 5 & 9 & 8 & 3 & 0 & 4 & 7 & 6 & 2 & 1 \\ 7 & 6 & 9 & 8 & 4 & 1 & 5 & 0 & 3 & 2 \\ 6 & 7 & 0 & 9 & 8 & 5 & 2 & 1 & 4 & 3 \\ 3 & 0 & 7 & 1 & 9 & 8 & 6 & 2 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 8 & 9 & 7 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & 9 & 7 & 8 \end{bmatrix}, \begin{bmatrix} 0 & 7 & 8 & 6 & 9 & 3 & 5 & 4 & 1 & 2 \\ 6 & 1 & 7 & 8 & 0 & 9 & 4 & 5 & 2 & 3 \\ 5 & 0 & 2 & 7 & 8 & 1 & 9 & 6 & 3 & 4 \\ 9 & 6 & 1 & 3 & 7 & 8 & 2 & 0 & 4 & 5 \\ 3 & 9 & 0 & 2 & 4 & 7 & 8 & 1 & 5 & 6 \\ 8 & 4 & 9 & 1 & 3 & 5 & 7 & 2 & 6 & 0 \\ 7 & 8 & 5 & 9 & 2 & 4 & 6 & 3 & 0 & 1 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 9 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 & 8 & 9 & 7 \end{bmatrix} \right)$$

or orthogonal Latin squares of order 10. Bose and Shrikhande used so-called *pairwise balanced block designs* and Parker Galois fields in order to obtain constructions for pairs of orthogonal Latin squares of an infinite number of orders (but not all orders) of the form $n = 2 \pmod 4$. These two construction methods were combined by the three authors, and a complete disproof of Euler's conjecture was soon after published in [23]. Their theorem is not reproduced in

[4]It may be noted that Euler's conjecture is a special case of the MacNeish conjecture. If $n = 2 \pmod 4$, then n is an odd multiple of 2 and n therefore must be of the form $2^1 \prod_{i=1}^{q} p_i^{r_i}$ where $p_i \neq 2$ is prime and $r_i \in \mathbb{N}$ for all $i = 1, \ldots, q$. The MacNeish conjecture states that a MOLS of order $n = 2 \pmod 4$ can only contain $\min\{2^1, p_1^{r_1}, p_2^{r_2}, \ldots, p_q^{r_q}\} - 1 = 1$ Latin square.

this dissertation due the fact that it requires a lengthy proof and notions from the field of combinatorial designs that fall beyond the scope of this dissertation.

Another (much shorter) disproof of Euler's conjecture was, however, given by Zhu [154], and this proof is partially reproduced here. The proof relies on the following construction using prolongation of the λ-Latin square of $GF(n)$ (see §2.1 and §2.2). Let $\boldsymbol{L}$ be the λ-Latin square of $GF(n)$. If $(G, +, \times) = GF(p)$, it may be noted that the i-th entry on the k-th diagonal of $\boldsymbol{L}$ contains $\boldsymbol{L}(k+i, i) = k + (1+\lambda)i$, and therefore that the k-th diagonal is a transversal (it is the k-th row of the $(1+\lambda)$-Latin square of $GF(n)$) provided, however, that $\lambda \neq p-1$. If $K = (k_1, k_2, \ldots, k_q) \in G^q$ for $q \leq n$ is an ordered q-tuple, α is a permutation of K and $\boldsymbol{Q}$ is a Latin square of order q, then the $(K, \alpha, \boldsymbol{Q})$-*prolongation of* $\boldsymbol{L}$ is the Latin square resulting from prolongation of $\boldsymbol{L}$ using the k_i-th diagonals for all $1 \leq i \leq q$, where the row-projection of the k_1-st diagonal is appended first, the row-projection of the k_2-nd diagonal second, and so on, while the column-projection of the $\alpha(k_1)$-st diagonal is appended first, the column-projection of the $\alpha(k_2)$-nd diagonal second, and so on. Finally, the Latin square $\boldsymbol{Q}$ is used to fill in the $q \times q$ empty square in the lower right-hand corner of the resulting array.

The following theorem shows that if the diagonals used to prolongate two such orthogonal Latin squares satisfy certain conditions, then the resulting Latin squares are also orthogonal.

Theorem 3.2.4 (Theorem 1, [154]) *Let $\boldsymbol{L}_\lambda$ be the λ-Latin square and $\boldsymbol{L}_\mu$ the μ-Latin square of $GF(p)$, where p is prime and where λ and μ are distinct elements of $GF(p)\backslash\{p-1\}$, and let $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ be two orthogonal Latin squares of order q. If $K = (k_1, k_2, \ldots, k_q) \in G^q$ and $L = (\ell_1, \ell_2, \ldots, \ell_q) \in G^q$ are ordered q-tuples, and α and β are permutations of K and L respectively, then the $(K, \alpha, \boldsymbol{Q}_1)$-prolongation of $\boldsymbol{L}_\lambda$ is orthogonal to the $(L, \beta, \boldsymbol{Q}_2)$-prolongation of $\boldsymbol{L}_\mu$ if $k_i \neq \ell_j$ for all $k_i \in K$ and $\ell_j \in L$, and if the set containing*

$$h_i = \frac{((1+\mu)k_i - (1+\lambda)\ell_i)}{(\mu - \lambda)}$$

and

$$h_i' = \frac{((1+\mu)(-\lambda\alpha(k_i)) - (1+\lambda)(-\mu\beta(\ell_i)))}{(\mu - \lambda)}$$

for all $1 \leq i \leq q$ contains each element of $K \cup L$ exactly once.

In order to illustrate, to some extent, the usefulness of the preceding theorem, Zhu gave the following example of the construction of a pair of orthogonal Latin squares of order 18, which is an odd multiple of 2. Consider the 4-Latin square and the 10-Latin square of $GF(13)$, which are given by

$$\begin{bmatrix} 0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 \\ 1 & 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 6 & 10 \\ 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 & 11 \\ 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 \\ 4 & 8 & 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 \\ 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 \\ 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 \\ 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 & 3 \\ 8 & 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 \\ 9 & 0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 \\ 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 6 \\ 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 \\ 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 \\ 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 \\ 2 & 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 \\ 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 \\ 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 & 7 \\ 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 \\ 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 \\ 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 \\ 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 \\ 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 \\ 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 \\ 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 \\ 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 \end{bmatrix},$$

respectively (hence $\lambda = 4$ and $\mu = 10$). Furthermore, let $K = (1, 2, 3, 4, 5)$, $L = (9, 12, 11, 10, 8)$, $\alpha = \binom{0\,1\,2\,3\,4}{3\,0\,1\,2\,4}$ and $\beta = \binom{0\,1\,2\,3\,4}{1\,2\,3\,0\,4}$. It may easily be verified that the set containing

$$\frac{((1+\mu)k_i - (1+\lambda)\ell_i)}{(\mu-\lambda)} = \frac{11k_i - 5\ell_i}{6} = 4k_i - 3\ell_i$$

and

$$\frac{((1+\mu)(-\lambda\alpha(k_i)) - (1+\lambda)(-\mu\beta(\ell_i)))}{(\mu-\lambda)} = \frac{8\alpha(k_i) + 11\beta(\ell_i)}{6} = 10\alpha(k_i) + 4\beta(\ell_i)$$

for all $1 \leq i \leq 5$ is the set $\mathbb{Z}_{13}\backslash\{0\} = K \cup L$, and therefore that the $(K, \alpha, \boldsymbol{Q}_1)$-prolongation of the 4-Latin square of $GF(13)$ is orthogonal to the $(L, \beta, \boldsymbol{Q}_2)$-prolongation of the 10-Latin square of $GF(13)$, where $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ may be any two orthogonal Latin squares of order 5. Taking $\boldsymbol{Q}_1$ and $\boldsymbol{Q}_2$ as the 1-Latin square and the 4-Latin square of $GF(5)$ respectively, the two orthogonal Latin square of order 18 are

$$\boldsymbol{L}_{3.7} = \begin{bmatrix}
0 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 17 & 16 & 15 & 14 & 13 & 10 & 9 & 5 & 1 & 6 \\
13 & 5 & 9 & 0 & 4 & 8 & 12 & 3 & 7 & 17 & 16 & 15 & 14 & 2 & 1 & 10 & 6 & 11 \\
14 & 13 & 10 & 1 & 5 & 9 & 0 & 4 & 8 & 12 & 17 & 16 & 15 & 7 & 6 & 2 & 11 & 3 \\
15 & 14 & 13 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 17 & 16 & 12 & 11 & 7 & 3 & 8 \\
16 & 15 & 14 & 13 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 17 & 4 & 3 & 12 & 8 & 0 \\
17 & 16 & 15 & 14 & 13 & 12 & 3 & 7 & 11 & 2 & 6 & 10 & 1 & 9 & 8 & 4 & 0 & 5 \\
6 & 17 & 16 & 15 & 14 & 13 & 4 & 8 & 12 & 3 & 7 & 11 & 2 & 1 & 0 & 9 & 5 & 10 \\
7 & 11 & 17 & 16 & 15 & 14 & 13 & 9 & 0 & 4 & 8 & 12 & 3 & 6 & 5 & 1 & 10 & 2 \\
8 & 12 & 3 & 17 & 16 & 15 & 14 & 13 & 1 & 5 & 9 & 0 & 4 & 11 & 10 & 6 & 2 & 7 \\
9 & 0 & 4 & 8 & 17 & 16 & 15 & 14 & 13 & 6 & 10 & 1 & 5 & 3 & 2 & 11 & 7 & 12 \\
10 & 1 & 5 & 9 & 0 & 17 & 16 & 15 & 14 & 13 & 11 & 2 & 6 & 8 & 7 & 3 & 12 & 4 \\
11 & 2 & 6 & 10 & 1 & 5 & 17 & 16 & 15 & 14 & 13 & 3 & 7 & 0 & 12 & 8 & 4 & 9 \\
12 & 3 & 7 & 11 & 2 & 6 & 10 & 17 & 16 & 15 & 14 & 13 & 8 & 5 & 4 & 0 & 9 & 1 \\
1 & 6 & 11 & 3 & 8 & 0 & 5 & 10 & 2 & 7 & 12 & 4 & 9 & 13 & 14 & 15 & 16 & 17 \\
2 & 7 & 12 & 4 & 9 & 1 & 6 & 11 & 3 & 8 & 0 & 5 & 10 & 14 & 15 & 16 & 17 & 13 \\
3 & 8 & 0 & 5 & 10 & 2 & 7 & 12 & 4 & 9 & 1 & 6 & 11 & 15 & 16 & 17 & 13 & 14 \\
4 & 9 & 1 & 6 & 11 & 3 & 8 & 0 & 5 & 10 & 2 & 7 & 12 & 16 & 17 & 13 & 14 & 15 \\
5 & 10 & 2 & 7 & 12 & 4 & 9 & 1 & 6 & 11 & 3 & 8 & 0 & 17 & 13 & 14 & 15 & 16
\end{bmatrix},$$

and

$$\boldsymbol{L}_{3.8} = \begin{bmatrix}
0 & 14 & 15 & 16 & 13 & 17 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 10 & 7 & 4 & 1 & 11 \\
1 & 11 & 14 & 15 & 16 & 13 & 17 & 6 & 3 & 0 & 10 & 7 & 4 & 8 & 5 & 2 & 12 & 9 \\
2 & 12 & 9 & 14 & 15 & 16 & 13 & 17 & 4 & 1 & 11 & 8 & 5 & 6 & 3 & 0 & 10 & 7 \\
3 & 0 & 10 & 7 & 14 & 15 & 16 & 13 & 17 & 2 & 12 & 9 & 6 & 4 & 1 & 11 & 8 & 5 \\
4 & 1 & 11 & 8 & 5 & 14 & 15 & 16 & 13 & 17 & 0 & 10 & 7 & 2 & 12 & 9 & 6 & 3 \\
5 & 2 & 12 & 9 & 6 & 3 & 14 & 15 & 16 & 13 & 17 & 11 & 8 & 0 & 10 & 7 & 4 & 1 \\
6 & 3 & 0 & 10 & 7 & 4 & 1 & 14 & 15 & 16 & 13 & 17 & 9 & 11 & 8 & 5 & 2 & 12 \\
7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 14 & 15 & 16 & 13 & 17 & 9 & 6 & 3 & 0 & 10 \\
17 & 5 & 2 & 12 & 9 & 6 & 3 & 0 & 10 & 14 & 15 & 16 & 13 & 7 & 4 & 1 & 11 & 8 \\
13 & 17 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 14 & 15 & 16 & 5 & 2 & 12 & 9 & 6 \\
16 & 13 & 17 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 14 & 15 & 3 & 0 & 10 & 7 & 4 \\
15 & 16 & 13 & 17 & 12 & 9 & 6 & 3 & 0 & 10 & 7 & 4 & 14 & 1 & 11 & 8 & 5 & 2 \\
14 & 15 & 16 & 13 & 17 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 & 12 & 9 & 6 & 3 & 0 \\
9 & 7 & 5 & 3 & 1 & 12 & 10 & 8 & 6 & 4 & 2 & 0 & 11 & 13 & 17 & 16 & 15 & 14 \\
12 & 10 & 8 & 6 & 4 & 2 & 0 & 11 & 9 & 7 & 5 & 3 & 1 & 14 & 13 & 17 & 16 & 15 \\
11 & 9 & 7 & 5 & 3 & 1 & 12 & 10 & 8 & 6 & 4 & 2 & 0 & 15 & 14 & 13 & 17 & 16 \\
10 & 8 & 6 & 4 & 2 & 0 & 11 & 9 & 7 & 5 & 3 & 1 & 12 & 16 & 15 & 14 & 13 & 17 \\
8 & 6 & 4 & 2 & 0 & 11 & 9 & 7 & 5 & 3 & 1 & 12 & 10 & 17 & 16 & 15 & 14 & 13
\end{bmatrix}.$$

The following two theorems, also due to Zhu [154], give infinite classes of orders for which the above construction is possible. The proofs are omitted since they require number theoretic methods beyond the scope of this dissertation.

Theorem 3.2.5 (Theorem 2, [154]) *Suppose $p = 3k + 1$ is prime for some integer $k > 1$. Let $q = 2$ if $k = 2$ and let $q = a^k$ if $k > 2$ for any $a \in GF(p)$. Then the conditions required in Theorem 3.2.4 are satisfied if $\lambda = q^{-1}(q-1)$, $\mu = (q-1)^{-1}q$, $K = (1, q, q^2)$, $L = (-q, -q^2, -1)$, $\alpha = \binom{0\,1\,2}{0\,1\,2}$ and $\beta = \binom{0\,1\,2}{1\,2\,0}$.*

Theorem 3.2.6 (Theorem 3, [154]) *If $p = 3k - 1$ is prime for some integer $k > 2$, let q be the element of $\in GF(p)$ for which $q^3 = 10$. Then the conditions required in Theorem 3.2.4 are satisfied if $\lambda = -3$, $\mu = 3^{-1} + 2(3^{-1})q$, $K = (0, 1, -\mu^{-1}b)$, $L = (a, b, c)$, $\alpha = \binom{0\,1\,2}{0\,1\,2}$ and $\beta = \binom{0\,1\,2}{0\,2\,1}$, where $a = -(2\mu)^{-1}(\mu + 3)b$, $b = -2^{-1}(1 + \mu)$ and $c = 1 - (\mu^{-1} + 1)b - a$.*

It follows from the two preceding theorems that a pair of orthogonal Latin squares of order $p+3$ exists if p is not a multiple of 3. This fact, together with a number of the results discussed in §2.2, may be used to disprove Euler's conjecture for all orders except 6, as follows.

Theorem 3.2.7 (Lemma 3, [154]) *A pair of orthogonal Latin squares of order n exists if $n = 2 \,(\mathrm{mod}\ 4) > 6$.*

Proof: Two cases are considered, namely where $n = 4k + 2$, for some integer k, is a multiple of 3, and where it is not.

Case 1: n is not a multiple of 3. In this case the odd integer $n - 3 = 4k - 1$ is also not a multiple of 3, and therefore must be an odd multiple of an odd prime which is not a multiple of 3. Hence $n = pm + 3$ where p is prime and not a multiple of three, and where m is an odd integer. Since p is prime and not a multiple of 3, it follows from Theorems 3.2.5 and 3.2.6 that a pair of orthogonal Latin squares of order $p + 3$ exist with a pair of orthogonal Latin squares of order 3 as subsquares. Furthermore, by Corollary 3.2.1 a pair of orthogonal Latin squares of order m exists, and therefore a pair of orthogonal Latin squares of order $n = pm + 3$ exists by Corollary 2.4.2.

Case 2: n is a multiple of 3. If n is a multiple of an odd prime other than 3, then it is of the form $n = 2(2t+1)3^s = (4t+2)3^s$, where s and t are integers. Since $4t+2$ is not a multiple of 3, a pair of orthogonal Latin squares of order $4t + 2$ exists by Case 1 above. Then by Corollary 2.4.1 a pair of orthogonal Latin squares of order n exists. If n is of the form $n = 2(3^s)$ for some integer s, then n may be written as $n = 18(3^{s-2})$, and since $\boldsymbol{L}_{3.7}$ and $\boldsymbol{L}_{3.8}$ are two orthogonal Latin squares of order 18, a pair of orthogonal Latin squares of order n exists by Corollary 2.4.1. ■

Since Euler's conjecture was settled in 1960 by Bose, Shrikhande and Parker [23], researchers turned their attention to the next step in the construction of sets of orthogonal Latin squares, namely the construction of 3-MOLS. A number of constructions of 3-MOLS of various orders have been given by Hanani [70], Mills [106], Wang and Wilson [144], Wallis [141] and Todorov [137]. In 1970 Hanani used constructions based on pairwise balanced designs to show that a 3-MOLS exists for any order larger than 51, and also gave some constructions for 5-MOLS and 29-MOLS, while in 1972 Mills showed that a 3-MOLS of order n exists if $n = 0, 1 \,(\mathrm{mod}\ 4)$. The existence of 3-MOLS for any $n \notin \{2, 3, 6, 10, 14\}$ was established by Wang and Wilson in 1978, while another proof of the same result was given by Wallis in 1984. The case of $n = 14$ was the last case to be resolved; this was done in 1985 by Todorov, who found a 3-MOLS of order 14 by means of a computer search.

In spite of various efforts by researchers to resolve this question, the question of the existence of a 3-MOLS of order 10 is still open. Attempts at constructing a 3-MOLS of order 10 have been published, among various others, by Acketa and Matić-Kekić [2], Brown [26], Brown and Parker [27, 28], Delisle [43], Myrvold [109] and Parker [117], but so far only necessary conditions for the existence of a 3-MOLS of order 10 have been established.

The following theorem shows how some of the constructions of §2.2 may be used to guarantee a 3-MOLS for an infinite number of orders, the proof of which is similar to the proof of Theorem 2 in Mendelsohn [105].

Theorem 3.2.8 *A 3-MOLS of order n exists if $n \neq 2 \pmod 4$, $n \neq 3 \pmod 9$ and $n \neq 6 \pmod 9$.*

Proof: Let $n = \prod_{i=1}^{q} p_i^{r^i}$ be the unique factorisation of $n \in \mathbb{N}$ into powers of distinct primes where $r_1, \ldots, r_q > 0$. Since Theorem 2.2.2 guarantees the construction of a 3-MOLS of order $p^r \geq 4$, where p is prime and $r > 0$, a 3-MOLS of order n may be constructed using Theorems 2.2.2 and 2.4.3 provided that $n = 2^a 3^b \prod_{i=1}^{q} p_i^{r^i}$ where $a \neq 1 \neq b$. This excludes the case where $n = 2\prod_{i=1}^{q} p_i^{r_i}$ (where n is an odd multiple of 2, *i.e.* $n = 2 \pmod 4$) and the case where $n = 3\prod_{i=1}^{q} p_i^{r_i}$ (where $n = 3k$ such that k is not divisible by 3, *i.e.* $n = 3 \pmod 9$ or $n = 6 \pmod 9$). ■

An interesting construction of a 3-MOLS was given by Todorov [137], who used this construction to resolve the existence question for 3-MOLS for the penultimate unresolved order, namely $n = 14$. His construction utilises a so-called $(n+1, k)$-*near-difference matrix*[5], which, given a group $(G, \circ)$ of order n, is a $k \times (n+2)$ matrix $\boldsymbol{D}$ containing elements of G, and k empty cells, such that in any $2 \times (n+2)$ submatrix $\boldsymbol{D}'$ there is exactly one column j such that $\boldsymbol{D}'(0,j) \circ \boldsymbol{D}'(1,j)^{-1} = a$ for every $a \in G$, exactly one column j for which $\boldsymbol{D}(0,j)$ is empty and $\boldsymbol{D}(1,j)$ non-empty, and exactly one column j for which $\boldsymbol{D}(1,j)$ is empty and $\boldsymbol{D}(0,j)$ non-empty. An example of such an array (which is one of three found via a computer search by Todorov) containing elements from the group $(\mathbb{Z}_{13}, +)$ is

$$\begin{bmatrix} \infty & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \infty & 0 & 1 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 0 & 0 & \infty & 2 & 12 & 10 & 7 & 9 & 5 & 4 & 1 & 11 & 8 & 3 & 6 \\ 0 & 1 & 2 & \infty & 9 & 5 & 3 & 12 & 7 & 11 & 0 & 4 & 6 & 8 & 10 \\ 0 & 3 & 12 & 9 & \infty & 6 & 2 & 7 & 11 & 1 & 5 & 10 & 0 & 4 & 8 \end{bmatrix},$$

where the symbol ∞ is used to denote an empty cell. Given any $(n+1, k)$-near-difference matrix $\boldsymbol{D}$ over the group $(\mathbb{Z}_n, +)$, let $\boldsymbol{D}_i$, for some $i \in \mathbb{Z}_n$, denote the matrix such that $\boldsymbol{D}_i(j,k) = \boldsymbol{D}(j,k) + i \pmod n$ for all $0 \leq j \leq k$ and $0 \leq k \leq n+2$, where the convention $\infty \pm a = a \pm \infty = \infty$ is henceforth assumed for all $a \in \mathbb{Z}_n$. It is easy to see that $\boldsymbol{D}_i$ for any $i \in \mathbb{Z}_n$ is also a $(n+1, k)$-near-difference matrix, and the following theorem utilises this fact to show that a $(n+1, k)$-near-difference matrix may be used to construct a $(k-2)$-MOLS of order $n+1$. This theorem is simply a combination of Lemma 4.6 and Corollary 4.16 in [18, pp. 546–551], and the proof of this theorem is achieved below by generalising the method for obtaining a 3-MOLS of order 14 from a $(14, 5)$-near-difference matrix by Todorov [137].

Theorem 3.2.9 *If a $(n+1, k)$-near-difference matrix exists, then an $OA(k, n+1)$ exists.*

[5]A near-difference matrix is a special case of a *quasi-difference matrix*, a general definition of which may be found in Beth *et al.* [18, p. 550].

Proof: Let $\boldsymbol{D}$ be a $(n+1,k)$-near-difference matrix defined over the group $(\mathbb{Z}_n,+)$, let $\boldsymbol{\infty}$ be a column vector of length k containing only the symbol ∞ and let

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{\infty} & \boldsymbol{D}_0 & \boldsymbol{D}_1 & \boldsymbol{D}_2 & \dots & \boldsymbol{D}_{n-1} \end{bmatrix}.$$

If i and j are any two rows of $\boldsymbol{A}$, then it is first of all easy to see that, by definition, no two columns in $\boldsymbol{D}+a$ are the same for any $a \in \mathbb{Z}_n$, and that the first column of $\boldsymbol{A}$ is the only column that contains the symbol ∞ more than once. Assume that $\boldsymbol{D}_i(a,k) = \boldsymbol{D}_j(a,\ell)$ and $\boldsymbol{D}_i(b,k) = \boldsymbol{D}_j(b,\ell)$ for any two rows a and b of $\boldsymbol{A}$ and $i<j$. Then

$$\begin{aligned} \boldsymbol{D}_i(a,k) - \boldsymbol{D}_i(b,k) &= \boldsymbol{D}_j(a,\ell) - \boldsymbol{D}_j(b,\ell) \\ &= (\boldsymbol{D}_i(a,\ell) + (j-i)) - (\boldsymbol{D}_i(b,\ell) + (j-i)) \\ &= \boldsymbol{D}_i(a,\ell) - \boldsymbol{D}_i(b,\ell), \end{aligned}$$

contradicting one of the defining properties of an $(n+1,k)$-near-difference matrix. Hence $\boldsymbol{A}$ is an orthogonal array with k rows and $(n+1)n+1 = (n+1)^2$ columns. ■

By Theorem 2.3.1, an $OA(k,n+1)$ is equivalent to a $(k-2)$-MOLS of order $n+1$. For example, the $(14,5)$-near-difference matrix

$$\begin{bmatrix} \infty & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \infty & 0 & 1 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 0 & 0 & \infty & 2 & 12 & 10 & 7 & 9 & 5 & 4 & 1 & 11 & 8 & 3 & 6 \\ 0 & 1 & 2 & \infty & 9 & 5 & 3 & 12 & 7 & 11 & 0 & 4 & 6 & 8 & 10 \\ 0 & 3 & 12 & 9 & \infty & 6 & 2 & 7 & 11 & 1 & 5 & 10 & 0 & 4 & 8 \end{bmatrix}$$

given by Todorov [137] may used to construct the three mutually orthogonal Latin squares

$$\begin{bmatrix} \infty & 2 & 10 & 12 & 7 & 9 & 5 & 4 & 1 & 11 & 8 & 3 & 6 & 0 \\ 7 & \infty & 3 & 11 & 0 & 8 & 10 & 6 & 5 & 2 & 12 & 9 & 4 & 1 \\ 5 & 8 & \infty & 4 & 12 & 1 & 9 & 11 & 7 & 6 & 3 & 0 & 10 & 2 \\ 11 & 6 & 9 & \infty & 5 & 0 & 2 & 10 & 12 & 8 & 7 & 4 & 1 & 3 \\ 2 & 12 & 7 & 10 & \infty & 6 & 1 & 3 & 11 & 0 & 9 & 8 & 5 & 4 \\ 6 & 3 & 0 & 8 & 11 & \infty & 7 & 2 & 4 & 12 & 1 & 10 & 9 & 5 \\ 10 & 7 & 4 & 1 & 9 & 12 & \infty & 8 & 3 & 5 & 0 & 2 & 11 & 6 \\ 12 & 11 & 8 & 5 & 2 & 10 & 0 & \infty & 9 & 4 & 6 & 1 & 3 & 7 \\ 4 & 0 & 12 & 9 & 6 & 3 & 11 & 1 & \infty & 10 & 5 & 7 & 2 & 8 \\ 3 & 5 & 1 & 0 & 10 & 7 & 4 & 12 & 2 & \infty & 11 & 6 & 8 & 9 \\ 9 & 4 & 6 & 2 & 1 & 11 & 8 & 5 & 0 & 3 & \infty & 12 & 7 & 10 \\ 8 & 10 & 5 & 7 & 3 & 2 & 12 & 9 & 6 & 1 & 4 & \infty & 0 & 11 \\ 1 & 9 & 11 & 6 & 8 & 4 & 3 & 0 & 10 & 7 & 2 & 5 & \infty & 12 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & \infty \end{bmatrix}, \begin{bmatrix} 2 & \infty & 5 & 9 & 3 & 12 & 7 & 11 & 0 & 4 & 6 & 8 & 10 & 1 \\ 11 & 3 & \infty & 6 & 10 & 4 & 0 & 8 & 12 & 1 & 5 & 7 & 9 & 2 \\ 10 & 12 & 4 & \infty & 7 & 11 & 5 & 1 & 9 & 0 & 2 & 6 & 8 & 3 \\ 9 & 11 & 0 & 5 & \infty & 8 & 12 & 6 & 2 & 10 & 1 & 3 & 7 & 4 \\ 8 & 10 & 12 & 1 & 6 & \infty & 9 & 0 & 7 & 3 & 11 & 2 & 4 & 5 \\ 5 & 9 & 11 & 0 & 2 & 7 & \infty & 10 & 1 & 8 & 4 & 12 & 3 & 6 \\ 4 & 6 & 10 & 12 & 1 & 3 & 8 & \infty & 11 & 2 & 9 & 5 & 0 & 7 \\ 1 & 5 & 7 & 11 & 0 & 2 & 4 & 9 & \infty & 12 & 3 & 10 & 6 & 8 \\ 7 & 2 & 6 & 8 & 12 & 1 & 3 & 5 & 10 & \infty & 0 & 4 & 11 & 9 \\ 12 & 8 & 3 & 7 & 9 & 0 & 2 & 4 & 6 & 11 & \infty & 1 & 5 & 10 \\ 6 & 0 & 9 & 4 & 8 & 10 & 1 & 3 & 5 & 7 & 12 & \infty & 2 & 11 \\ 3 & 7 & 1 & 10 & 5 & 9 & 11 & 2 & 4 & 6 & 8 & 0 & \infty & 12 \\ \infty & 4 & 8 & 2 & 11 & 6 & 10 & 12 & 3 & 5 & 7 & 9 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & \infty \end{bmatrix}$$

and

$$\begin{bmatrix} 12 & 9 & 6 & \infty & 2 & 7 & 11 & 1 & 5 & 10 & 0 & 4 & 8 & 3 \\ 9 & 0 & 10 & 7 & \infty & 3 & 8 & 12 & 2 & 6 & 11 & 1 & 5 & 4 \\ 6 & 10 & 1 & 11 & 8 & \infty & 4 & 9 & 0 & 3 & 7 & 12 & 2 & 5 \\ 3 & 7 & 11 & 2 & 12 & 9 & \infty & 5 & 10 & 1 & 4 & 8 & 0 & 6 \\ 1 & 4 & 8 & 12 & 3 & 0 & 10 & \infty & 6 & 11 & 2 & 5 & 9 & 7 \\ 10 & 2 & 5 & 9 & 0 & 4 & 1 & 11 & \infty & 7 & 12 & 3 & 6 & 8 \\ 7 & 11 & 3 & 6 & 10 & 1 & 5 & 2 & 12 & \infty & 8 & 0 & 4 & 9 \\ 5 & 8 & 12 & 4 & 7 & 11 & 2 & 6 & 3 & 0 & \infty & 9 & 1 & 10 \\ 2 & 6 & 9 & 0 & 5 & 8 & 12 & 3 & 7 & 4 & 1 & \infty & 10 & 11 \\ 11 & 3 & 7 & 10 & 1 & 6 & 9 & 0 & 4 & 8 & 5 & 2 & \infty & 12 \\ \infty & 12 & 4 & 8 & 11 & 2 & 7 & 10 & 1 & 5 & 9 & 6 & 3 & 0 \\ 4 & \infty & 0 & 5 & 9 & 12 & 3 & 8 & 11 & 2 & 6 & 10 & 7 & 1 \\ 8 & 5 & \infty & 1 & 6 & 10 & 0 & 4 & 9 & 12 & 3 & 7 & 11 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & \infty \end{bmatrix}$$

of order 14.

3.3 Self-orthogonal Latin squares and SOLSSOMs

In 1957 Stein [131] considered, among other aspects of quasigroups, the implications (in terms of special properties that quasigroups may satisfy) of imposing various identities on quasigroups in an attempt to construct counterexamples to Euler's conjecture. The identities that he considered became known as *Stein's laws* in the theory of quasigroups (see, for instance, Dénes and Keedwell [41, §2] and Bennet and Zhu [15]). Two identities of particular interest in this section are $a \circ (a \circ b) = b \circ a$ (known as Stein's first law) and $(b \circ a) \circ (a \circ b) = a$ (known as Stein's third law), where a and b are elements of some quasigroup $(G, \circ)$.

Consider, for instance, a quasigroup $(G, \circ)$ which satisfies $a \circ (a \circ b) = b \circ a$ for each pair of elements $a, b \in G$, and let $\boldsymbol{L}$ be the Latin square representing the Cayley-table of $(G, \circ)$. Then $\boldsymbol{L}(i, \boldsymbol{L}(i, j)) = \boldsymbol{L}(j, i)$ for all $i, j \in \mathbb{Z}_n$. Furthermore, if $\boldsymbol{L}(i, j) = \boldsymbol{L}(k, \ell)$ and $\boldsymbol{L}^T(i, j) = \boldsymbol{L}^T(k, \ell)$ (*i.e* $\boldsymbol{L}(j, i) = \boldsymbol{L}(\ell, k)$), then

$$\boldsymbol{L}(i, \boldsymbol{L}(i, j)) = \boldsymbol{L}(j, i) = \boldsymbol{L}(\ell, k) = \boldsymbol{L}(k, \boldsymbol{L}(k, \ell)) = \boldsymbol{L}(k, \boldsymbol{L}(i, j)),$$

which implies that $i = k$ since $\boldsymbol{L}$ is a Latin square. Since now $\boldsymbol{L}(i, j) = \boldsymbol{L}(i, \ell)$, it also follows that $j = \ell$, and that $\boldsymbol{L}$ and $\boldsymbol{L}^T$ are, by definition, orthogonal. Furthermore, let $(G, \circ)$ be a quasigroup which satisfies the identity $(b \circ a) \circ (a \circ b) = a$ for all pairs of elements $a, b \in G$, and let $\boldsymbol{L}$ be the Latin square representing the Cayley-table of $(G, \circ)$. Hence $\boldsymbol{L}(\boldsymbol{L}(j, i), \boldsymbol{L}(i, j)) = i$ for any $i, j \in \mathbb{Z}_n$, and if $\boldsymbol{L}(i, j) = \boldsymbol{L}(k, \ell)$ and $\boldsymbol{L}^T(i, j) = \boldsymbol{L}^T(k, \ell)$, then

$$i = \boldsymbol{L}(\boldsymbol{L}(j, i), \boldsymbol{L}(i, j)) = \boldsymbol{L}(\boldsymbol{L}(\ell, k), \boldsymbol{L}(k, \ell)) = k.$$

It similarly follows that $j = \ell$. Hence $\boldsymbol{L}$ and $\boldsymbol{L}^T$ are again orthogonal. This gives rise to a very special case of a pair of orthogonal Latin squares, a formal definition of which follows (which may also be found in Colbourn *et al.* [38, §III.5]).

Definition 3.3.1 (Self-orthogonal Latin square) *A* self-orthogonal Latin square (SOLS) *is a Latin square orthogonal to its transpose. If the Cayley-table of a quasigroup is a SOLS, then the quasigroup is also said to be* self-orthogonal[6]*.* □

An example of a SOLS is

$$\boldsymbol{L}_{3.9} = \begin{bmatrix} 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \\ 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \end{bmatrix},$$

and it may be noted that there exists a bijection α from $\mathbb{Z}_n^{(2)}$ (the set of all 2-subsets of $\mathbb{Z}_n$) to itself such that $\alpha(\{i, j\}) = \{k, \ell\}$ if either $\boldsymbol{L}(i, j) = k$ and $\boldsymbol{L}(j, i) = \ell$, or $\boldsymbol{L}(i, j) = \ell$ and $\boldsymbol{L}(j, i) = k$ for any SOLS $\boldsymbol{L}$, while there exists a bijection β from $\mathbb{Z}_n$ to itself such that $\alpha(i) = k$ if $\boldsymbol{L}(i, i) = k$. This provides a means for quickly verifying whether a Latin square is self-orthogonal. For example, for the SOLS $\boldsymbol{L}_{3.9}$ the bijections

$$\alpha = \begin{pmatrix} \{0,1\} & \{0,2\} & \{0,3\} & \{1,2\} & \{1,3\} & \{2,3\} \\ \{2,3\} & \{0,2\} & \{0,3\} & \{1,2\} & \{1,3\} & \{0,1\} \end{pmatrix}$$

and $\beta = \binom{0\,1\,2\,3}{1\,0\,3\,2}$ satisfy the above-mentioned properties. Any SOLS is therefore a Latin square with the property that its diagonal is a transversal (henceforth referred to as a *diagonal Latin*

[6]It should be noted, however, that self-orthogonal quasigroups have also been called *anti-abelian* by Sade [127].

square), and also has the property that $\boldsymbol{L}(i,j) = \boldsymbol{L}(j,i)$ implies $i = j$. This property is summarised in the following theorem in terms of universal permutations in order to facilitate further referencing.

Theorem 3.3.1 *The universal-permutation of an element in a SOLS has exactly one fixed point and no 2-cycles.*

Sade's [127] use of the phrase "anti-abelian" to describe self-orthogonal quasigroups seems to imply that there exists some "opposite" relationship between Abelian quasigroups[7] and self-orthogonal quasigroups (*i.e.* between symmetric Latin squares and SOLS), or that they might be seen as counterparts of one another. Indeed, a Latin square cannot be both symmetric and self-orthogonal, since in the former case each universal permutation contains only fixed points and 2-cycles (it will soon be illustrated why this is the case), while in the latter case each universal permutation contains exactly one fixed point and no 2-cycles. However, in both cases a very special relationship exists between the Latin square and its transpose, namely equality and orthogonality, respectively. A natural question is therefore whether there exist symmetric Latin squares and SOLS exhibiting the special relationship of orthogonality between them. This notion was first considered by Wang [143] in his 1978 diploma thesis, and in 1979 Wallis [139] highlighted the fact that such designs may be used to schedule a special type of resolvable mixed doubles tournament. Since then these designs have been studied extensively in the field of Latin squares, and a formal definition of this notion follows which may also be found in Colbourn *et al.* [38, §5.6].

Definition 3.3.2 (SOLSSOM) *A* self-orthogonal Latin square with a symmetric orthogonal mate (SOLSSOM) *of order n is a pair of orthogonal Latin squares $(\boldsymbol{L},\boldsymbol{S})$ of order n such that $\boldsymbol{L}$ is self-orthogonal and $\boldsymbol{S}$ is symmetric.* □

It may easily be verified that the pair of orthogonal Latin squares

$$\begin{bmatrix} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix},$$

form a SOLSSOM of order 4. It is important to note that the universal permutations of a symmetric Latin square are *involutions*, *i.e.* permutations which only admit fixed points and 2-cycles. This is true since, if $\boldsymbol{S}$ is a symmetric Latin square, either $\boldsymbol{S}(i,i) = k$ or $\boldsymbol{S}(i,j) = k = \boldsymbol{S}(j,i)$ for any $i,j,k \in \mathbb{Z}_n$, *i.e.* either $\boldsymbol{u}(i) = i$ or $\boldsymbol{u}(i) = j$ and $\boldsymbol{u}(j) = i$. Furthermore, if n is even, it is easy to see that a universal permutation in a symmetric Latin square has an even number of fixed points, while for odd n a universal permutation in a symmetric Latin square has an odd number of fixed points. Since no two universal permutations in a Latin square may have the same fixed point, and since a universal permutation in a symmetric Latin square of odd order cannot only have 2-cycles, each universal permutation in a symmetric Latin square of odd order has exactly one fixed point. A symmetric Latin square of odd order is therefore a diagonal Latin square. On the other hand, a symmetric Latin square of even order may contain repeated elements on the diagonal, provided that an even number of copies of each element

[7] A quasigroup (or group) $(G,\circ)$ is *Abelian* if $a \circ b = b \circ a$ for all $a,b \in G$.

appears on the diagonal. For example, the symmetric Latin squares

$$\begin{bmatrix} 0&1&2&3&4&5&6&7\\ 1&0&4&7&2&6&5&3\\ 2&4&0&5&1&3&7&6\\ 3&7&5&0&6&2&4&1\\ 4&2&1&6&0&7&3&5\\ 5&6&3&2&7&0&1&4\\ 6&5&7&4&3&1&0&2\\ 7&3&6&1&5&4&2&0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0&1&2&3&4&5&6&7\\ 1&4&5&0&2&6&7&3\\ 2&5&7&4&1&3&0&6\\ 3&0&4&7&6&2&5&1\\ 4&2&1&6&5&7&3&0\\ 5&6&3&2&7&0&1&4\\ 6&7&0&5&3&1&4&2\\ 7&3&6&1&0&4&2&5 \end{bmatrix}$$

of order 8 contain one element and four elements on the diagonal, respectively.

For the purpose of enumerating SOLSSOMs (a problem considered later in this dissertation) it is necessary to define the notion of a *standard form* for SOLSSOMs. A SOLSSOM $(\boldsymbol{L}, \boldsymbol{S})$ is *standard* if $\boldsymbol{L}$ is idempotent and $\boldsymbol{S}$ is reduced. A SOLSSOM $(\boldsymbol{L}, \boldsymbol{S})$ of order n has also been called *regular* [38, Definition 5.34] if $\boldsymbol{S}$ is idempotent for odd n and unipotent with $\boldsymbol{S}(i,i) = 0$, for all $i \in \mathbb{Z}_n$, for even n. In this dissertation, however, standard SOLSSOMs are considered since in this case it is not necessary to distinguish between SOLSSOMs of even and odd order.

3.3.1 Spouse-avoiding mixed doubles round-robin tennis tournaments

An interesting application of Latin squares to mixed doubles tournament scheduling was first considered by Brayton *et al.* [24] in 1974, one of whom was approached by the director of the Briarcliff Racquet Club in Briarcliff, New York, who sought a schedule for such a tournament. The tournament consists of n married couples taking part in a mixed-doubles tennis tournament in such a way that each player opposes each other player exactly once and each pair of players are in partnership exactly once, with the exception that no player may be in partnership with or oppose his/her own spouse. Brayton *et al.* referred to such a tournament in which n players take part as a *spouse-avoiding mixed doubles round-robin (SAMDRR) tournament of order n*. More recently, in 2004, Laurie [87] was also approached by the Recreation Tennis Club in Somerset West, South Africa, which sought a schedule for the same type of tournament. This led to a popular publication by Burger and Van Vuuren [35], who utilised constructions from the literature on SOLSSOMs in order to provide schedules for SAMDRR tournaments of orders $4 \leq n \leq 20$ so that sports clubs could have access to such schedules without requiring prior mathematical knowledge of combinatorial design theory.

If n couples participate in an SAMDRR tournament, then each player takes part in $n-1$ rounds, and each player receives a bye in exactly one round of the tournament if n is odd. Hence an SAMDRR tournament cannot be scheduled in fewer than $2 \times \lceil \frac{n}{2} \rceil - 1$ rounds, and if an SAMDRR tournament can be scheduled in exactly $2 \times \lceil \frac{n}{2} \rceil - 1$ rounds, each consisting of $\lfloor \frac{n}{2} \rfloor$ matches, then the tournament is *resolvable*.

Consider, for example, an SAMDRR tournament in which 4 married couples take part, where H_i denotes the husband of the i-th couple and W_i the wife of the i-th couple for all $i \in \mathbb{Z}_4$. A schedule for a resolvable SAMDRR tournament of order 4 is shown in Table 3.5. It may easily be verified that this schedule indeed satisfies the requirements of an SAMDRR tournament.

The following well-known result establishes the connection between SAMDRR tournaments and Latin squares.

Theorem 3.3.2 ([38], Theorem 5.2) *An SAMDRR tournament of order n is equivalent to an idempotent SOLS of order n.*

Round 1		Round 2		Round 3	
H_0	H_1	H_0	H_2	H_0	H_3
W_2	W_3	W_3	W_1	W_1	W_2
H_2	H_3	H_1	H_3	H_1	H_2
W_0	W_1	W_2	W_0	W_0	W_3

TABLE 3.5: *A schedule for an SAMDRR tournament of order 4.*

Proof: Let n couples participate in an SAMDRR tournament of order n, where H_i denotes the husband of the i-th couple and W_i the wife of the i-th couple, for all $i \in \mathbb{Z}_n$. Let $\boldsymbol{L}$ be an $n \times n$ array such that $\boldsymbol{L}(i, j) = k$ if H_i is in partnership with W_k when he opposes H_j for all $i, j \in \mathbb{Z}_n$, $i \neq j$, and such that $\boldsymbol{L}(i, i) = i$ for all $i \in \mathbb{Z}_n$. If $\boldsymbol{L}(i, j) = k$ and $\boldsymbol{L}(i, j') = k$ for any $i, j, j', k \in \mathbb{Z}_n$, then H_i is in partnership with W_k in two distinct matches, and if $\boldsymbol{L}(i, j) = i$ for $i, j \in \mathbb{Z}_n$, $i \neq j$, then H_i is in partnership with his own wife. These two contradictions imply that each element of $\mathbb{Z}_n$ appears exactly once in each row of $\boldsymbol{L}$. Similarly, it may be shown that each element of $\mathbb{Z}_n$ appears exactly once in each column of $\boldsymbol{L}$, and therefore that $\boldsymbol{L}$ is a Latin square. Finally, in the match where H_i opposes H_j, $W_{\boldsymbol{L}(i,j)}$ opposes $W_{\boldsymbol{L}(j,i)}$, and since any two women only oppose one another once throughout the tournament, the pair $(W_{\boldsymbol{L}(i,j)}, W_{\boldsymbol{L}(j,i)})$, or equivalently, the pair $(\boldsymbol{L}(i, j), \boldsymbol{L}(j, i))$, is unique as i and j vary over $\mathbb{Z}_n$. Hence $\boldsymbol{L}$ is an idempotent SOLS, and it may similarly be shown that any idempotent SOLS may be used to schedule an SAMDRR tournament. ■

For example, the idempotent SOLS corresponding the SAMDRR tournament shown in Table 3.5 is given in Table 3.6.

	H_0	H_1	H_2	H_3
H_0	W_0	W_2	W_3	W_1
H_1	W_3	W_1	W_0	W_2
H_2	W_1	W_3	W_2	W_0
H_3	W_2	W_0	W_1	W_3

TABLE 3.6: *The matches of an SAMDRR tournament of order 4 as represented by a SOLS of order 4.*

If an idempotent SOLS of order n therefore exists, then an SAMDRR tournament schedule for n couples may be obtained. It may be noted that since a SOLS of order n is a special case of a pair of orthogonal Latin squares of order n, it may also be used to schedule an MDTT tournament of order n. Furthermore, the existence of an idempotent SOLS of order n does not guarantee the existence of a resolvable SAMDRR tournament.

Consider a resolvable SAMDRR tournament of order n, namely a tournament where the matches are partitioned into the minimum number of rounds so that no player plays twice in any round, and where each couple receives a bye during exactly one round for odd n. Let $\boldsymbol{L}$ be an idempotent SOLS of order n such that $\boldsymbol{L}(i, j) = k$ if H_i (using the same notation as above) is in partnership with W_k when opposing H_j, and let $\boldsymbol{S}$ be an $n \times n$ symmetric array such that $\boldsymbol{S}(i, j) = \boldsymbol{S}(j, i)$ gives the round in which H_i opposes H_j, for all $i, j \in \mathbb{Z}_n$. Furthermore, let $\boldsymbol{S}(i, i) = 0$ for all $i \in \mathbb{Z}_n$ if n is even (where 0 is not used to denote any round), whereas $\boldsymbol{S}(i, i) = i$ for all $i \in \mathbb{Z}_n$ if n is odd (where the couple $\{H_i, W_i\}$ receives a bye in round i). Since each player participates in exactly one match per round, and since for odd n each couple receives a bye in exactly one round, the ordered pairs $(H_i, \boldsymbol{S}(i,j))$, *i.e.* the ordered pairs $(i, \boldsymbol{S}(i,j))$, are unique as i and j vary over $\mathbb{Z}_n$. For the same reason the ordered pairs $(j, \boldsymbol{S}(i,j))$ and $(\boldsymbol{L}(i,j), \boldsymbol{S}(i,j))$ are unique as i and j vary over $\mathbb{Z}_n$. It therefore follows that $\boldsymbol{S}$ is a symmetric Latin square which is orthogonal to $\boldsymbol{L}$, and that $(\boldsymbol{L}, \boldsymbol{S})$ is a SOLSSOM (which is unipotent if n is even).

For example, the SOLSSOM in Table 3.7 represents the resolvable SAMDRR tournament in Table 3.5. If a SOLSSOM of order n may be constructed (which is unipotent if n is even), then a resolvable SAMDRR tournament of order n may be obtained.

	H_0	H_1	H_2	H_3
H_0	W_0	W_2	W_3	W_1
H_1	W_3	W_1	W_0	W_2
H_2	W_1	W_3	W_2	W_0
H_3	W_2	W_0	W_1	W_3

	H_0	H_1	H_2	H_3
H_0	0	1	2	3
H_1	1	0	3	2
H_2	2	3	0	1
H_3	3	2	1	0

TABLE 3.7: *A schedule for a resolvable SAMDRR tournament of order 4 as represented by a SOLSSOM of order 4.*

3.3.2 Constructions of self-orthogonal Latin squares and SOLSSOMs

Further mention of SOLS in published work on Latin squares appear some time after Stein [131] presented his work on quasigroups[8] in 1957, namely in 1963 by Weisner [145]. Weisner used the permutation $p = \binom{0\,1\,2\,3\,4\,5\,6\,7\,8\,9}{1\,2\,3\,4\,5\,6\,7\,8\,0\,9}$ to construct pairs of orthogonal Latin squares of order 10 where, given two permutations r and s, the i-th rows of the two Latin squares are given by $p^i \circ r \circ (p^i)^{-1}$ and $p^i \circ s \circ (p^i)^{-1}$ respectively for $0 \leq i \leq 8$, while th 9-th rows are given by powers of r^k and s^ℓ respectively. Weisner constructed three pairs of orthogonal Latin squares of order 10, and noted that one of these pairs consists of a Latin square and its transpose, namely where $r = \binom{0\,1\,2\,3\,4\,5\,6\,7\,8\,9}{0\,2\,5\,8\,6\,3\,1\,9\,7\,4}$ and $s = \binom{0\,1\,2\,3\,4\,5\,6\,7\,8\,9}{0\,8\,9\,4\,7\,2\,5\,3\,1\,6}$, which results in the Latin squares

$$\begin{bmatrix} 0&2&5&8&6&3&1&9&7&4 \\ 8&1&3&6&0&7&4&2&9&5 \\ 9&0&2&4&7&1&8&5&3&6 \\ 4&9&1&3&5&8&2&0&6&7 \\ 7&5&9&2&4&6&0&3&1&8 \\ 2&8&6&9&3&5&7&1&4&0 \\ 5&3&0&7&9&4&6&8&2&1 \\ 3&6&4&1&8&9&5&7&0&2 \\ 1&4&7&5&2&0&9&6&8&3 \\ 6&7&8&0&1&2&3&4&5&9 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0&8&9&4&7&2&5&3&1&6 \\ 2&1&0&9&5&8&3&6&4&7 \\ 5&3&2&1&9&6&0&4&7&8 \\ 8&6&4&3&2&9&7&1&5&0 \\ 6&0&7&5&4&3&9&8&2&1 \\ 3&7&1&8&6&5&4&9&0&2 \\ 1&4&8&2&0&7&6&5&9&3 \\ 9&2&5&0&3&1&8&7&6&4 \\ 7&9&3&6&1&4&2&0&8&5 \\ 4&5&6&7&8&0&1&2&3&9 \end{bmatrix},$$

respectively. It may be verified that these two Latin squares are orthogonal and transposes of each other. Weisner did not, however, provide any conditions under which the permutations r and s may be used as above to construct pairs of orthogonal Latin squares in general, nor did he explain how he obtained the permutations used for his three constructions.

Early general constructions of SOLS were put forward during the same time by Sade [127] in 1960 using Galois fields, which is similar to the constructions of SOLS given by Mendelsohn [104, 105] in 1971 (see a discussion on these similarities by Dénes and Keedwell [42, pp. 458–459]). The construction given in [105] is somewhat simpler than the one given in [104] and

[8] Stein himself made no explicit reference to SOLS, only to quasigroups with so-called *orthogonal complements*, a definition of which may be found in Dénes and Keedwell [41, p. 175].

covers a larger spectrum of SOLS. This simpler construction is summarised in the following theorem.

Theorem 3.3.3 ([105], Theorem 1) *Let p^q be any prime power other than 2^1 and 3^1, and let λ be any element of $(G,+,\times) = GF(p^q)$ except 0, 1 and 2^{-1}. Then $(G,\circ)$ where $a \circ b = \lambda a + (1-\lambda)b$ for any two elements $a, b \in G$ is a quasigroup whose Cayley-table is a self-orthogonal Latin square.*

Proof: It is easy to see that, since $\lambda \neq 0$ and $\lambda \neq 1$, the equation $c = \lambda a + (1-\lambda)b$ has a unique solution, given any two of a, b or c, and hence that $(G,\circ)$ is a quasigroup. Let $a \circ b = c \circ d$ and $b \circ a = d \circ c$. Then $\lambda a + (1-\lambda)b = \lambda c + (1-\lambda)d$ and $\lambda b + (1-\lambda)a = \lambda d + (1-\lambda)c$. Upon adding these two equations it follows that $a + b = c + d$. Substituting $a = c + d - b$ into the first equation delivers $(1-2\lambda)b = (1-2\lambda)d$. Since $\lambda \neq 2^{-1}$, $(1-2\lambda) \neq 0$ and therefore $b = d$. It may similarly be shown that $a = c$. Hence the Cayley-table of $(G,\circ)$ is a SOLS. ■

For example, let $n = 7$ and $\lambda = 2$. Then the SOLS constructed using the method of Theorem 3.3.3 is

$$\begin{bmatrix} 0&6&5&4&3&2&1\\ 2&1&0&6&5&4&3\\ 4&3&2&1&0&6&5\\ 6&5&4&3&2&1&0\\ 1&0&6&5&4&3&2\\ 3&2&1&0&6&5&4\\ 5&4&3&2&1&0&6 \end{bmatrix}.$$

The following theorem elaborates on the spectrum of orders for which SOLS-constructions are covered by the above theorem.

Theorem 3.3.4 ([105], Theorem 2) *If $n \neq 2\,(\mathrm{mod}\ 4)$, $n \neq 3\,(\mathrm{mod}\ 9)$ and $n \neq 6\,(\mathrm{mod}\ 9)$, then a SOLS of order n exists.*

Proof: By Lemma 2.4.1 and Theorem 2.4.3 it follows that the direct product of two SOLS is again a SOLS, and hence that the existence of SOLS of orders n and m implies the existence of a SOLS of order nm. This result, together with the result of Theorem 3.3.3, states that if $n = 2^a 3^b \prod_{i=1}^{q} p_i^{r_i}$ where $r_i > 0$ is the unique factorisation of $n \in \mathbb{N}$ into powers of distinct primes such that $a \neq 1 \neq b$, then a SOLS of order n exists. As in Theorem 3.2.8, this excludes the case where $n = 2\prod_{i=1}^{q} p_i^{r_i}$ (where n is an odd multiple of 2, *i.e.* $n = 2\,(\mathrm{mod}\ 4)$) and the case where $n = 3\prod_{i=1}^{q} p_i^{r_i}$ (where $n = 3k$ such that k is not divisible by 3, *i.e.* $n = 3\,(\mathrm{mod}\ 9)$ or $n = 6\,(\mathrm{mod}\ 9)$). ■

At roughly the same time that Mendelsohn gave his constructions of SOLS, Németh [110] and Mullin and Németh [107, 108] presented some constructions of SOLS using so-called *room squares* (see, for instance, Laywine and Mullen [88, §11]), while Lindner [90] showed how the generalised singular direct product (see §2.4) may be used to construct SOLS recursively (a similar result for room squares was established by Horton [77]). This may be achieved by means of the following theorem, the proof of which is omitted here.

Theorem 3.3.5 ([90], Theorem 1) *Let $(Q,\circ)$ be a self-orthogonal quasigroup of order n with a subquasigroup $(S,\circ)$ of order m, let $(Q\backslash S, \bullet_1)$ and $(Q\backslash S, \bullet_2)$ be a pair of orthogonal quasigroups of order $\ell = n - m$ and let $(R,\star)$ be an idempotent self-orthogonal quasigroup of order k.*

Furthermore, let $R^2 \backslash \{(r, r) \mid r \in R\}$ be partitioned into two sets R_1 and R_2 such that if $(a, b) \in R_1$, then $(b, a) \in R_2$ and vice versa. *Then the generalised singular direct product $(Q \cup ((Q\backslash S) \times R), *)$ is a self-orthogonal quasigroup of order $\ell k + m$ where, for $a = (a_1, a_2), b = (b_1, b_2) \in ((Q\backslash S) \times R)$,*

$$a * b = \begin{cases} (a_1 \bullet_1 b_1, a_2 \star b_2) & \textit{if } (a_2, b_2) \in R_1, \\ (b_1 \bullet_2 a_1, a_2 \star b_2) & \textit{if } (a_2, b_2) \in R_2. \end{cases}$$

For example, let the Cayley table of a self-orthogonal quasigroup $(Q, \circ)$ be represented by the SOLS

$$\begin{bmatrix} 0 & 4 & 3 & 2 & 1 \\ 3 & 2 & 1 & 0 & 4 \\ 1 & 0 & 4 & 3 & 2 \\ 4 & 3 & 2 & 1 & 0 \\ 2 & 1 & 0 & 4 & 3 \end{bmatrix},$$

where $S = \{0\}$ forms the trivial subquasigroup $(S, \circ)$ of order 1 (which is clearly self-orthogonal). Furthermore, let the Cayley-tables of two orthogonal quasigroups $(Q\backslash S, \bullet_1)$ and $(Q\backslash S, \bullet_2)$ be represented by the pair of orthogonal Latin squares

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 4 & 2 & 3 \\ 4 & 1 & 3 & 2 \\ 3 & 2 & 4 & 1 \\ 2 & 3 & 1 & 4 \end{bmatrix},$$

respectively, and let the Cayley-table of an idempotent self-orthogonal quasigroup $(R, \star)$ be the represented by the SOLS

$$\begin{bmatrix} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \end{bmatrix},$$

where $R^2 \backslash \{(r, r) \mid r \in R\}$ is partitioned into the two sets sets $R_1 = \{(1, 2), (1, 3), (2, 3)\}$ and $R_2 = \{(2, 1), (3, 1), (3, 2)\}$. Then the construction in Theorem 3.3.5 delivers a self-orthogonal quasigroup $(Q \cup ((Q\backslash S) \times R), *)$ whose Cayley-table is given by the SOLS

$$\left[\begin{array}{c|cccc|cccc|cccc|cccc}
0 & (4,0) & (3,0) & (2,0) & (1,0) & (4,1) & (3,1) & (2,1) & (1,1) & (4,2) & (3,2) & (2,2) & (1,2) & (4,3) & (3,3) & (2,3) & (1,3) \\
(3,0) & (2,0) & (1,0) & 0 & (4,0) & (1,2) & (2,2) & (3,2) & (4,2) & (1,3) & (2,3) & (3,3) & (4,3) & (1,1) & (2,1) & (3,1) & (4,1) \\
(1,0) & 0 & (4,0) & (3,0) & (2,0) & (3,2) & (4,2) & (1,2) & (2,2) & (3,3) & (4,3) & (1,3) & (2,3) & (3,1) & (4,1) & (1,1) & (2,1) \\
(4,0) & (3,0) & (2,0) & (1,0) & 0 & (2,2) & (1,2) & (4,2) & (3,2) & (2,3) & (1,3) & (4,3) & (3,3) & (2,1) & (1,1) & (4,1) & (3,1) \\
(2,0) & (1,0) & 0 & (4,0) & (3,0) & (4,2) & (3,2) & (2,2) & (1,2) & (4,3) & (3,3) & (2,3) & (1,3) & (4,1) & (3,1) & (2,1) & (1,1) \\
(3,1) & (1,3) & (4,3) & (2,3) & (3,3) & (2,1) & (1,1) & 0 & (4,1) & (1,0) & (2,0) & (3,0) & (4,0) & (1,2) & (2,2) & (3,2) & (4,2) \\
(1,1) & (4,3) & (1,3) & (3,3) & (2,3) & 0 & (4,1) & (3,1) & (2,1) & (3,0) & (4,0) & (1,0) & (2,0) & (3,2) & (4,2) & (1,2) & (2,2) \\
(4,1) & (3,3) & (2,3) & (4,3) & (1,3) & (3,1) & (2,1) & (1,1) & 0 & (2,0) & (1,0) & (4,0) & (3,0) & (2,2) & (1,2) & (4,2) & (3,2) \\
(2,1) & (2,3) & (3,3) & (1,3) & (4,3) & (1,1) & 0 & (4,1) & (3,1) & (4,0) & (3,0) & (2,0) & (1,0) & (4,2) & (3,2) & (2,2) & (1,2) \\
(3,2) & (1,1) & (4,1) & (2,1) & (3,1) & (1,3) & (4,3) & (2,3) & (3,3) & (2,2) & (1,2) & 0 & (4,2) & (1,0) & (2,0) & (3,0) & (4,0) \\
(1,2) & (4,1) & (1,1) & (3,1) & (2,1) & (4,3) & (1,3) & (3,3) & (2,3) & 0 & (4,2) & (3,2) & (2,2) & (3,0) & (4,0) & (1,0) & (2,0) \\
(4,2) & (3,1) & (2,1) & (4,1) & (1,1) & (3,3) & (2,3) & (4,3) & (1,3) & (3,2) & (2,2) & (1,2) & 0 & (2,0) & (1,0) & (4,0) & (3,0) \\
(2,2) & (2,1) & (3,1) & (1,1) & (4,1) & (2,3) & (3,3) & (1,3) & (4,3) & (1,2) & 0 & (4,2) & (3,2) & (4,0) & (3,0) & (2,0) & (1,0) \\
(3,3) & (1,2) & (4,2) & (2,2) & (3,2) & (1,0) & (4,0) & (2,0) & (3,0) & (1,1) & (4,1) & (2,1) & (3,1) & (2,3) & (1,3) & 0 & (4,3) \\
(1,3) & (4,2) & (1,2) & (3,2) & (2,2) & (4,0) & (1,0) & (3,0) & (2,0) & (4,1) & (1,1) & (3,1) & (2,1) & 0 & (4,3) & (3,3) & (2,3) \\
(4,3) & (3,2) & (2,2) & (4,2) & (1,2) & (3,0) & (2,0) & (4,0) & (1,0) & (3,1) & (2,1) & (4,1) & (1,1) & (3,3) & (2,3) & (1,3) & 0 \\
(2,3) & (2,2) & (3,2) & (1,2) & (4,2) & (2,0) & (3,0) & (1,0) & (4,0) & (2,1) & (3,1) & (1,1) & (4,1) & (1,3) & 0 & (4,3) & (3,3)
\end{array}\right]$$

of order 17.

Further work on SOLS was conducted (among various others) by Hedayat [71] in 1973, who constructed a SOLS of order 10 utilising a recursive technique similar to prolongation, known as *sum composition*. In 1974 Brayton *et al.* [24] finally settled the existence question for SOLS of all orders. Brayton *et al.* proved that a SOLS exists for any order $n \notin \{2, 3, 6\}$[9] using various constructions that were known at that time, most notably constructions using pairwise balanced designs (Brayton *et al.* [24] give a number of references to papers on such designs in which SOLS were also constructed). This proof is not discussed here since it requires notions from the field of combinatorial designs which fall beyond the scope of this dissertation.

Various other constructions of SOLS have been given since the early 1970s. In 1973 and 1975 Hedayat [72, 73] noted the importance of SOLS in terms of applications to experimental design and sports tournament scheduling, and in 1978 Hedayat [74] generalised his technique for constructing a SOLS of order 10, using sum composition, in order to obtain a construction of SOLS containing sub-SOLS for an infinte number of orders. Other interesting techniques for constructing SOLS include a method by McLaurin and Smith [103] which utilises so-called *starters* and *skew adders* in Abelian groups of odd order, as well as a method by Franklin [58] which cyclically develops the diagonals of a SOLS, given only the first column, before also using sum composition to construct SOLS recursively.

Some of the first constructions of SOLSSOMs were given by Wang [143] in 1978 and Wallis [139] in 1979. Wallis, in particular, gave a number of interesting constructions of SOLSSOMs, including constructions from Galois fields (based on Mendelsohn's [105] constructions of SOLS), constructions using so-called *start sequences* in Abelian groups of odd order and recursive constructions. Both these authors gave constructions for an infinite number of orders, and according to [91], Wang covered the largest set of integers, leaving only orders

$$\begin{aligned} n \in \{&10, 14, 39, 46, 51, 54, 58, 62, 66, 70, 74, 82, 87, 98, 102, 118, 123, 142, 159, 174, 183, 194, 202,\\ &214, 219, 230, 258, 267, 278, 282, 303, 394, 398, 402, 422, 1322\}. \end{aligned}$$

unresolved (*i.e.* for any $n \neq 2, 3, 6$ not in this set, a construction was known, while the non-existence of SOLSSOMs of orders $n = 2, 3, 6$ is trivial). In 1983, Lindner *et al.* [91] used so-called *frame-type SOLSSOMs* and a recursive construction similar to the singular direct product, referred to as the *singular indirect product*, in order to construct SOLSSOMs recursively, thereby reducing the above list of unresolved orders to

$$n \in \{10, 14, 39, 46, 54, 58, 62, 66, 70, 87, 102, 194, 230\}.$$

Thereafter, in 1984, Zhu [155] also used a recursive construction of SOLSSOMs similar to the one presented by Lindner *et al.* [91] in order to construct SOLSSOMs of orders 39, 87, 102, 194 and 230. By 1996 no further orders had been resolved, and a new design known as a *holey SOLSSOM (HSOLSSOM)* (see Colbourn *et al.* [38, §5.9]) caught the attention of researchers in the field of Latin squares. In this year Bennet and Zhu [16, 17] resolved the existence question of HSOLSSOMs for various orders, and in the process were able to construct a SOLSSOM of order 62 in [17] and SOLSSOMs of orders 46, 54 and 58 in [16]. The last authors to resolve the existence of SOLSSOMs for previously undecided orders were Abel *et al.* [1], who constructed SOLSSOMs of orders 66 and 70 in a 2000 paper on *incomplete* and *holey* SOLS (see Colbourn *et al.* [38, §5.3–5.4]). The list of unresolved orders was thus reduced to only orders 10 and 14, and at the time of writing this dissertation it was still not known whether SOLSSOMs of orders 10 and 14 exist. Table 3.8 gives a summary of the above discussion on the existence of SOLSSOMs.

A large number of constructions of SOLSSOMs have been proposed in the papers cited above, and others may also be found in Du [49] and Colbourn *et al.* [38, §5.7–5.8]. The following two theorems show how Mendelsohn's construction, given in Theorem 3.3.3, may be extended to also include a symmetric Latin square orthogonal to the constructed SOLS.

[9] See Burger *et al.* [31] for a very simple graph theoretic proof of the non-existence of a SOLS of order 6 .

Year	Orders resolved	Author(s)
1978	$n \notin \{10, 14, 39, 46, 51, 54, 58, 62, 66, 70, 74, 82, 87, 98, 102, 118, 123, 142, 159, 174, 183, 194, 202, 214, 219, 230, 258, 267, 278, 282, 303, 394, 398, 402, 422, 1322\}$	Wang [143]
1983	$n \notin \{10, 14, 39, 46, 54, 58, 62, 66, 70, 87, 102, 194, 230\}$	Lindner, Mullin & Stinson [91]
1984	$n \notin \{10, 14, 46, 54, 58, 62, 66, 70\}$	Zhu [155]
1996	$n \notin \{10, 14, 46, 54, 58, 66, 70\}$	Bennet & Zhu [17]
1996	$n \notin \{10, 14, 66, 70\}$	Bennet & Zhu [16]
2000	$n \notin \{10, 14\}$	Abel, Bennet, Zhang & Zhu [1]

TABLE 3.8: *Existence history of SOLSSOMs.*

Theorem 3.3.6 ([38], Construction 5.44) *Let p^q be any odd prime power, and let λ be any element of $(G, +, \times) = GF(p^q)$ except 0, 1 and 2^{-1}. Then $(\boldsymbol{L}, \boldsymbol{S})$ forms a SOLSSOM, where $\boldsymbol{L}$ represents the Cayley table of the self-orthogonal quasigroup $(G, \circ)$ in which $a \circ b = \lambda a + (1-\lambda)b$ for any two elements $a, b \in G$, while $\boldsymbol{S}$ represents the Cayley-table of the Abelian quasigroup $(G, \bullet)$ where $a \bullet b = 2^{-1}(a+b)$ for any two elements $a, b \in G$.*

Theorem 3.3.7 ([38], Construction 5.45) *Let $p^q \geq 4$ be any even prime power, and let λ be any element of $(G, +, \times) = GF(p^q)$ except 0 and 1. Then $(\boldsymbol{L}, \boldsymbol{S})$ forms a SOLSSOM, where $\boldsymbol{L}$ represents the Cayley table of the self-orthogonal quasigroup $(G, \circ)$ where $a \circ b = \lambda a + (1-\lambda)b$ for any two elements $a, b \in G$, while $\boldsymbol{S}$ represents the Cayley-table of the Abelian group $(G, +)$.*

For example, if $n = 7$ and $\lambda = 2$, then the pair of orthogonal Latin squares

$$\begin{bmatrix} 0&6&5&4&3&2&1 \\ 2&1&0&6&5&4&3 \\ 4&3&2&1&0&6&5 \\ 6&5&4&3&2&1&0 \\ 1&0&6&5&4&3&2 \\ 3&2&1&0&6&5&4 \\ 5&4&3&2&1&0&6 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0&4&1&5&2&6&3 \\ 4&1&5&2&6&3&0 \\ 1&5&2&6&3&0&4 \\ 5&2&6&3&0&4&1 \\ 2&6&3&0&4&1&5 \\ 6&3&0&4&1&5&2 \\ 3&0&4&1&5&2&6 \end{bmatrix}$$

forms a SOLSSOM of order 7, constructed using the method of Theorem 3.3.6. If $n = 4$, for example, the polynomials 0, 1, x and $x+1$ may be used to represent the elements of $GF(4)$, and if $\lambda = x$, then the pair of orthogonal Latin squares

$$\begin{bmatrix} 0 & 1+x & 1 & x \\ x & 1 & 1+x & 0 \\ 1+x & 0 & x & 1 \\ 1 & x & 0 & 1+x \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & x & 1+x \\ 1 & 0 & 1+x & x \\ x & 1+x & 0 & 1 \\ 1+x & x & 1 & 0 \end{bmatrix}$$

forms a SOLSSOM of order 4, constructed using the method of Theorem 3.3.7.

3.4 Chapter summary

This chapter contains a review of the application of Latin squares to the problem of scheduling various types of balanced sports tournaments. Round-robin tournaments were considered in §3.1, and the usefulness of representing such tournaments as Latin squares was highlighted using the problem of balancing carry-over effects in round robin tournaments as an example. A number of references were also provided for further reading on the application of Latin squares (as well as other combinatorial designs) to sports tournament scheduling.

Two types of mixed doubles tournaments, in particular, were considered in this chapter, namely *mixed doubles table tennis (MDTT) tournaments* in §3.2 and *spouse-avoiding mixed doubles round-robin (SAMDRR) tournaments* in §3.3. In §3.2.1 it was shown that an MDTT tournament schedule may be obtained by constructing a pair of orthogonal Latin squares, and that by constructing a third Latin square orthogonal to the first two, a resolvable MDTT tournament schedule may be obtained. In §3.2.2 a review was presented on constructions of sets of two and three mutually orthogonal Latin squares, and in particular a disproof from the literature was given of Euler's well-known conjecture that a pair of orthogonal Latin squares of order $n = 2 \pmod 4$ does not exist. A number of constructions of sets of three mutually orthogonal Latin squares were also presented, and the unresolved question of the existence of a set of three mutually orthogonal Latin squares of order 10 was highlighted.

In §3.3.1 it was shown that a SAMDRR tournament schedule may be obtained by constructing a SOLS, and that by constructing a symmetric Latin square which is orthogonal to this SOLS (*i.e.* a SOLSSOM), a resolvable SAMDRR tournament may be obtained. In §3.3.2 a review was presented on various constructions of SOLS, and the difficulties encountered in the construction of SOLSSOMs during the past 32 years was highlighted. In particular, it was mentioned that by the time of writing this dissertation it was still unknown whether SOLSSOMs of orders 10 and 14 exist; the former of these two questions is settled later in this dissertation.

CHAPTER 4

Enumeration methodology

Contents

In this chapter a number of methodologies for enumerating Latin squares and Latin square classes are presented. These methodologies include procedures for generating Latin squares by means of computer searches as well as theoretical counts via formulas derived from group theoretic results. The operations discussed in §2.3 are used in §4.1 to define various equivalence classes of Latin squares, and a standard notation for describing any equivalence class induced by a subset of the operations that may be applied to Latin squares without destroying their defining property is also presented. A number of important classes of Latin squares are also reviewed in this section. A brief historical background of Latin square enumeration is given in §4.2, highlighting the difficulty of the problem of counting Latin squares. In §4.3 a backtracking tree-search approach towards generating equivalence class representatives of Latin squares is described. An illustrative example is presented in order to clarify the working of the algorithm, followed by a discussion on how the algorithm may be implemented in order to enumerate certain classes of Latin squares and MOLS. In §4.4 a generalisation of a method from the literature on Latin squares is presented which may be used to compute stabilisers (see §A.2.2) for Latin squares under various operations, and further results from §A.2.2 are utilised in §4.5 to establish formulae which may be used to enumerate Latin squares and classes of Latin squares theoretically (*i.e.* without explicitly generating the squares).

4.1 Classes of Latin squares

In §2.3 it was shown that there are four operations which may be used to transform a Latin square $\boldsymbol{L}$ into another (not necessarily distinct) Latin square, namely a permutation on either the rows, columns or symbol set of $\boldsymbol{L}$, or a permutation on the elements of $T(\boldsymbol{L})$. Any combination of these operations which may be applied to a Latin square is henceforth referred to as a *transformation* of the Latin square. The *order* of the transformation is equal to the order of the Latin square and the Latin square resulting from the transformation α applied to a Latin square $\boldsymbol{L}$ is denoted by $\boldsymbol{L}^\alpha$. By the discussions of §2.3 any transformation of order n is a group action on the set of all Latin squares of order n, and the group acting on the set of all Latin squares of order n is henceforth referred to as the *transformation group*. By Definition A.2.8 this group action results in a number of orbits on the set of all Latin squares of order n which, by definition, are equivalence classes. Any equivalence class resulting from a transformation in this way is henceforth referred to as a *transformation class* of Latin squares of order n, and any transformation class containing a Latin square $\boldsymbol{L}$ is referred to as a *transformation class generated by* $\boldsymbol{L}$. Given a transformation group G, the stabiliser (see Definition A.2.9) of a Latin square $\boldsymbol{L}$ is called the *autotransformation group* of $\boldsymbol{L}$. The autotransformation group of $\boldsymbol{L}$ is therefore a subgroup H of G for which $\boldsymbol{L}^\alpha = \boldsymbol{L}$ for all $\alpha \in H$. Since a transformation is a mapping, two transformations α and β applied to a Latin square (in that order) may be denoted by their composition, namely $\beta\alpha$. Therefore, $(\boldsymbol{L}^\alpha)^\beta = \boldsymbol{L}^{\beta\alpha}$.

The *type* of a transformation will henceforth be specified as $(\pi_{t_1}, \ldots, \pi_{t_k}, \epsilon)$ where $t_i \in \{r, c, s, rc, rs, cs, rcs\}$, $1 \leq k \leq 3$ and $\epsilon \in \{\tau, \rho, \gamma, \tau\rho, \delta\}$. Here π represents a permutation of the order of the Latin square to which a transformation is applied, and any of the symbols r, c and s appearing in the subscript of π denote respectively a permutation applied to the rows, columns and symbols of the Latin square. If the symbol π_{rc} is present in the definition of the type of the transformation, for example, then the same permutation is to be applied to the rows and columns. The symbols τ, ρ, γ, $\tau\rho$ and δ represent the conjugate operations defined in §2.3, except for the symbol δ which represents the case where any conjugate operation may be applied to the Latin square. If the symbol $\tau\rho$ is present in the definition of the type of a transformation, for example, then the operation $\tau\rho$ may be applied to the Latin square, as well as the operations $\tau\gamma$ and ι, since $\tau\rho$ generates the subgroup $\{\iota, \tau\rho, \tau\gamma\}$ of D_3.

If a type of transformation σ specifies that some operation may be applied to a Latin square, then that operation is σ*-permissible*. The operation is also *permissible* by the specific symbol in σ which specifies that the operation may be used. A $(\pi_{t_1}, \ldots, \pi_{t_k}, \epsilon)$-transformation is henceforth denoted by a $(k+1)$-tuple $(p_1, p_2, \ldots, p_k, c)$, where p_i is the operation permissible by π_{t_i} and c the operation permissible by ϵ. It may also be noted that $(p_1, p_2, \ldots, p_k, c)$ is an element of the $(\pi_{t_1}, \ldots, \pi_{t_k}, \epsilon)$-transformation group.

A (π_{rc}, π_s, τ)-transformation, for instance, is an element (p, q, t) of the group $S_n^2 \times S_2$ applied to a Latin square $\boldsymbol{L}$, where p is applied to $R(\boldsymbol{L})$ and $C(\boldsymbol{L})$, q to $S(\boldsymbol{L})$ and the Latin square may be transposed (or not). The group $S_n^2 \times S_2$ is therefore the (π_{rc}, π_s, τ)-transformation group, and two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are in the same (π_{rc}, π_s, τ)-transformation class if two permutations, one applied to the rows and columns and one to the symbol set of $\boldsymbol{L}$ or $\boldsymbol{L}^T$, results in $\boldsymbol{L}'$. Other examples include a $(\pi_r, \pi_c, \pi_s, \tau\rho)$-transformation, where $S_n \wr \langle\tau\rho\rangle$ is the transformation group, and a $(\pi_r, \pi_c, \pi_s, \delta)$-transformation, where $S_n \wr D_3$ is the transformation group.

Some of the designs considered in this dissertation, such as MOLS, SOLS and SOLSSOMs, consist of tuples of special types of Latin squares satisfying some property relating the Latin squares to one another. For the purpose of classifying these types of Latin squares, a *Latin object*, denoted by $\mathcal{O} = (\boldsymbol{L}_1, \ldots, \boldsymbol{L}_m)$, is defined as an ordered list of m Latin squares of order n. The two parameters of a Latin object (namely the order of its members and its cardinality) are henceforth denoted by an ordered pair (n, m), where n is the order of the Latin squares in the object and m is the number of Latin squares in the object. For all $1 \leq j \leq m$, the type of transformation of a Latin object $\mathcal{O} = (\boldsymbol{L}_1, \ldots, \boldsymbol{L}_m)$ will include $\pi_{t_i}^{(j)}$ and/or $\epsilon^{(j)}$ if π_{t_i} and/or ϵ are present in the definition of the type of transformation for $\boldsymbol{L}_j$. If, for any two Latin squares $\boldsymbol{L}_k$ and $\boldsymbol{L}_\ell$ in $\mathcal{O}$, the permutations permissible by $\pi_{t_i}^{(k)}$ and $\pi_{t_j}^{(\ell)}$ are restricted to be equal for some t_i and t_j, then the symbol $\pi_{t_i}^{(k)}\pi_{t_j}^{(\ell)}$ is used to denote this restriction. In the special case where $t_i = t_j$, the notation $\pi_{t_i}^{(k,\ell)}$ is used instead. If the conjugate operations which may be applied to any two Latin squares $\boldsymbol{L}_k$ and $\boldsymbol{L}_\ell$ in $\mathcal{O}$ are permissible by the same element ϵ, then the notation $\epsilon^{(k,\ell)}$ is used. Finally, in the case of a k-MOLS of order n, the symbol δ will also be used to specify that a transformation may include any one of the $(k+2)!$ conjugate operations as discussed in §2.3.

For example, a $(\pi_r^{(1)}\pi_c^{(2)}, \pi_s^{(1)}, \rho^{(1)}, \tau^{(1,2)})$-transformation of the Latin object $(\boldsymbol{L}_1, \boldsymbol{L}_2)$ requires that if a permutation p is applied to the rows of $\boldsymbol{L}_1$, then p is to be applied to the columns of $\boldsymbol{L}_2$. A permutation applied to the symbols of $\boldsymbol{L}_1$, however, does not have such a requirement. Each row of $\boldsymbol{L}_1$ may be replaced by its inverse without applying any transformation to $\boldsymbol{L}_2$. However, if $\boldsymbol{L}_1$ is transposed, then it is required that $\boldsymbol{L}_2$ is also transposed. If a permutation applied to the rows of $\boldsymbol{L}_1$ required the same permutation to be applied to the rows of $\boldsymbol{L}_2$ (instead of the columns), then the transformation would have been a $(\pi_r^{(1,2)}, \pi_s^{(1)}, \rho^{(1)}, \tau^{(1,2)})$-transformation.

A transformation α applied to a Latin object $\mathcal{O}$ is henceforth denoted by $\mathcal{O}^\alpha$ and the set of transformations α for which $\mathcal{O}^\alpha = \mathcal{O}$ is the *α-autotransformation group* of that Latin object. A Latin object with parameters $(n, 1)$ is referred to simply as a Latin square.

The following definitions introduce the three most important classes of Latin squares, namely *isomorphism classes*, *isotopy classes* and *main classes*. Similar definitions of these classes may be found in Colbourn *et al.* [38, p. 136] and in Dénes and Keedwell [41, §4.1].

Definition 4.1.1 (Isomorphism) *An* isomorphism *of a Latin square is a (π_{rcs})-transformation, and an* isomorphism class *of Latin squares is a (π_{rcs})-transformation class of Latin squares. If two Latin squares are in the same isomorphism class, then they are* isomorphic*. The (π_{rcs})-autotransformation group of a Latin square is the* automorphism group *of that Latin square.* □

Hence two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are isomorphic, henceforth denoted by $\boldsymbol{L} \cong \boldsymbol{L}'$, if a single permutation $p \in S_n$ applied to the rows, columns and symbol set of $\boldsymbol{L}$ transforms it into $\boldsymbol{L}'$. Since p maps the triple $(i, j, \boldsymbol{L}(i,j)) \in T(\boldsymbol{L})$ to the triple $(p(i), p(j), p(\boldsymbol{L}(i,j))) \in T(\boldsymbol{L}')$, an isomorphism between two Latin squares is equivalent to an isomorphism between their underlying quasigroups. The two Latin squares

$$\boldsymbol{L}_{4.1} = \begin{bmatrix} 0&3&1&2\\ 1&2&0&3\\ 3&0&2&1\\ 2&1&3&0 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{4.2} = \begin{bmatrix} 1&2&0&3\\ 2&1&3&0\\ 3&0&2&1\\ 0&3&1&2 \end{bmatrix}$$

are isomorphic since the isomorphism $p = \binom{0\,1\,2\,3}{1\,3\,2\,0}$ maps $\boldsymbol{L}_{4.1}$ to $\boldsymbol{L}_{4.2}$.

An isomorphism p from a Latin square $\boldsymbol{L}$ to a Latin square $\boldsymbol{L}'$ also induces the relationship $p \circ \boldsymbol{L}(i) \circ p^{-1} = \boldsymbol{L}'(p(i))$ between the rows of the two Latin squares (see §2.3). Hence each row in $\boldsymbol{L}$ is a conjugate permutation[1] of some row in $\boldsymbol{L}'$, and by Proposition A.1.2 it therefore follows that an isomorphism preserves the cycle structures of the rows.

[1] See §A.1 for the definitions of permutation cycles and conjugate permutations.

The Latin square

$$\boldsymbol{L}_{4.3} = \begin{bmatrix} 0&1&2&3 \\ 1&2&3&0 \\ 2&3&0&1 \\ 3&0&1&2 \end{bmatrix}$$

is therefore not isomorphic to $\boldsymbol{L}_{4.1}$ since the first row of $\boldsymbol{L}_{4.3}$ contains only fixed points while $\boldsymbol{L}_{4.1}$ contains no row with such a cycle structure.

If a property exhibited by a Latin square is preserved (as above, for instance) by a transformation, then the property is said to be *invariant* under that specific transformation. In other words, if one Latin square in a transformation class exhibits a property invariant under that class, then all Latin squares in the class exhibit that property. Class invariant properties may therefore be used (as above) to show that two Latin squares are not in the same class.

The following class may be seen as a natural generalisation of an isomorphism class.

Definition 4.1.2 (Isotopy) *An* isotopism *of a Latin square is a (π_r, π_c, π_s)-transformation, and an* isotopy class *of Latin squares is a (π_r, π_c, π_s)-transformation class of Latin squares. If two Latin squares are in the same isotopy class, then they are* isotopic. *The (π_r, π_c, π_s)-autotransformation group of a Latin square is the* autotopy group *of that Latin square.* □

Two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are therefore isotopic, henceforth denoted by $\boldsymbol{L} \simeq \boldsymbol{L}'$, if there exists a transformation $(p_r, p_c, p_s) \in S_n^3$ (where p_r is applied to $R(\boldsymbol{L})$, p_c to $C(\boldsymbol{L})$ and p_s to $S(\boldsymbol{L})$) that transforms $\boldsymbol{L}$ into $\boldsymbol{L}'$. The Latin squares $\boldsymbol{L}_{2.11}$ and $\boldsymbol{L}_{2.12}$ in §2.3 are isotopic since the isotopism $\left(\binom{0\,1\,2\,3}{1\,2\,3\,0}, \binom{0\,1\,2\,3}{2\,3\,0\,1}, \binom{0\,1\,2\,3}{1\,0\,3\,2}\right)$ maps $\boldsymbol{L}_{2.11}$ to $\boldsymbol{L}_{2.12}$, as discussed in that subsection.

An example of an isotopy class invariant is the number of intercalates of a Latin square. An *intercalate* in a Latin square $\boldsymbol{L}$ is an ordered quadruple $(i, j, k, \ell) \in \mathbb{Z}_n^4$ for which $\boldsymbol{L}(i,k) = \boldsymbol{L}(j,\ell)$ and $\boldsymbol{L}(i,\ell) = \boldsymbol{L}(j,k)$; in other words, it is a 2×2 subsquare of a Latin square. An example of an intercalate in the Latin square

$$\boldsymbol{L}_{4.4} = \begin{bmatrix} 0&1&\mathbf{2}&\mathbf{3}&4 \\ 1&4&\mathbf{3}&\mathbf{2}&0 \\ 2&0&4&1&3 \\ 3&2&0&4&1 \\ 4&3&1&0&2 \end{bmatrix}$$

is $(0,1,2,3)$ (since $\boldsymbol{L}(0,2) = \boldsymbol{L}(1,3) = 2$ and $\boldsymbol{L}(0,3) = \boldsymbol{L}(1,2) = 3$), as shown in boldface above. Consider applying an isotopism (p_r, p_c, p_s) to a Latin square $\boldsymbol{L}$ with intercalate (i,j,k,ℓ). Since $\boldsymbol{L}(i,k) = \boldsymbol{L}(j,\ell)$ and $\boldsymbol{L}(i,\ell) = \boldsymbol{L}(j,k)$, it follows that $\boldsymbol{L}(p_r(i), p_c(k)) = \boldsymbol{L}(p_r(j), p_c(\ell))$ and $\boldsymbol{L}(p_r(i), p_c(\ell)) = \boldsymbol{L}(p_r(j), p_c(k))$, and the intercalate (i,j,k,ℓ) is mapped to the intercalate $(p_r(i), p_r(j), p_c(k), p_c(\ell))$. No intercalate is therefore destroyed by any isotopism, and so the number of intercalates is preserved by an isotopism. It is a simple task to verify that the Latin square

$$\boldsymbol{L}_{4.5} = \begin{bmatrix} 0&1&2&3&4 \\ 1&2&3&4&0 \\ 2&3&4&0&1 \\ 3&4&0&1&2 \\ 4&0&1&2&3 \end{bmatrix}$$

contains no intercalates and is therefore not isotopic to $\boldsymbol{L}_{4.4}$.

The following class is the largest class of Latin squares in the sense that it includes all the operations discussed in §2.3, and this class may be defined not only for Latin squares, but also for MOLS.

Definition 4.1.3 (Main class) *A* paratopism *of a k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n is a $(\pi_r^{(0,1,\ldots,k-1)}, \pi_c^{(0,1,\ldots,k-1)}, \pi_s^{(0)}, \pi_s^{(1)}, \ldots, \pi_s^{(k-1)}, \delta)$-transformation, and a* main class *of k-MOLS of order n is a $(\pi_r^{(0,1,\ldots,k-1)}, \pi_c^{(0,1,\ldots,k-1)}, \pi_s^{(0)}, \pi_s^{(1)}, \ldots, \pi_s^{(k-1)}, \delta)$-transformation class. If two k-MOLS of order n are in the same main class, then they are* paratopic*. The $(\pi_r^{(0,1,\ldots,k-1)}, \pi_c^{(0,1,\ldots,k-1)}, \pi_s^{(0)}, \pi_s^{(1)}, \ldots, \pi_s^{(k-1)}, \delta)$-autotransformation group of a k-MOLS of order n is the* autoparatopy group *of that k-MOLS.* $\square$

Hence a paratopism of a k-MOLS of order n potentially consists of all possible operations that may be applied to it in order to obtain another k-MOLS of order n as a result. Furthermore, a Latin square $\boldsymbol{L}$ is paratopic to a Latin square $\boldsymbol{L}'$, henceforth denoted by $\boldsymbol{L} \sim \boldsymbol{L}'$, if $\boldsymbol{L}$ is isotopic to any conjugate of $\boldsymbol{L}'$.

The number of intercalates of a Latin square is also paratopism-invariant. Let (i, j, k, ℓ) be an intercalate of a Latin square $\boldsymbol{L}$ for which $\boldsymbol{L}(i, k) = a = \boldsymbol{L}(j, \ell)$ and $\boldsymbol{L}(i, \ell) = b = \boldsymbol{L}(j, k)$. The intercalate may alternatively be represented by the four triples (i, k, a), (j, ℓ, a), (i, ℓ, b) and (j, k, b), which satisfy the necessary condition (for these triples to form an intercalate) that each pair of triples has only one element in common. It is easy to see that if any permutation is applied to these triples (hence if a conjugate operation is applied to the Latin square), then the resulting four triples still satisfy the necessary condition and therefore form an intercalate in the resulting Latin square. The Latin squares $\boldsymbol{L}_{4.4}$ and $\boldsymbol{L}_{4.5}$ are therefore non-paratopic.

An isomorphism is simply an isotopism (p_r, p_c, p_s) for which $p_r = p_c = p_s$ and an isotopism is simply a paratopism (p_r, p_c, p_s, c) for which $c = e$ (representing the identity conjugate operation). Hence, for any two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$, if $\boldsymbol{L} \cong \boldsymbol{L}'$ then $\boldsymbol{L} \simeq \boldsymbol{L}'$ and if $\boldsymbol{L} \simeq \boldsymbol{L}'$ then $\boldsymbol{L} \sim \boldsymbol{L}'$. Each main class of Latin squares is therefore a union of disjoint isotopy classes, each of which is, in turn, a union of disjoint isomorphism classes. Consequently, a main class is also a union of disjoint isomorphism classes. In fact, any transformation is a special case of a paratopism, and hence a main class is a union of σ-transformation classes for any transformation type σ. It is interesting to note that an isotopy class consisting of a Latin square which is the Cayley table of a group consists of a single isomorphism class. This follows from the fact that two isotopic groups are isomorphic (see Corollary 2 in Dénes and Keedwell [41, p. 27]).

The following transformation classes are of particular interest in this dissertation.

Definition 4.1.4 (CS-paratopy class) *A* CS-paratopism *of a Latin square is a (π_r, π_{cs}, ρ)-transformation, and a* CS-paratopy class *of Latin squares is a (π_r, π_{cs}, ρ)-transformation class of Latin squares. If two Latin squares are in the same CS-paratopy class, then they are* CS-paratopic*. The (π_r, π_{cs}, ρ)-autotransformation group of a Latin square is the* CS-autoparatopy group *of that Latin square.* $\square$

The next definition is a special case of the above definition.

Definition 4.1.5 (Row-isomorphism class) *A* row-isomorphism *of a Latin square is a (π_{rcs}, ρ)-transformation, and a* row-isomorphism class *of Latin squares is a (π_{rcs}, ρ)-transformation class of Latin squares. If two Latin squares are in the same row-isomorphism class, then they are* row-isomorphic*. The (π_{rcs}, ρ)-autotransformation group of a Latin square is the* row-automorphism group *of that Latin square.* $\square$

Hence two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are CS-paratopic if two permutations, one applied to the columns and symbols, and one applied to the rows of $\boldsymbol{L}$ or $\boldsymbol{L}^{-1}$, results in $\boldsymbol{L}'$. If the two permutations are equal, then $\boldsymbol{L}$ and $\boldsymbol{L}'$ are row-isomorphic. It has been noted in §2.3 that if a permutation p is applied to the columns and symbols of a Latin square, then any row r of this Latin square is mapped to $p \circ r \circ p^{-1}$, *i.e.* one of its conjugate permutations. Also, any permutation and its inverse permutation have the same cycle structure. A CS-paratopism therefore preserves the cycle structures of the rows of a Latin square. Furthermore, it is the most general transformation with this property in the sense that any operation added to the definition of a CS-paratopism does not guarantee that the cycle structures of the rows are preserved. Similar transformations may be defined if the prefixes "CS" and "(π_r, π_{cs}, ρ)" in Definition 4.1.4 are replaced by "RS" and "$(\pi_{rs}, \pi_c, \gamma)$," or by "RC" and "$(\pi_{rc}, \pi_s, \tau)$," respectively. These three definitions, however, are equivalent by the following proposition.

Proposition 4.1.1 *For any two Latin squares $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$ the following are equivalent:*

(1) $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$ are CS-paratopic,

(2) $\boldsymbol{L}_1^T$ and $\boldsymbol{L}_2^T$ are RS-paratopic,

(3) ${}^{-1}\boldsymbol{L}_1$ and ${}^{-1}\boldsymbol{L}_2$ are RC-paratopic.

Proof: It is easy to see that the following are equivalent for all $i, j \in \mathbb{Z}_n$ by simply performing the appropriate conjugate operations on the triples (where $p, q \in S_n$):

(1) $(i, j, k) \in T(\boldsymbol{L}_1)$ and either $(p(i), q(j), q(k)) \in T(\boldsymbol{L}_2)$ or $(p(i), q(k), q(j)) \in T(\boldsymbol{L}_2)$,

(2) $(j, i, k) \in T(\boldsymbol{L}_1^T)$ and either $(q(j), p(i), q(k)) \in T(\boldsymbol{L}_2^T)$ or $(q(k), p(i), q(j)) \in T(\boldsymbol{L}_2^T)$,

(3) $(k, j, i) \in T({}^{-1}\boldsymbol{L})$ and either $(q(k), q(j), p(i)) \in T({}^{-1}\boldsymbol{L}_2)$ or $(q(j), q(k), p(i)) \in T({}^{-1}\boldsymbol{L}_2)$.

The proposition follows by the actions of p and q on the triples in each of these three cases. ∎

The prefixes "row" and "(π_{rcs}, ρ)" in Definition 4.1.5 may also be replaced by "column" and "(π_{rcs}, γ)," or by "transpose" and "(π_{rcs}, τ)," respectively. Since these transformations are special cases of CS-paratopisms and RC-paratopisms respectively, the above proposition is true for these classes as well.

4.2 Historical background on the enumeration of Latin squares

In this section a brief historical account is given of the problem of enumerating Latin squares (*i.e.* determining the number of distinct ways to construct a Latin square of a given order). A more detailed historical account of the research activities in this area before 1974 may, however, be found in Dénes and Keedwell [41, §4.3], while Norton [112] gives an even more detailed description of activities in the area of Latin square enumeration before 1939. A historical background on Latin square enumeration has also been given by McKay *et al.* [99].

In 1782 Euler [52] not only considered the problem of constructing pairs of orthogonal Latin squares (as discussed in §1.1 and §3.2.2), but also touched on the problem of enumerating Latin squares, a difficult problem that has since received almost as much attention in the literature as the problem of constructing sets of mutually orthogonal Latin squares. Euler found that there is only one reduced Latin square of orders 1, 2 and 3, while there are four reduced Latin squares of order 4 and 56 reduced Latin squares of order 5. He also attempted to enumerate reduced Latin squares of order 6, but without success.

The problem of enumerating Latin squares then remained untouched until Cayley [37] and Frolov [59] independently considered the problem in 1890. Cayley verified the numbers of reduced Latin squares up to order 5 obtained by Euler, and remarked on the difficulty of finding a simple formula for the number of Latin squares of any order. Frolov, on the other hand, attempted to enumerate reduced Latin squares of orders 6 and 7, counting 9 408 reduced Latin squares of order 6 and 221 276 160 of order 7, while also providing two recurrence relations for the number of Latin squares of any order. It was later found, however, that both his formulae were in error, and that the number of reduced Latin squares of order 7 was incorrect (see Dénes and Keedwell [41, pp. 139–140] for more detail).

As briefly mentioned in §1.1 and §3.2.2, Tarry [136] proved the non-existence of a pair of orthogonal Latin squares of order 6 by classifying all Latin squares of order 6 into classes. These classes were $(\pi_r, \pi_c, \pi_s, \tau)$-transformation classes [41] (*i.e.* two Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ are in the same class if $\boldsymbol{L}'$ is isotopic to either $\boldsymbol{L}$ or $\boldsymbol{L}^T$), and Tarry counted 17 of these classes. Exactly five of these classes contained Latin squares none of which is isotopic to its transpose, and these five $(\pi_r, \pi_c, \pi_s, \tau)$-transformation classes therefore constitute ten isotopy classes. The remaining 12 $(\pi_r, \pi_c, \pi_s, \tau)$-transformation classes contain only Latin squares which are isotopic to their transposes, and these classes are therefore simply isotopy classes. Hence there are 22 isotopy classes of Latin squares of order 6. These numbers determined for Latin squares of order 6 were later verified by Fisher and Yates [57] in 1934, who (possibly unaware of Tarry's work) also counted 9 408 reduced Latin squares of order 6, 22 isotopy classes and 17 $(\pi_r, \pi_c, \pi_s, \tau)$-transformation classes (which they referred to as "families" of Latin squares). They also established the important and useful relationship between the number of Latin squares and the number of reduced Latin squares of any given order, namely that the number of Latin squares of order n is $n!(n-1)!$ times the number of reduced Latin squares of order n (the proof of this fact is recounted later in this dissertation).

In 1939 Norton [112] attempted the enumeration of Latin squares of order 7, and counted 146 main classes, 562 isotopy classes and 16 927 968 reduced Latin squares of order 7. He was, however, not able to prove that these 146 main classes are exhaustive, and conjectured that any Latin square of order 7 lies in one of these classes. A disproof to his conjecture was only presented much later, in 1951, by Sade [126], who determined that Norton omitted a single main class of Latin squares of order 7, which contains two isotopy classes and 14 112 reduced Latin squares. Sade then gave the correct number of main classes and isotopy classes of Latin squares of order 7 as 147 and 564, respectively, and the number of reduced Latin squares as 16 942 080 (see Dénes and Keedwell [41, pp. 142–143] for more detail on Sade's enumeration methods).

The next step, namely enumerating Latin squares of order 8, was only taken much later, in 1967, by Wells [146] who used a computer adaptation of Sade's method in order to determine that there are 535 281 401 856 reduced Latin squares of order 8. Wells also estimated that there are over a quarter of a million main classes of Latin squares of this order. Shortly thereafter, in 1968, Brown [25] incorrectly enumerated the isotopy classes of Latin squares of order 8 as 1 676 257, and also incorrectly quoted the number of isotopy classes of Latin squares of order 7 (as 563, where Norton counted 562 and Sade 564), two errors which unfortunately made their way into the authoritative work by Dénes and Keedwell [41] in 1974. The number of isotopy classes of Latin squares of order 8 was only corrected in 1990 by Kolesova *et al.* [85], who correctly enumerated 1 676 267 isotopy classes.

Latin squares of order 9 were enumerated in 1975 by Bammel and Rothstein [13], who gave the number of reduced Latin squares of this order as 377 597 570 964 258 816, and estimated that there are more than 10^{10} main classes of Latin squares of order 9. Latin squares of order 10 were enumerated by McKay and Rogoyski [100] in 1995, and estimates were given by these authors for the number of Latin squares of orders larger than 10 up to and including order 15, while McKay *et al.* [99] established the number of main classes of Latin squares, isotopy classes of Latin squares, isomorphism classes of Latin squares and isomorphism classes of reduced Latin squares of orders $1 \leq n \leq 10$. McKay *et al.* obtained their results by utilising the number of reduced Latin squares of orders $1 \leq n \leq 10$ together with various results from group theory, as will be discussed later in this chapter.

The largest order for which enumeration results have thus far been published is order 11. Reduced Latin squares of order 11 were enumerated by McKay and Wanless [102] in 2005, while the numbers of various classes of Latin squares of order 11 were determined by Hulpke *et al.* [78] in 2010. In particular, Hulpke *et al.* enumerated distinct Latin squares, reduced Latin squares, isomorphism classes of Latin squares, isomorphism classes of reduced Latin squares, isotopy classes of Latin squares and main classes of Latin squares of order 11.

The numbers of various classes of Latin squares of orders $2 \leq n \leq 11$ are given in Table 4.1, and these numbers may also be found in Tables 1.16 and 1.24 of Colbourn *et al.* [38], as well as in the *Online Encyclopedia of Integer Sequences (OEIS)* [129]. If a sequence appears in OEIS, the sequence number for each class of Latin squares is given together with the class name in Table 4.1.

In most work on the enumeration of Latin squares, Latin rectangles[2] were also enumerated, as was done by, for instance, McKay and Rogoyski [100] and by McKay and Wanless [102], and these numbers may also be found in Table 1.24 of Colbourn *et al.* [38]. A number of formulae for the number of Latin squares have also been given (see, for instance, Shao and Wie [128], Stones [134], and Dénes and Keedwell [41, §4.3]), but these formulae are not in closed form and implementing them are often computationally more expensive than performing a brute force count. Formulae for the number of $3 \times n$ Latin rectangles were also proposed by Gessel [62, 63], and asymptotic enumeration results for the number of Latin rectangles of order n were given by Erdös and Kaplansky [51] in 1946, by Yamamoto [151] in 1951, by Stein [130] in 1978 and by Godsil and McKay [64] in 1984.

Some work has also been done on the enumeration of sets of orthogonal Latin squares. Owens and Preece [113], for example, determined in 1995 that there are 19 σ-transformation classes of 8-MOLS of order 9, where σ permits a permutation applied to the rows and columns of all eight squares, as well as eight permutations applied to the symbol sets of each of the Latin squares in the set independently. Their results are tabulated in Table 3.77 of Colbourn *et al.* [38]. A list of main class representatives of 2-MOLS (*i.e.* Graeco-Latin squares) was also given by McKay [98] for orders $3 \leq n \leq 8$, while Graham and Roberts [66] enumerated distinct SOLS, idempotent SOLS and isomorphism classes of idempotent SOLS of orders $4 \leq n \leq 9$ in 2006. The latter work will be discussed in more detail in the next chapter.

4.3 Exhaustive enumeration of Latin square classes

The most popular means of exhaustive enumeration of combinatorial objects is the use of backtracking search trees, sometimes also referred to as *recursive backtracking* (see, for instance, Edmonds [50, §17] for the use of this term in particular as well as a discussion and examples

[2]A *Latin rectangle* is a $k \times n$ array in which each symbol from a set of n^2 symbols appears exactly once in each row and at most once in each column. A more formal definition is given later in this chapter.

n	Distinct Latin squares of order n (#A002860)
2	2
3	12
4	576
5	161 280
6	812 851 200
7	61 479 419 904 000
8	108 776 032 459 082 956 800
9	5 524 751 496 156 892 842 531 225 600
10	9 982 437 658 213 039 871 725 064 756 920 320 000
11	776 966 836 171 770 144 107 444 346 734 230 682 311 065 600 000

n	Isomorphism classes of Latin squares of order n
2	1
3	5
4	35
5	1 411
6	1 130 531
7	12 198 455 835
8	2 697 818 331 680 661
9	15 224 734 061 438 247 321 497
10	2 750 892 211 809 150 446 995 735 533 513
11	19 464 657 391 668 924 966 791 023 043 937 578 299 025

n	Reduced Latin squares (#A000315)	Isomorphism classes of reduced squares
2	1	1
3	1	1
4	4	2
5	56	6
6	9 408	109
7	16 942 080	23 746
8	535 281 401 856	106 228 849
9	377 597 570 964 258 816	9 365 022 303 540
10	7 580 721 483 160 132 811 489 280	20 890 436 195 945 769 617
11	5 363 937 773 277 371 298 119 673 540 771 840	1 478 157 455 158 044 452 849 321 016

n	Isotopy classes of Latin squares (#A040082)	Main classes of Latin squares (#A003090)
2	1	1
3	1	1
4	2	2
5	2	2
6	22	12
7	564	147
8	1 676 267	283 657
9	115 618 721 533	19 270 853 541
10	208 904 371 354 363 006	34 817 397 894 749 939
11	12 216 177 315 369 229 261 482 540	2 036 029 552 582 883 134 196 099

TABLE 4.1: *Enumeration results for various classes of Latin squares of order $2 \leq n \leq 11$, together with sequence numbers where the sequences of number appear in the Online Encyclopedia of Integer Sequences [129].*

on the topic). In addition to enumerating all possible instances of a combinatorial object, this method also generates each object counted, and provides a means of cataloguing the objects in a repository.

Progression of the method may be described by means of a tree, where each vertex in the tree represents a partially completed object. The root of the tree represents an initial partially completed object (usually an empty object) and the branches of the tree represent all possible extensions (in some sense) of the partially completed object to a larger object (*i.e.* an object closer to a completed object). The leaves of the tree represent either completed objects or partially completed objects for which there are no extensions to larger partially completed objects. The leaves representing completed objects therefore represent all possible completions of the partially completed object represented by the root of the tree.

In what follows it is necessary to define the concept of a partially completed Latin square. A *partial Latin square* of order n is an $n \times n$ array containing at most one symbol from $\mathbb{Z}_n$ in each position and each symbol from $\mathbb{Z}_n$ at most once in each row and column, and a *Latin rectangle* of order n with m rows is an $m \times n$ array (where $m \leq n$) in which each symbol from $\mathbb{Z}_n$ appears exactly once in each row and at most once in each column (see, for instance, Colbourn *et al.* [38, p. 141 & p. 146] for these definitions). Hence a Latin rectangle is a special case case of a partial Latin square. A *completion* of a partial Latin square $\boldsymbol{P}$ is a Latin square $\boldsymbol{L}$ for which $\boldsymbol{L}(i,j) = \boldsymbol{P}(i,j)$ if $\boldsymbol{P}(i,j)$ is not empty, for all $i, j \in \mathbb{Z}_n$.

Latin squares may be enumerated by branching on the inclusion of either rows, columns or universals in a partial Latin square of order n, in which case the tree has n levels. It may be noted, however, that each universal U in a Latin square $\boldsymbol{L}$ corresponds to a row in ${}^{-1}\boldsymbol{L}$. Since $\boldsymbol{L}(i,j) = k$ for every element $(i,j) \in U$ and some $k \in \mathbb{Z}_n$, it holds that ${}^{-1}\boldsymbol{L}(k,j) = i$ for every element $(i,j) \in U$, and therefore U represents row k in ${}^{-1}\boldsymbol{L}$. Hence, for some partial Latin square $\boldsymbol{L}$, if $\boldsymbol{L}_1, \boldsymbol{L}_2, \ldots, \boldsymbol{L}_m$ are the leaves on the $(n-1)$-st level of the tree with root $\boldsymbol{L}$ (on the 0-th level) when branching on the inclusion of universals, then ${}^{-1}\boldsymbol{L}_1, {}^{-1}\boldsymbol{L}_2, \ldots, {}^{-1}\boldsymbol{L}_m$ are the leaves on the $(n-1)$-st level of the tree with root ${}^{-1}\boldsymbol{L}$ when branching on the inclusion of rows. Similarly, branching on the inclusion of universals in $\boldsymbol{L}$ is equivalent to branching on the inclusion of columns in $\boldsymbol{L}^{-1}$, and *vice verca*. It follows that all three approaches are equivalent in the sense that the output of one may be derived from the output of another.

Branching on the inclusion of rows is discussed here, in which case each verticex of the tree represents a Latin rectangle. The method is generalised not only to count Latin squares, but Latin squares satisfying a set of properties $\mathbb{P}$. Hence on each level the tree branches on the inclusion of a row only if the inclusion of that row does not destroy any of the properties in $\mathbb{P}$. The method is given in pseudo code form as Algorithm 4.1.

Step 6 of Algorithm 4.1 is clearly computationally the most complex step since an exhaustive list of possible rows has to be generated. One way of achieving this is to generate a list of rows, no element of which destroys the latinness when inserted into the current Latin rectangle, and thereafter testing for each row whether its insertion into the current Latin rectangle satisfies all the properties in $\mathbb{P}$. Given an $m \times n$ Latin rectangle $\boldsymbol{L}$, all possibilities for the $(m+1)$-st row are simply all possible SDRs[3] of $(\mathbb{Z}_n \backslash \ell_0, \mathbb{Z}_n \backslash \ell_1, \ldots, \mathbb{Z}_n \backslash \ell_{n-1})$, where ℓ_i denotes the set $\{\boldsymbol{L}(0,i), \boldsymbol{L}(1,i), \ldots, \boldsymbol{L}(m-1,i)\}$ for all $0 \leq i \leq n-1$, *i.e.* the i-th column of $\boldsymbol{L}$. For instance, consider the 2×4 Latin rectangle

$$\boldsymbol{L}_{4.6} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{bmatrix}.$$

[3]A *system of distinct representatives (SDR)* of a family of sets $\{S_1, S_2, \ldots, S_n\}$ is an n-tuple $(s_1, s_2, \ldots, s_n)$ for which $s_i \in S_i$ for all $1 \leq i \leq n$ and $s_i \neq s_j$ for $i \neq j$.

Algorithm 4.1 ExhaustiveTreeSearch

Input: A Latin rectangle $\boldsymbol{L}$ which satisfies all properties in a set $\mathbb{P}$.
Output: All possible completions of $\boldsymbol{L}$ to Latin squares satisfying all properties in $\mathbb{P}$.

$m \leftarrow$ the number of rows of $\boldsymbol{L}$
$n \leftarrow$ the number of columns of $\boldsymbol{L}$
if $m = n$ **then**
  print $\boldsymbol{L}$
else
  $R \leftarrow$ the set of all possibilities for row $m+1$ that contradicts no property in $\mathbb{P}$ nor destroys the latinness when inserted into $\boldsymbol{L}$
  if $R \neq \emptyset$ **then**
    for all $r_i \in R$ **do**
      $\boldsymbol{L}' \leftarrow r_i$ inserted as row $m+1$ in $\boldsymbol{L}$
      ExhaustiveTreeSearch($\boldsymbol{L}'$)
    end for
  end if
end if

The only SDRs of the tuple $(\{2,3\},\{0,3\},\{0,1\},\{1,2\})$ are $(2,3,0,1)$, and $(3,0,1,2)$, and these are therefore the only possibilities for a third row in any extension of $\boldsymbol{L}_{4.6}$. The idea of extending Latin rectangles via SDRs is discussed by Dénes and Keedwell [42, §8.2] and by Roberts and Tesman [121, §12.2.2], while Hall [68] used this idea to prove that any Latin rectangle may be extended in at least one way to a Latin square.

As an example of how Algorithm 4.1 may be used, consider enumerating reduced Latin squares of order 5 without any intercalates. The number of reduced Latin squares without intercalates (commonly known as N_2-*squares* [38, p. 144]) has been enumerated by McKay and Wanless [101] up to and including order 9, and the results are listed as sequence A000611 in Sloane [129]. According to their results, there are six distinct reduced N_2-squares of order 5. In order for Algorithm 4.1 to generate these reduced Latin squares, the initial partial Latin square may be taken as

$$\begin{bmatrix} 0 & 1 \; 2 \; \ldots \; n-1 \\ 1 & \\ 2 & \\ \vdots & \\ n-1 & \end{bmatrix}.$$

If this partial Latin square represents the root of the tree, then all the leaves on the $(n-1)$-st level of the tree represent reduced Latin squares. Figure 4.1 shows the progression of the search if the above partial Latin square with $n = 5$ is given as input to Algorithm 4.1 and if $\mathbb{P}$ prohibits any intercalates. Here all vertices on the i-th level of the tree represent partial Latin squares without intercalates and with rows 0 to i filled, and each branch from a vertex on level i represents a possible completion of row $i+1$, for $i = 0,1,2,3,4$.

For instance, the root vertex represents the partial Latin square

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & & & & \\ 2 & & & & \\ 3 & & & & \\ 4 & & & & \end{bmatrix},$$

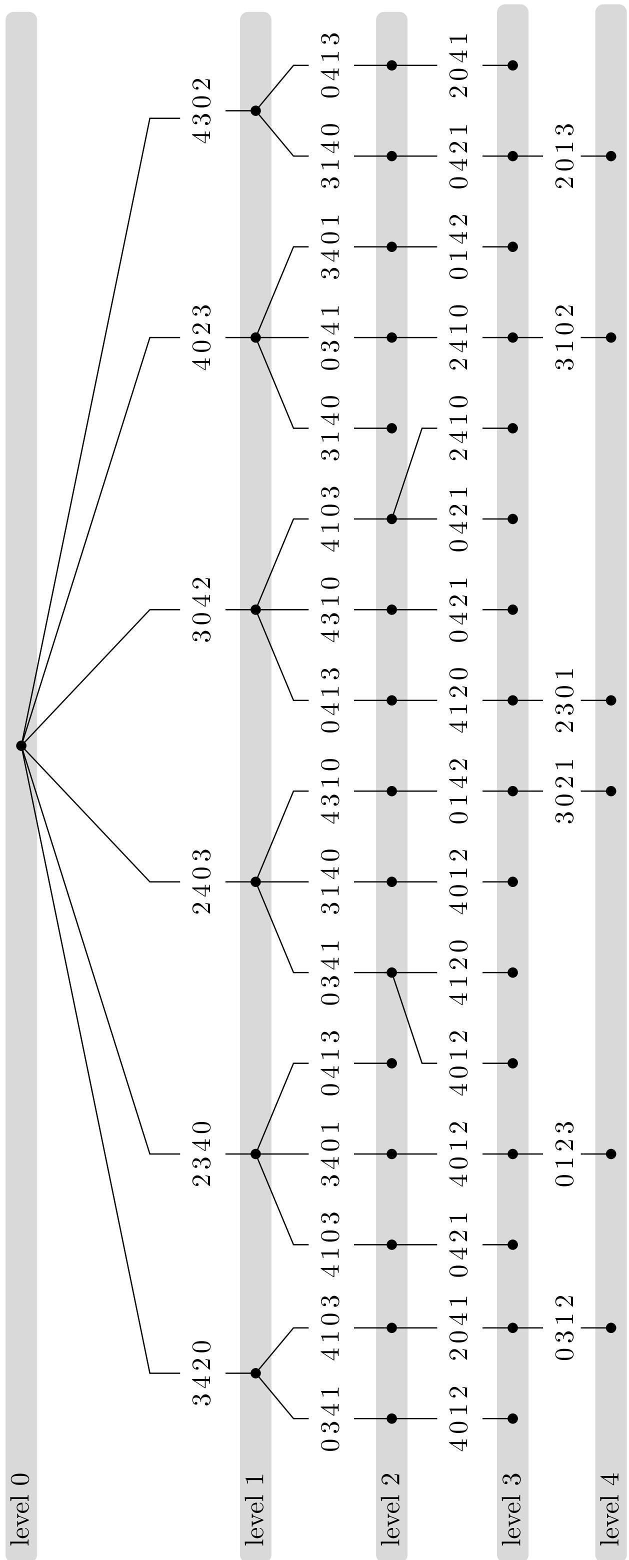

FIGURE 4.1: *A search tree for reduced Latin squares of order 5 containing no intercalates. The root vertex represents a partial Latin square which is empty, except for the first row and first column which are both in natural order. Each branch represents the inclusion of another row in the current partial Latin square, and the six leaves on the 5-th level represent the six distinct reduced Latin squares of order 5 containing no intercalates.*

while the left-most vertex on level 3 represents the partial Latin square

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 & 0 \\ 2 & 0 & 3 & 4 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & & & & \end{bmatrix}.$$

The only possible completion of row 4 in the above partial Latin square is 2 1 0 3. This, however, is not allowed since it will result in the intercalate $(3, 4, 2, 3)$ containing the symbols 0 and 1. The six leaves on level 4 of this tree represent the six distinct reduced N_2-squares mentioned previously, which are shown in Table 4.2. Furthermore, this number agrees with the number found by McKay and Wanless [101].

$$\begin{bmatrix} 0&1&2&3&4 \\ 1&3&4&2&0 \\ 2&4&1&0&3 \\ 3&2&0&4&1 \\ 4&0&3&1&2 \end{bmatrix} \quad \begin{bmatrix} 0&1&2&3&4 \\ 1&2&3&4&0 \\ 2&3&4&0&1 \\ 3&4&0&1&2 \\ 4&0&1&2&3 \end{bmatrix} \quad \begin{bmatrix} 0&1&2&3&4 \\ 1&2&4&0&3 \\ 2&4&3&1&0 \\ 3&0&1&4&2 \\ 4&3&0&2&1 \end{bmatrix} \quad \begin{bmatrix} 0&1&2&3&4 \\ 1&3&0&4&2 \\ 2&0&4&1&3 \\ 3&4&1&2&0 \\ 4&2&3&0&1 \end{bmatrix} \quad \begin{bmatrix} 0&1&2&3&4 \\ 1&4&0&2&3 \\ 2&0&3&4&1 \\ 3&2&4&1&0 \\ 4&3&1&0&2 \end{bmatrix} \quad \begin{bmatrix} 0&1&2&3&4 \\ 1&4&3&0&2 \\ 2&3&1&4&0 \\ 3&0&4&2&1 \\ 4&2&0&1&3 \end{bmatrix}$$

TABLE 4.2: *The six reduced N_2-squares (Latin squares without intercalates) of order 5.*

Given a transformation of type σ, one of the properties in $\mathbb{P}$ might be that the Latin square should be restricted to be the lexicographically smallest Latin square in its σ-transformation class, where the lexicographical ordering is defined in such a way that there is only one smallest square in each such class. Hence Algorithm 4.1 will produce exactly one Latin square satisfying all the other properties of $\mathbb{P}$ from each σ-transformation class, thereby enumerating the number of σ-transformation classes of Latin squares satisfying all other properties of $\mathbb{P}$. This method is known as *orderly generation* [97], and it is a common method used for the enumeration of combinatorial objects. See Faradžev [54] and Read [120] for more general discussions of this method.

A Latin square $\boldsymbol{L}$ is *lexicographically smaller* than a Latin square $\boldsymbol{L}'$, denoted by $\boldsymbol{L} < \boldsymbol{L}'$, if $\boldsymbol{L}(k) < \boldsymbol{L}'(k)$ for some $k \leq n$ and $\boldsymbol{L}(i) = \boldsymbol{L}(i)$ for all $i < k$ (see §A.1 for the definition of the lexicographical ordering of permutations). Not all the entries of two Latin squares are used when comparing them lexicographically, and the ordering of two partial Latin squares may therefore be determined if the necessary entries to compare them are present. If not, then the ordering is inconclusive. For instance, the two partial Latin squares

$$\boldsymbol{L}_{4.7} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ & & & \\ 3 & 0 & 1 & 2 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{4.8} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ & & & \\ 2 & 0 & 3 & 1 \end{bmatrix}.$$

cannot be compared in respect of the lexicographical ordering mentioned above, since their ordering depends on the entries of row 2, while the partial Latin square

$$\boldsymbol{L}_{4.9} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ & & & \\ 2 & 3 & 0 & 1 \end{bmatrix}.$$

is smaller than both $\boldsymbol{L}_{4.7}$ and $\boldsymbol{L}_{4.8}$. If a partial Latin square $\boldsymbol{L}$ is smaller than a partial Latin square $\boldsymbol{L}'$, it simply means that any completion of $\boldsymbol{L}$ will be smaller than any completion of $\boldsymbol{L}'$.

In order to ensure that Algorithm 4.1 generates only the smallest Latin squares in each σ-transformation class, a search may be employed to find a σ-transformation α such that $\boldsymbol{L}^\alpha < \boldsymbol{L}$ for any partial Latin square $\boldsymbol{L}$ at any stage of the algorithm. If such a transformation exists, then this transformation maps any completion of $\boldsymbol{L}$ to some completion of $\boldsymbol{L}^\alpha$, and the latter is smaller than the former. Hence no completion of $\boldsymbol{L}$ is the smallest Latin square in its class, and $\boldsymbol{L}$ becomes a leaf of the tree (*i.e.* the search does branch further from $\boldsymbol{L}$). If no such transformation exists, then the search continues since a completion of $\boldsymbol{L}$ may possibly be the smallest Latin square in its class.

Consider, for example, enumerating the isomorphism classes of N_2-squares of order 5 containing a reduced Latin square. The same approach as in Figure 4.1 may be used together with the additional requirement that, for each reduced N_2-square $\boldsymbol{L}$, $\boldsymbol{L} < \boldsymbol{L}'$ for any $\boldsymbol{L}'$ isomorphic to $\boldsymbol{L}$. Consider the left-most vertex on level 1 in Figure 4.1, which represents the partial Latin square

$$\boldsymbol{L}_{4.10} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 & 0 \end{bmatrix},$$

(the bottom three rows may be ignored for simplicity) and let $p \in S_n$ be an isomorphism for which $\boldsymbol{L}^p_{4.10} < \boldsymbol{L}_{4.10}$ (if such an isormophism exists). It is easy to see that the first row of $\boldsymbol{L}^p_{4.10}$ is also in natural order and that the first entry of row 2 contains the element 1, otherwise it cannot be smaller than $\boldsymbol{L}_{4.10}$. Also, row 1 may not be empty, because in that case the two Latin squares cannot be compared. Hence $p(0) = 0$ and $p(1) = 1$. Utilising Wolfram's MATHEMATICA [150], all permutations of order 5 which fix the first two elements may quickly be listed and applied to $\boldsymbol{L}_{4.10}$. It follows that the permutation $\binom{0\,1\,2\,3\,4}{0\,1\,3\,2\,4}$ maps $\boldsymbol{L}_{4.10}$ to the partial Latin square

$$\boldsymbol{L}_{4.11} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix},$$

and that $\boldsymbol{L}_{4.10}$ is a leaf in the new tree. The same method applied to all partial Latin squares represented by the vertices on level 1 in Figure 4.1 shows that all of these vertices except one (the second one from the left) are leaves of the new tree. Hence there is only one isomorphism class of N_2-squares of order 5 containing a reduced Latin square.

4.3.1 Enumeration of CS-paratopism classes of Latin squares

Burger *et al.* [33] describe a method using orderly generation in order to enumerate the CS-paratopism classes of special types of Latin squares for which it may be shown that there is at least one idempotent Latin square in each CS-paratopy class. The following lemma states that it is sufficient to only enumerate the row-isomorphism classes of idempotent Latin squares in order to enumerate the CS-paratopism classes containing idempotent Latin squares.

Lemma 4.3.1 *If two idempotent Latin squares are CS-paratopic, then they are row-isomorphic.*

Proof: Suppose $\boldsymbol{L}$ and $\boldsymbol{L}'$ are idempotent Latin squares and let the CS-paratopism (p, q, c) map $\boldsymbol{L}$ to $\boldsymbol{L}'$. Then, since $(i, i, i) \in T(\boldsymbol{L})$ for all $i \in \mathbb{Z}_n$, $(p(i), q(i), q(i)) \in T(\boldsymbol{L}')$. Since $\boldsymbol{L}'$ is also idempotent, $p(i) = q(i)$ for all $i \in \mathbb{Z}_n$, and therefore $\boldsymbol{L}$ and $\boldsymbol{L}'$ are row-isomorphic. ■

By Lemma 4.3.1 it follows that the number of row-isomorphism classes of idempotent Latin squares of order n equals the total number of CS-paratopism classes containing idempotent Latin squares. Since the triple $(i, i, i) \in T(\boldsymbol{L})$ remains unchanged under any conjugate operation, the above lemma also holds for RS-paratopisms and RC-paratopisms by Proposition 4.1.1. It is also useful to note that idempotency is a row-isomorphism class invariant.

The following lemma and theorem make use of the fact that the cycle structures of the rows of a Latin square are CS-paratopy class invariant, as discussed in §4.1 (see §A.1.1 for the notions of a lexicographical ordering of cycle structures and a cycle structure representative.).

Lemma 4.3.2 *Any row in an idempotent Latin square $\boldsymbol{L}$ may be mapped to the first row and transformed into a cycle structure representative via a row-isomorphism.*

Proof: Let $\boldsymbol{L}(i)$ be any row in $\boldsymbol{L}$. By Proposition A.1.3 there is at least one permutation p such that $p \circ \boldsymbol{L}(i) \circ p^{-1}$ is a cycle structure representative. Since $\boldsymbol{L}$ is idempotent, $\boldsymbol{L}(i)$ fixes i and $p \circ \boldsymbol{L} \circ p^{-1}$ fixes 0 (by the definition of a cycle structure representative). Since p maps each cycle of $\boldsymbol{L}(i)$ to a cycle of the same length in $p \circ \boldsymbol{L}(i) \circ p^{-1}$ (see the proof of Proposition A.1.3), it follows that $p(i) = 0$. Hence $p \circ \boldsymbol{L}(i) \circ p^{-1}$ is the first row of $\boldsymbol{L}^{(p,\iota)}$ where (p, ι) is a row-isomorphism. ■

The following theorem provides a means of quickly identifying when an idempotent Latin square is not the smallest idempotent Latin square in its row-isomorphism class.

Theorem 4.3.1 *If $\boldsymbol{L}$ is the lexicographically smallest idempotent Latin square in its row-isomorphism class, then*

(1) $\boldsymbol{L}(0)$ is a cycle structure representative,

(2) the cycle structure of $\boldsymbol{L}(i)$ is not lexicographically smaller than the cycle structure of $\boldsymbol{L}(0)$ for all $2 \leq i \leq n$.

Proof: If (1) is false, then, by Lemma 4.3.2, $\boldsymbol{L}(0)$ may be transformed into a cycle structure representative, resulting in a lexicographically smaller Latin square. If (2) is false, then, by Lemma 4.3.2, any row with a lexicographically smaller cycle structure than the first row may be mapped as a cycle structure representative to the first row. Even if the first row is a cycle structure representative (by Proposition A.1.1) the resulting Latin square is still lexicographically smaller than $\boldsymbol{L}$. Either case contradicts the fact that $\boldsymbol{L}$ is the lexicographically smallest idempotent Latin square in its row-isomorphism class. ■

By Theorem 4.3.1, the first row to be inserted in the search tree (initialised with an empty array) must be a cycle structure representative, otherwise no completion of it can be the lexicographically smallest idempotent Latin square in its row-isomorphism class. Also, the cycle structure of any row added at any stage of the search may not be lexicographically smaller than the cycle structure of the first row. If, at some stage of the search, a Latin rectangle $\boldsymbol{L}$ passes both these tests, it is then necessary to look for a row-isomorphism α for which $\boldsymbol{L}^{\alpha} < \boldsymbol{L}$, if such a transformation exists.

If such a row-isomorphism α exists, then, by Theorem 4.3.1 and the above two pruning rules, $\boldsymbol{L}^{\alpha}(0) = \boldsymbol{L}(0)$. Hence, if $i_1, i_2, \ldots, i_r$ are the indices of all the rows of $\boldsymbol{L}$ with the same cycle structure as the first row, then α maps $\boldsymbol{L}(i_j)$ to $\boldsymbol{L}(0)$ for some $1 \leq j \leq r$. Hence α consists of a permutation p for which $p \circ \boldsymbol{L}(i_j) \circ p^{-1} = \boldsymbol{L}(0)$ (implying that $p(i_j) = 0$ by the idempotency of $\boldsymbol{L}$). Proposition A.1.3 states that there are $\prod_{i=1}^{n} a_i! i^{a_i}$ distinct choices of p for which $p \circ \boldsymbol{L}(i_j) \circ p^{-1} = \boldsymbol{L}(0)$ and the proof of the proposition also provides a means of finding these permutations. Hence, for each i_j, these permutations may be used in a row-isomorphism in either of the two forms $\alpha = (p, \iota)$ or $\alpha = (p, \rho)$ in order to verify that $\boldsymbol{L}^{\alpha} < \boldsymbol{L}$. If no such a row-isomorphism α exists, then the search continues to branch on $\boldsymbol{L}$. Otherwise $\boldsymbol{L}$ becomes a leaf of the search tree.

Although the method described above delivers row-isomorphism class representatives of idempotent Latin squares, these may also be taken as CS-paratopism class representatives by Lemma 4.3.1. By Proposition 4.1.1 it follows that enumerating CS-paratopy classes of Latin squares is equivalent to enumerating either RS-paratopy classes or RC-paratopy classes. Hence, in order to enumerate either RS-paratopy classes or RC-paratopy classes, the CS-paratopy classes may be enumerated by the method described above, and appropriate conjugates of the resulting squares may be taken (as illustrated in Proposition 4.1.1) in order to obtain either RS-main class representatives or RC-main class representatives.

4.3.2 Enumeration of main classes of MOLS

In this section a method for the enumeration of main classes of k-MOLS of order n using an orderly generation approach is discussed. A notion that proves useful in this regard is the *relative cycle structure* of two universals from two different Latin squares in a k-MOLS. If $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ is a k-MOLS of order n, let $U(\mathcal{M})$ denote the set of all universal permutations of $\boldsymbol{L}_i$ for all $i \in \mathbb{Z}_n$ and let $u_i^{(j)} \in U(\mathcal{M})$ denote the universal permutation of the element $i \in \mathbb{Z}_n$ in $\boldsymbol{L}_j$ for $j \in \mathbb{Z}_k$. Then the *relative cycle structure* of $u_i^{(j)} \in U(\mathcal{M})$ and $u_\ell^{(m)} \in U(\mathcal{M})$ for $i, \ell \in \mathbb{Z}_n$ and $j, m \in \mathbb{Z}_k$ is defined as the cycle structure of the permutation

$$u_\ell^{(m)} \circ \left(u_i^{(j)}\right)^{-1},$$

i.e. the permutation under which the image of $u_i^{(j)}(a)$ is $u_\ell^{(m)}(a)$. For example, consider the pair of orthogonal Latin squares

$$\boldsymbol{L}_{4.12} = \begin{bmatrix} 0&1&2&3&4&5&6\\ 4&0&3&1&6&2&5\\ 5&6&0&4&2&1&3\\ 6&4&1&0&5&3&2\\ 1&3&5&2&0&6&4\\ 2&5&4&6&3&0&1\\ 3&2&6&5&1&4&0 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{4.13} = \begin{bmatrix} 0&1&2&3&4&5&6\\ 5&6&0&4&2&1&3\\ 6&4&1&0&5&3&2\\ 1&3&5&2&0&6&4\\ 2&5&4&6&3&0&1\\ 3&2&6&5&1&4&0\\ 4&0&3&1&6&2&5 \end{bmatrix}$$

of order 7, and consider the universal permutations $\binom{0123456}{1352064}$ and $\binom{0123456}{2463015}$ of the element 1 in $\boldsymbol{L}_{4.12}$ and the element 2 in $\boldsymbol{L}_{4.13}$ respectively. The relative cycle structure of these two universal permutations is the cycle structure of $\binom{0123456}{2463015} \circ \binom{0123456}{4031625} = \binom{0123456}{0234561}$, which is $z_1^1 z_6^1$. It may be noted that there is always exactly one fixed point in the relative cycle structure of two universal permutations $u_i^{(j)}$ and $u_\ell^{(m)}$ in a k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n. This is true since, due to the orthogonality of $\boldsymbol{L}_j$ and $\boldsymbol{L}_m$, the universals of i in $\boldsymbol{L}_j$ and ℓ in $\boldsymbol{L}_m$ must have exactly one entry, (r, c) say, in common. Hence $u_i^{(j)}(r) = c$ is mapped to $u_\ell^{(m)}(r) = c$ in the product

$$u_\ell^{(m)} \circ \left(u_i^{(j)}\right)^{-1},$$

resulting in exactly one fixed point.

More importantly, however, the relative cycle structures of universals in a MOLS are invariant under row, column and symbol permutations. Let a permutation $p_r \in S_n$ be applied to the rows of a Latin square $\boldsymbol{L}$ of order n in order to obtain a Latin square $\boldsymbol{L}'$ of order n as result, and let u_k and u'_k be the universal permutations of the element $k \in \mathbb{Z}_n$ in $\boldsymbol{L}$ and $\boldsymbol{L}'$ respectively. Since each triple $(i,j,k) \in T(\boldsymbol{L})$ is replaced by $(p_r(i),j,k)$, it follows that $u_k(i) = u'_k(p_r(i)) = j$ for all $(i,j,k) \in T(\boldsymbol{L})$, and consequently that p_r replaces the universal permutation u_k with $u_k \circ p_r^{-1}$. If p_c is a permutation applied to the columns of $\boldsymbol{L}$, then each triple $(i,j,k) \in T(\boldsymbol{L})$ is replaced by $(i,p_c(j),k)$, and it follows that $u'_k(i) = p_c(j) = p_c(u_k(i))$ for all $(i,j,k) \in T(\boldsymbol{L})$. Hence in this case the universal permutation u_k is replaced by $p_c \circ u_k$.

Consider two universal permutations $u_i^{(j)} \in U(\mathcal{M})$ and $u_\ell^{(m)} \in U(\mathcal{M})$ in a k-MOLS $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n for some $i, \ell \in \mathbb{Z}_n$ and $j, m \in \mathbb{Z}_k$. If a permutation p_r is applied to the rows of $\boldsymbol{L}_i$ for all $i \in \mathbb{Z}_k$, then $u_i^{(j)}$ and $u_\ell^{(m)}$ are replaced by $u_i^{(j)} \circ p_r^{-1}$ and $u_\ell^{(m)} \circ p_r^{-1}$ respectively, while the product

$$u_\ell^{(m)} \circ \left(u_i^{(j)}\right)^{-1}$$

is mapped to

$$u_\ell^{(m)} \circ p_r^{-1} \circ \left(u_i^{(j)} \circ p_r^{-1}\right)^{-1} = u_\ell^{(m)} \circ p_r^{-1} \circ p_r \circ \left(u_i^{(j)}\right)^{-1} = u_\ell^{(m)} \circ \left(u_i^{(j)}\right)^{-1}.$$

Hence the relative cycle structure of the universal permutations of two universals in a MOLS is preserved under a row permutation applied to all the Latin squares in the MOLS. Now let p_c be a column permutation applied to the columns of $\boldsymbol{L}_i$ for all $i \in \mathbb{Z}_k$. Then $u_i^{(j)}$ and $u_\ell^{(m)}$ are replaced by $p_c \circ u_i^{(j)}$ and $p_c \circ u_\ell^{(m)}$ respectively, while the product

$$u_\ell^{(m)} \circ \left(u_i^{(j)}\right)^{-1}$$

is mapped to

$$p_c \circ u_\ell^{(m)} \circ \left(p_c \circ u_i^{(j)}\right)^{-1} \quad = \quad p_c \circ u_\ell^{(m)} \circ \left(u_i^{(j)}\right)^{-1} \circ p_c^{-1},$$

i.e. to one of its conjugate permutations. Since two conjugate permutations have the same cycle structure, the relative cycle structures are preserved under a column permutation as well.

Finally, since a symbol permutation applied to a Latin square simply renames the universals of the Latin square, it clearly does not change the relative cycle structures of the universals in a MOLS. It may also be noted that the conjugate operations of transposing all the Latin squares in a MOLS and of changing the order of the Latin squares in the MOLS do not change the relative cycle structures of the universals.

Another notion that will prove to be useful in the enumeration of MOLS is that of a *row-reduced* k-MOLS of order n. A k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n is *row-reduced* if $\boldsymbol{L}_i(0,j) = j$ for all $i \in \mathbb{Z}_k$ and $j \in \mathbb{Z}_n$, in other words if the first row of each Latin square in the MOLS is in natural order. It is easy to verify that any k-MOLS of order n may be transformed into a row-reduced k-MOLS of order n using k symbol permutations, each applied to a different Latin square in the MOLS. Hence every main class of k-MOLS of order n contains a row-reduced k-MOLS of order n, and it is sufficient only to consider row-reduced MOLS in order to enumerate main classes using an orderly generation approach. The fact that the operations discussed above preserve the relative cycle structures of the universals in a MOLS leads to the following useful lemma.

Lemma 4.3.3 *For any $i, \ell \in \mathbb{Z}_n$ and $j, m \in \mathbb{Z}_k$ the universal permutations $u_i^{(j)} \in U(\mathcal{M})$ and $u_\ell^{(m)} \in U(\mathcal{M})$ in a row-reduced k-MOLS $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n may be mapped* *to the universal permutations $v_0^{(0)} \in U(\mathcal{M}')$ and $v_0^{(1)} \in U(\mathcal{M}')$ of a new row-reduced k-MOLS $\mathcal{M}' = (\boldsymbol{L}_0', \boldsymbol{L}_1', \ldots, \boldsymbol{L}_{k-1}')$ of order n, respectively, using a paratopism in such a way that $v_0^{(0)}$ is the identity permutation and $v_0^{(1)}$ is a cycle structure representative.*

Proof: Let $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ be mapped to $\mathcal{M}'' = (\boldsymbol{L}_0'', \boldsymbol{L}_1'', \ldots, \boldsymbol{L}_{k-1}'')$ by using symbol permutations $s_1 \in S_n$ and $s_2 \in S_n$ applied to $\boldsymbol{L}_j$ and $\boldsymbol{L}_m$, respectively, where $s_1(i) = s_2(\ell) = 0$ and a conjugate permutation c applied to $\mathcal{M}$ where $c(j) = 0$ and $c(m) = 1$. Hence $w_0^{(0)} = u_i^{(j)}$ and $w_0^{(1)} = u_\ell^{(m)}$ for $w_0^{(0)}, w_0^{(1)} \in U(\mathcal{M}'')$. A row permutation r may now be applied to $\mathcal{M}''$ such that $w_0^{(0)} \circ r^{-1}$ is the identity permutation, and this may be followed by a permutation p applied to the rows and columns of $\mathcal{M}''$ in such a way that $p \circ w_0^{(1)} \circ r^{-1} \circ p^{-1}$ is a cycle structure representative (by Proposition A.1.3). Finally, $k-1$ symbol permutations may be applied to $\boldsymbol{L}_i$ for $1 \leq i \leq k-1$ in order for the resulting MOLS to be row-reduced without changing the fact that $p \circ w_0^{(1)} \circ r^{-1} \circ p^{-1}$ is a cycle structure representative. If $\mathcal{M}' = (\boldsymbol{L}_0', \boldsymbol{L}_1', \ldots, \boldsymbol{L}_{k-1}')$ is the resulting k-MOLS of order n after these operations are applied to $\mathcal{M}''$, and if $v_0^{(0)}, v_0^{(1)} \in U(\mathcal{M}')$, then $v_0^{(0)} = p \circ w_0^{(0)} \circ r^{-1} \circ p^{-1}$ is the identity permutation and $v_0^{(1)} = p \circ w_0^{(1)} \circ r^{-1} \circ p^{-1}$ is a cycle structure representative. ■

In order for an orderly generation approach to be utilised for the enumeration of MOLS, it is necessary to define a lexicographical ordering on the set of all k-MOLS of order n. A k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n is *lexicographically smaller* than a k-MOLS $(\boldsymbol{L}_0', \boldsymbol{L}_1', \ldots, \boldsymbol{L}_{k-1}')$ of order n if $(^{-1}\boldsymbol{L}_i)^T < (^{-1}\boldsymbol{L}_i')^T$ for some $i \in \mathbb{Z}_k$ and $(^{-1}\boldsymbol{L}_j)^T = (^{-1}\boldsymbol{L}_j')^T$ for all $0 \leq j \leq i-1$. Since row $i \in \mathbb{Z}_n$ of $(^{-1}\boldsymbol{L})^T$ is the universal permutation of the element i in a Latin square $\boldsymbol{L}$, MOLS are compared lexicographically by comparing the universals of their Latin squares lexicographically. The following theorem provides a means of quickly identifying when a row-reduced k-MOLS of order n is not the smallest row-reduced k-MOLS of order n in its main class.

Theorem 4.3.2 *If $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ is the lexicographically smallest row-reduced k-MOLS of order n in its main class, and if $u_i^{(j)} \in U(\mathcal{M})$ is the universal permutation of $i \in \mathbb{Z}_n$ in $\boldsymbol{L}_j$, then*

(1) $u_0^{(0)}$ is the identity permutation,

(2) $u_0^{(1)}$ is a cycle structure representative, and

(3) the relative cycle structure of two universal permutations $u_i^{(j)}, u_\ell^{(m)} \in U(\mathcal{M})$ is not lexicographically smaller than the cycle structure of $u_0^{(1)} \in U(\mathcal{M})$ for all $i, \ell \in \mathbb{Z}_k$ and $j, m \in \mathbb{Z}_n$.

Proof: If (1) is false, then, by Lemma 4.3.3, $u_0^{(0)}$ may be transformed into the identity permutation, and the result will clearly be a lexicographically smaller k-MOLS of order n. Similarly, also by Lemma 4.3.3, if (2) is false (and assuming (1) is true) then $u_0^{(1)}$ may be transformed into a cycle structure representative which will also result in a lexicographically smaller k-MOLS of order n. Finally, if (3) is false, then, by Lemma 4.3.3, any pair of universal permutations $u_i^{(j)}$ and $u_\ell^{(m)}$ with a relative cycle structure smaller than the relative cycle structure of $u_0^{(0)}$ and $u_0^{(1)}$ (which is identical to the cycle structure of $u_0^{(1)}$) may be mapped to $u_0^{(0)}$ and $u_0^{(1)}$ as the identity permutation and a cycle structure representative, respectively, and the result will be a lexicographically smaller row-reduced k-MOLS of order n. ■

A *partial* k-MOLS $(\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n is a MOLS in which $\boldsymbol{L}_i$ is a partial Latin square for all $i \in \mathbb{Z}_k$. The search tree for a k-MOLS $\mathcal{M}$ of order n branches on the inclusion of a set of k universals of a given symbol, one for each Latin square, into a partial k-MOLS of order n. These universals are generated as discussed earlier in this section, and a set S of k universals is only included if the relative cycle structure of every two universals in $S \cup U(\mathcal{M})$ has exactly one fixed point. This ensures that the tuples of Latin squares eventually generated all contain pairwise orthogonal Latin squares.

By Theorem 4.3.2, the universal permutation of the first universal in the first Latin square of a k-MOLS of order n must be the identity permutation, and the first universal of the second Latin square must be a cycle structure representative. Furthermore, the relative cycle structure of no two universals already inserted may be lexicographically smaller than the cycle structure of the first universal of the second Latin square. As was the case in the previous section, if these requirements are met for a partial k-MOLS $\mathcal{M}$ of order n, then it is necessary to look for a paratopism that maps $\mathcal{M}$ to a lexicographically smaller partial k-MOLS of order n, if such a transformation exists.

Given a partial k-MOLS $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order n, let $\bar{U}(\mathcal{M})$ be the set of all pairs $(u_i^{(j)}, u_\ell^{(m)}) \in U(\mathcal{M}) \times U(\mathcal{M})$ of universal permutations such that $j \neq m$ and such that the relative cycle structure of $u_i^{(j)}$ and $u_\ell^{(m)}$ is equal to the cycle structure of $u_0^{(1)}$. In order to determine whether $\mathcal{M}$ can be mapped to a lexicographically smaller partial k-MOLS of order n, all possible paratopisms should be considered which map each of these pairs of universal permutations to $u_0^{(0)}$ and $u_0^{(1)}$. This may be achieved by generating all possible paratopisms which include the necessary operations either to map $u_i^{(j)}$ to $u_0^{(0)}$ and $u_\ell^{(m)}$ to $u_0^{(1)}$, or to map $\left(u_i^{(j)}\right)^{-1}$ to $u_0^{(0)}$ and $\left(u_\ell^{(m)}\right)^{-1}$ to $u_0^{(1)}$, for each pair $(u_i^{(j)}, u_\ell^{(m)}) \in \bar{U}(\mathcal{M})$ (as discussed in Lemma 4.3.3). Mapping the inverses of these universal permutations may be achieved by applying the transpose conjugate operation to $\mathcal{M}$. Any of the conjugate operations which only permutes the order of the Latin squares in $\mathcal{M}$ may also be used. If any one of these paratopisms results in a lexicographically smaller partial k-MOLS of order n, then the current partial k-MOLS of order n immediately becomes a leaf of the tree (*i.e.* the search tree is pruned or bounded at this point).

Except for the conjugate operations of transposing the Latin squares in $\mathcal{M}$ and permuting the order of the Latin squares in $\mathcal{M}$, no other conjugate operation can be applied if $\mathcal{M}$ is a partial k-MOLS of order n since this will result in incomplete universals. Once $\mathcal{M}$ is a complete k-MOLS of order n (*i.e.* once the search tree reaches level n), then all conjugates have to be considered in order to determine whether $\mathcal{M}$ is the lexicographically smallest MOLS in its main class. Let $\mathcal{C}$ be a conjugate of $\mathcal{M}$ which not only transposes the Latin squares or permutes their order. Then all pairs of universals in $\bar{U}(\mathcal{C})$ should be mapped to $u_0^{(0)} \in U(\mathcal{M})$ and $u_0^{(1)} \in U(\mathcal{M})$ in the same way as discussed above. In this way all leaves of the tree that are represented by complete k-MOLS of order n and that are not pruned will give exactly one k-MOLS of order n from each main class of k-MOLS of order n.

4.4 Computation of autotransformation groups of Latin squares

In this section various methods of computing the autotransformation groups of Latin squares are described. These methods play an essential part in enumerating Latin squares and Latin square classes theoretically, as will be discussed in the next section. Let $G_\sigma(n)$ be the σ-transformation group acting on the set of all Latin objects of order n for some transformation type σ. The simplest way of computing the σ-autotransformation group of a Latin square $\boldsymbol{L}$ is to apply all elements of $G_\sigma(n)$ to $\boldsymbol{L}$ exhaustively and to list those that map $\boldsymbol{L}$ to itself. This process is described in pseudo code form as Algorithm 4.2.

Algorithm 4.2 ExhaustiveAutotransformationGroupComputation

Input: A Latin square $\boldsymbol{L}$.
Output: The σ-autotransformation group $A_\sigma(\boldsymbol{L})$ of $\boldsymbol{L}$.

```
1: A_σ(L) ← ∅
2: for all α ∈ G_σ(n) do
3:   if L^α = L then
4:     A_σ(L) ← A_σ(L) ∪ {α}
5:   end if
6: end for
```

The method described in Algorithm 4.2 becomes extremely inefficient rather quickly. For instance, computing the autoparatopy group of a Latin square requires $|S_n \wr D_3| = 6(n!)^3$ executions of Steps 2 and 3, a number which grows quickly as n increases. A method for computing the automorphism group, autotopy group and autoparatopy group of a Latin square was presented by McKay *et al.* [99]. This method makes use of the computer program `nauty` (**no**-**aut**omorphisms, **y**es?) [96], written by McKay, which computes the automorphism groups of vertex-coloured graphs. The method requires the representation of a Latin square $\boldsymbol{L}$ as a graph G in such a way that the automorphism group of G is isomorphic to the σ-autotransformation group of $\boldsymbol{L}$ for any given σ. The method proposed by McKay *et al.* [99] for computing the automorphism, autotopy and autoparatopy group of a Latin square is generalised here for computing any σ-autotransformation group of a given Latin square.

For any Latin square $\boldsymbol{L}$ of order n and a type of transformation σ, the *σ-transformation graph* of $\boldsymbol{L}$ is a (possibly mixed, directed) graph G with vertex set

$$V(G) = \{\ell_{ij} \mid i, j \in \mathbb{Z}_n\} \cup \{r_i \mid i \in \mathbb{Z}_n\} \cup \{c_i \mid i \in \mathbb{Z}_n\} \cup \{s_i \mid i \in \mathbb{Z}_n\} \cup \{R, C, S\}.$$

The elements of $V(G)$ are coloured by up to five colours. Colours 1 and 2 are assigned to the vertices in the subsets $\{\ell_{ij} \mid i, j \in \mathbb{Z}_n\}$ and $\{R, C, S\}$ of $V(G)$ respectively, while Colours 3 to 5 are assigned to the vertices in the three subsets $\{r_i \mid i \in \mathbb{Z}_n\}$, $\{c_i \mid i \in \mathbb{Z}_n\}$ and $\{s_i \mid i \in \mathbb{Z}_n\}$, respectively, only if none of the conjugate operations is σ-permissible. Table 4.3 shows the colouring of the vertices if only one of the conjugate operations ρ, γ or τ is σ-permissible, while Colour 3 is assigned to the vertices in the subset $\{r_i \mid i \in \mathbb{Z}_n\} \cup \{c_i \mid i \in \mathbb{Z}_n\} \cup \{s_i \mid i \in \mathbb{Z}_n\}$ of $V(G)$ either if $\tau\rho$ is σ-permissible or if all the conjugate operations are σ-permissible.

Operation	Colour 3	Colour 4
ρ	$\{r_i \mid i \in \mathbb{Z}_n\}$	$\{c_i \mid i \in \mathbb{Z}_n\} \cup \{s_i \mid i \in \mathbb{Z}_n\}$
γ	$\{c_i \mid i \in \mathbb{Z}_n\}$	$\{r_i \mid i \in \mathbb{Z}_n\} \cup \{s_i \mid i \in \mathbb{Z}_n\}$
τ	$\{s_i \mid i \in \mathbb{Z}_n\}$	$\{r_i \mid i \in \mathbb{Z}_n\} \cup \{c_i \mid i \in \mathbb{Z}_n\}$

TABLE 4.3: *The colouring of the vertices of the σ-transformation graph of a Latin square according the specific conjugate operations that are σ-permissible.*

The edges in $E(G)$ depend on the specifications of σ. If either a row, column or symbol permutation is σ-permissible, then it implies that $r_i\ell_{ij} \in E(G)$, $c_j\ell_{ij} \in E(G)$ or $s_k\ell_{ij} \in E(G)$

for each triple $(i, j, k) \in T(\boldsymbol{L})$, respectively. If any one of π_{rc}, π_{rs} or π_{cs} are specified by σ, then it implies that $\{r_i c_i \mid i \in \mathbb{Z}_n\} \in E(G)$, $\{r_i s_i \mid i \in \mathbb{Z}_n\} \in E(G)$ or $\{c_i s_i \mid i \in \mathbb{Z}_n\} \in E(G)$, respectively, while all three of these cases are implied if π_{rcs} is specified by σ. If any one of τ, ρ, γ and δ are σ-permissible, then it implies that $\{Rr_i, Cc_i \mid i \in \mathbb{Z}_n\} \in E(G)$, $\{Cc_i, Ss_i \mid i \in \mathbb{Z}_n\} \in E(G)$, $\{Rr_i, Ss_i \mid i \in \mathbb{Z}_n\} \in E(G)$ and $\{Rr_i, Cc_i, Ss_i \mid i \in \mathbb{Z}_n\} \in E(G)$, respectively. If $\tau\rho$ is σ-permissible, then $E(G)$ contains three arcs, namely (R, C), (C, S) and (S, R).

For example, Figure 4.2 shows the CS-paratopism graph of the Latin square

$$\boldsymbol{L}_{4.14} = \begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}.$$

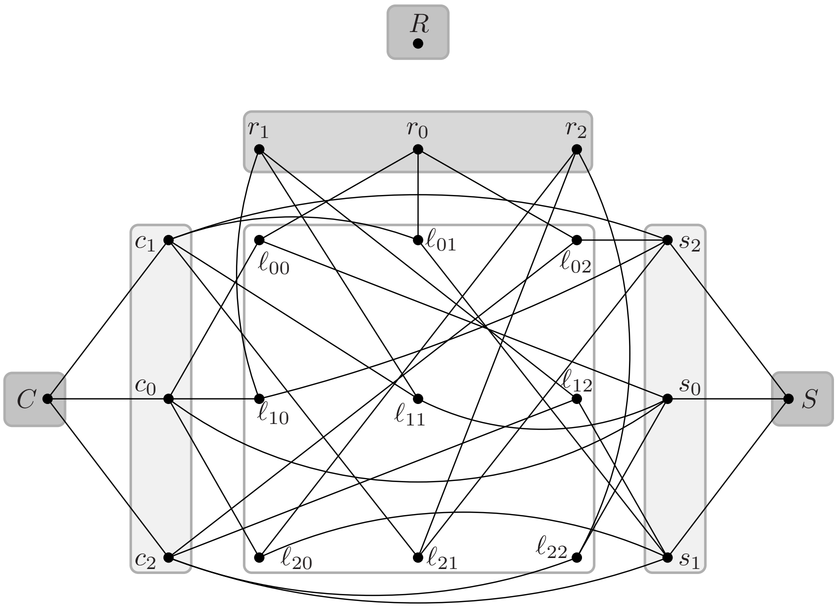

FIGURE 4.2: *The CS-paratopism graph of the Latin square* $\boldsymbol{L}_{4.14}$.

The following theorem states a useful property of the σ-transformation graph of a Latin square.

Theorem 4.4.1 *Two Latin squares are in the same σ-transformation class if and only if their σ-transformation graphs are isomorphic.*

Proof: Let the σ-transformation graphs G and G' of the Latin squares $\boldsymbol{L}$ and $\boldsymbol{L}'$ have vertex sets

$$V(G) = \{\ell_{ij} \mid i, j \in \mathbb{Z}_n\} \cup \{r_i \mid i \in \mathbb{Z}_n\} \cup \{c_i \mid i \in \mathbb{Z}_n\} \cup \{s_i \mid i \in \mathbb{Z}_n\} \cup \{R, C, S\}$$

and

$$V(G') = \{\ell'_{ij} \mid i, j \in \mathbb{Z}_n\} \cup \{r'_i \mid i \in \mathbb{Z}_n\} \cup \{c'_i \mid i \in \mathbb{Z}_n\} \cup \{s'_i \mid i \in \mathbb{Z}_n\} \cup \{R', C', S'\},$$

respectively. Suppose further that a σ-transformation α maps $\boldsymbol{L}$ to $\boldsymbol{L}'$. Let $p_r \in S_n$, $p_c \in S_n$, $p_s \in S_n$ and $c \in S_3$ be the row permutation, the column permutation, the symbol permutation and the conjugate operation in α, respectively (note that if any of these operations are not σ-permissible, then they may be taken as the identity operations). Three cases are considered, namely where $c = \iota$ (the identity conjugate operation), where $c = \rho$ (which is similar to the cases where $c = \gamma$ and $c = \tau$), and where $c = \tau\rho$.

Case 1: If no conjugate operations are σ-permissible, then the sets $\{r_i \mid i \in \mathbb{Z}_n\}$ and $\{r'_i \mid i \in \mathbb{Z}_n\}$ are each assigned Colour 1, the sets $\{c_i \mid i \in \mathbb{Z}_n\}$ and $\{c'_i \mid i \in \mathbb{Z}_n\}$ are each assigned Colour 2, while the sets $\{s_i \mid i \in \mathbb{Z}_n\}$ and $\{s'_i \mid i \in \mathbb{Z}_n\}$ are each assigned Colour 3. Hence an isomorphism from G to G' constitutes a permutation p that maps $\{r_i \mid i \in \mathbb{Z}_n\}$ to $\{r'_i \mid i \in \mathbb{Z}_n\}$, a permutation q that maps $\{c_i \mid i \in \mathbb{Z}_n\}$ to $\{c'_i \mid i \in \mathbb{Z}_n\}$ and a permutation r that maps $\{s_i \mid i \in \mathbb{Z}_n\}$ to $\{s'_i \mid i \in \mathbb{Z}_n\}$, which is equivalent to a (π_r, π_c, π_s)-transformation (p, q, r) which maps $\boldsymbol{L}$ to $\boldsymbol{L}'$.

Case 2: If the conjugate operation ρ is σ-permissible, then the sets $\{r_i \mid i \in \mathbb{Z}_n\}$ and $\{r'_i \mid i \in \mathbb{Z}_n\}$ are each assigned Colour 1, while the sets $\{c_i \mid i \in \mathbb{Z}_n\}$, $\{c'_i \mid i \in \mathbb{Z}_n\}$, $\{s_i \mid i \in \mathbb{Z}_n\}$ and $\{s'_i \mid i \in \mathbb{Z}_n\}$ are each assigned Colour 2. Since in this case each vertex c_i is joined to the vertex C and each vertex s_i is joined to the vertex S for all $i \in \mathbb{Z}_n$ (the same also being true for G'), $\{c_i \mid i \in \mathbb{Z}_n\}$ is either mapped to $\{c'_i \mid i \in \mathbb{Z}_n\}$ or to $\{s'_i \mid i \in \mathbb{Z}_n\}$ (*i.e.* these sets cannot be partially mapped to one another). If $\{c_i \mid i \in \mathbb{Z}_n\}$ is mapped to $\{s'_i \mid i \in \mathbb{Z}_n\}$ (in which case $\{s_i \mid i \in \mathbb{Z}_n\}$ is, in turn, mapped to $\{c'_i \mid i \in \mathbb{Z}_n\}$), then it is similar to Case 1 in that an isomorphism from G to G' is equivalent to a $(\pi_r, \pi_c, \pi_s, \rho)$-transformation which maps $\boldsymbol{L}$ to $\boldsymbol{L}'$. The cases where γ and τ are σ-permissible follow in a similar manner.

Case 3: If the conjugate operation $\tau\rho$ is σ-permissible, then all of the sets $\{r_i \mid i \in \mathbb{Z}_n\}$, $\{r'_i \mid i \in \mathbb{Z}_n\}$, $\{c_i \mid i \in \mathbb{Z}_n\}$, $\{c'_i \mid i \in \mathbb{Z}_n\}$, $\{s_i \mid i \in \mathbb{Z}_n\}$ and $\{s'_i \mid i \in \mathbb{Z}_n\}$ are each assigned Colour 1. However, the three arcs (R, C), (C, S) and (S, R) ensure that if the set $\{r_i \mid i \in \mathbb{Z}_n\}$ is mapped to the set $\{c'_i \mid i \in \mathbb{Z}_n\}$, then the set $\{c_i \mid i \in \mathbb{Z}_n\}$ is mapped to the set $\{s'_i \mid i \in \mathbb{Z}_n\}$, while the set $\{s_i \mid i \in \mathbb{Z}_n\}$ is mapped to the set $\{r'_i \mid i \in \mathbb{Z}_n\}$, which is equivalent to a $(\pi_r, \pi_c, \pi_s, \tau\rho)$-transformation which maps $\boldsymbol{L}$ to $\boldsymbol{L}'$. Similarly, it ensures that if the set $\{r_i \mid i \in \mathbb{Z}_n\}$ is mapped to the set $\{s'_i \mid i \in \mathbb{Z}_n\}$, then the set $\{s_i \mid i \in \mathbb{Z}_n\}$ is mapped to the set $\{c'_i \mid i \in \mathbb{Z}_n\}$, while the set $\{c_i \mid i \in \mathbb{Z}_n\}$ is mapped to the set $\{r'_i \mid i \in \mathbb{Z}_n\}$.

It may be noted that the case where $c = \delta$ is covered by all three cases above. Furthermore, if $\{r_i c_i \mid i \in \mathbb{Z}_n\} \in E(G)$, then the permutation applied to the set $\{r_i \mid i \in \mathbb{Z}_n\}$ is equal to the permutation applied to the set $\{c_i \mid i \in \mathbb{Z}_n\}$, which is equivalent to stating that the permutation applied to the rows and columns of $\boldsymbol{L}$ must be equal. The same is true for the cases where $\{r_i s_i \mid i \in \mathbb{Z}_n\} \in E(G)$ and $\{c_i s_i \mid i \in \mathbb{Z}_n\} \in E(G)$. Finally, the set $\{\ell_{ij} \mid i, j \in \mathbb{Z}_n\}$ can only be mapped to the set $\{\ell'_{ij} \mid i, j \in \mathbb{Z}_n\}$, and this mapping is uniquely defined by the permutations applied to the sets $\{r_i \mid i \in \mathbb{Z}_n\}$, $\{c_i \mid i \in \mathbb{Z}_n\}$ and $\{s_i \mid i \in \mathbb{Z}_n\}$. ■

The following corollary (which follows directly from the preceding theorem) may be used, together with the computer program `nauty`, to determine the σ-autotransformation group of a Latin square for any σ-transformation.

Corollary 4.4.1 *Given any σ-transformation of Latin squares of order n, the automorphism group of the σ-transformation graph of a Latin square $\boldsymbol{L}$ of order n is isomorphic to the σ-autotransformation group of $\boldsymbol{L}$.*

In order to determine the σ-autotransformation group of a Latin object, the direct product of the automorphism groups of the σ-transformation graphs of the Latin squares in the object may be taken. However, in order to determine the autoparatopism group of a k-MOLS of order n a graph similar to the one above is required. For any k-MOLS $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \ldots, \boldsymbol{L}_{k-1})$ of order

n, the *paratopism graph* of $\mathcal{M}$ is a mixed graph G with vertex set

$$V(G) = \{\ell_{ij} \mid i, j \in \mathbb{Z}_n\} \cup \{v_{ij} \mid i \in \mathbb{Z}_n, j \in \mathbb{Z}_{k+2}\} \cup \{V_i \mid i \in \mathbb{Z}_{k+2}\}.$$

The elements of $V(G)$ are coloured by using three colours, where Colour 1 is assigned to $\{\ell_{ij} \mid i, j \in \mathbb{Z}_n\}$, Colour 2 is assigned to $\{v_{ij} \mid i \in \mathbb{Z}_n, j \in \mathbb{Z}_{k+2}\}$ and Colour 3 is assigned to $\{V_i \mid i \in \mathbb{Z}_{k+2}\}$. Furthermore, for each tuple $(i, j, \boldsymbol{L}_0(i,j), \boldsymbol{L}_1(i,j), \ldots, \boldsymbol{L}_{k-1}(i,j)) \in T(\mathcal{M})$ the edge set $E(G)$ contains the edges $v_{i0}\ell_{ij}$, $v_{i0}V_0$, $v_{j1}\ell_{ij}$, $v_{j1}V_1$, $v_{gh}\ell_{ij}$ and $v_{gh}V_h$, where $g = \boldsymbol{L}_{h-2}(i,j)$ for all $h \in \mathbb{Z}_{k+2} \backslash \{0, 1\}$.

For example, the paratopism graph of the pair of orthogonal Latin squares

$$\mathcal{M}_{4.1} = \left(\begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \right),$$

is shown in Figure 4.3.

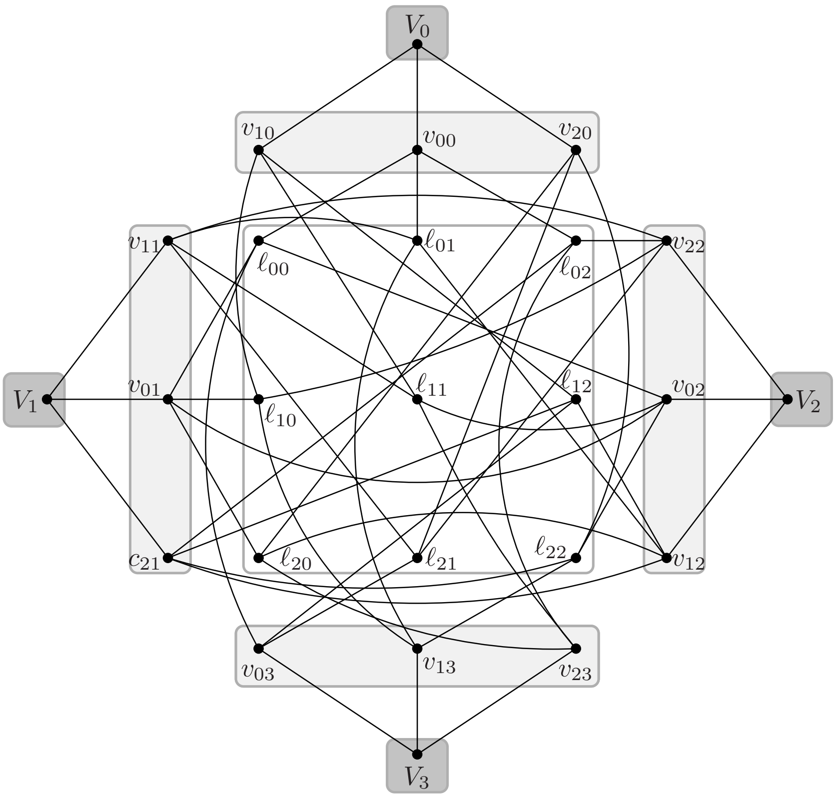

FIGURE 4.3: *The paratopism graph of the 2-MOLS $\mathcal{M}_{4.1}$.*

The following theorem and corollary provide a means for determining the autoparatopism group of a k-MOLS of order n.

Theorem 4.4.2 *Two k-MOLS of order n are in the same main class if and only if their paratopism graphs are isomorphic.*

Proof: Let $\mathcal{M}$ and $\mathcal{M}'$ be k-MOLS of order n with paratopism graphs G and G', respectively, and let

$$V(G) = \{\ell_{ij} \mid i, j \in \mathbb{Z}_n\} \cup \{v_{ij} \mid i \in \mathbb{Z}_n, j \in \mathbb{Z}_{k+2}\} \cup \{V_i \mid i \in \mathbb{Z}_{k+2}\}$$

and

$$V(G') = \{\ell'_{ij} \mid i, j \in \mathbb{Z}_n\} \cup \{v'_{ij} \mid i \in \mathbb{Z}_n, j \in \mathbb{Z}_{k+2}\} \cup \{V'_i \mid i \in \mathbb{Z}_{k+2}\}.$$

It is easy to see that for each $j \in \mathbb{Z}_{k+2}$ an isomorphism from G to G' maps the subset $\{v_{ij} \mid i \in \mathbb{Z}_n\}$ of $V(G)$ (in some order) to some subset $\{v'_{ij'} \mid i \in \mathbb{Z}_n\}$ of $V(G)$, where j not necessarily equals j'. Since this is equivalent to a conjugate operation together with a permutation applied either to the row indices of all Latin squares in $\mathcal{M}$, to the column indices of all Latin squares in $\mathcal{M}$ or to the symbols of some Latin square in $\mathcal{M}$, an isomorphism between G and G' is equivalent to a paratopism between $\mathcal{M}$ and $\mathcal{M}'$. ■

Corollary 4.4.2 *The automorphism group of the paratopism graph of a k-MOLS $\mathcal{M}$ of order n is isomorphic to the autoparatopism group of $\mathcal{M}$.*

4.5 Group theoretic enumeration of Latin squares

The main assumptions for this section, given any transformation of type σ of Latin objects of order n, are (i) that a set $\mathcal{C}(\sigma, n)$ of Latin objects of order n is given such that no two elements of this set are found in the same σ-transformation class, (ii) that there are exactly $|\mathcal{C}(\sigma, n)|$ σ-transformation classes of Latin objects of order n and (iii) that the σ-autotransformation group of every Latin object in $\mathcal{C}(\sigma, n)$ is known. In the remainder of this section it is shown how Latin objects, Latin object classes as well as various types of Latin objects may be enumerated utilising results from abstract algebra under the above assumptions.

Theorem 4.5.1 *Denote the σ-transformation group acting on the set of all Latin objects of order n by $G_\sigma(n)$ and denote the σ-autotransformation group of a Latin object $\mathcal{O}$ by $A_\sigma(\mathcal{O})$. Then the total number of Latin objects of order n is*

$$\sum_{\mathcal{O} \in \mathcal{C}(\sigma, n)} \frac{|G_\sigma(n)|}{|A_\sigma(\mathcal{O})|}.$$

Proof: Since $A_\sigma(\mathcal{O}) = \{\alpha \mid \mathcal{O}^\alpha = \mathcal{O}\}$, this group is the stabiliser of the element $\mathcal{O}$ by Definition A.2.9. By the orbit-stabiliser theorem (see Lemma A.2.1), the number of Latin objects of order n in the σ-transformation class containing $\mathcal{O}$ is $|G_\sigma(n)|/|A_\sigma(\mathcal{O})|$ since $G_\sigma(n)$ is a group acting on the set of all Latin objects of order n and since $A_\sigma(\mathcal{O})$ is a stabiliser. By the assumptions on the properties of $\mathcal{C}(\sigma, n)$, the desired result follows. ■

For example, consider the two non-isotopic Latin squares

$$\boldsymbol{L}_{4.15} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad \text{and} \quad \boldsymbol{L}_{4.16} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{bmatrix}$$

of order 4 (see Colbourn *et al.* [38, p. 137]). Since there are only two isotopy classes of Latin squares of order 4, these two Latin squares together form the set $\mathcal{C}((\pi_r, \pi_c, \pi_s), 2)$. Using Algorithm 4.2, the autotopy groups of each of these Latin squares may easily be computed via MATHEMATICA. The orders of the autotopism groups of $\boldsymbol{L}_{4.15}$ and $\boldsymbol{L}_{4.16}$ are 96 and 32 respectively, and the total number of Latin squares of order 4 therefore is $(4!)^3/96 + (4!)^3/32 = 576$.

Theorem 4.5.1 may also be used to establish relationships between the numbers of various types of Latin squares, as the following corollaries illustrate.

Corollary 4.5.1 *The number of diagonal Latin squares of order n is $n!$ times the number of idempotent Latin squares of order n.*

Proof: It is easy to see that any (π_s)-autotransformation class of diagonal Latin squares contains exactly one idempotent Latin square, and that the (π_s)-autotransformation group of any Latin square has order one. Hence the number of (π_s)-transformation classes of diagonal Latin squares of order n equals the number of idempotent Latin squares of order n, and since the (π_s)-transformation group has order $n!$, the desired result follows from Theorem 4.5.1. ■

The next corollary is a well-known result. See Laywine and Mullin [88, Theorem 1.2] for an alternative proof of this result.

Corollary 4.5.2 *The number of Latin squares of order n is $n!(n-1)!$ times the number of reduced Latin squares of order n.*

Proof: Consider applying a column permutation to a Latin square and a row permutation only to the last $n-1$ rows of the Latin square. Hence the group $S_n \times S_{n-1}$ acts on the set of Latin squares of order n in this way, and it is therefore a valid transformation (although no type has been defined for such a transformation). It is easy to see that the autotransformation group of any Latin square in this case has order one, and that any such class contains exactly one reduced Latin square. As in the proof of Corollary 4.5.1, the result follows since the group $S_n \times S_{n-1}$ has order $n!(n-1)!$. ■

A similar relationship to the one given above may be established for k-MOLS of order n and *reduced* k-MOLS of order n, where a *reduced* k-MOLS of order n is a row-reduced k-MOLS $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \dots, \boldsymbol{L}_{k-1})$ of order n such that $\boldsymbol{L}_0(i,0) = i$ for all $i \in \mathbb{Z}_n$ (*i.e.* a row-reduced k-MOLS in which the first column of the first Latin square is in natural order).

Corollary 4.5.3 *The number of k-MOLS of order n is $(n!)^k(n-1)!$ times the number of reduced k-MOLS of order n.*

Proof: Consider the action of the group $S_n^k \times S_{n-1}$ on the set of all k-MOLS of order n where, given a k-MOLS $\mathcal{M} = (\boldsymbol{L}_0, \boldsymbol{L}_1, \dots, \boldsymbol{L}_{k-1})$ of order n, a unique symbol permutation is applied to each $\boldsymbol{L}_i$ for $0 \leq i \leq k-1$ and where a permutation of order $n-1$ is applied to the last $n-1$ rows of $\boldsymbol{L}_i$ for all $0 \leq i \leq k-1$. It is easy to see that the autotransformation group of any Latin square in this case has order one, and that any such class contains exactly one reduced k-MOLS of order n. Since the group $S_n^k \times S_{n-1}$ has order $(n!)^k(n-1)!$, the desired result follows by Corollary 4.5.1. ■

It is also sometimes useful to enumerate the number of *subtransformation classes* of a transformation class. Given any transformation σ of order n, the *subtransformation* of σ, denoted by $\bar{\sigma}$, is the resulting transformation if all symbols of the form $\pi_{t_i}^{(j)}$ for all $1 \leq i \leq 3$ and $1 \leq j \leq m$ are removed and replaced by the symbol $\pi_{rcs}^{(1,\dots,m)}$. Hence all σ-permissible n-permutations are restricted to be equal. Any $\bar{\sigma}$-transformation is therefore a special case of a σ-transformation. In this case the transformation group will always be the direct product of S_n and some subgroups of D_3. For example, if $\sigma = (\pi_{rc}^{(1)}, \pi_s^{(1)}, \pi_r^{(2)}, \pi_c^{(2)}, \pi_s^{(2)}, \tau^{(1)}, \delta^{(2)})$ then $\bar{\sigma} = (\pi_{rcs}^{(1,2)}, \tau^{(1)}, \delta^{(2)})$ and the $\bar{\sigma}$-transformation group is $S_n \times S_2 \times D_3$. The most common example of a subtransformation class, however, is a isomorphism class of Latin squares, which is a subtransformation class of an isotopy class of Latin squares.

The following lemma and theorem are an adaptation of Theorem 4 in McKay *et al.* [99], which counts the number of isomorphism classes of Latin squares in each isotopy class of Latin squares. The theorem was also adapted in [32] and [33] to count subtransformation classes of special types of Latin squares which are considered later in this dissertation. The theorem is extended here to the general case where the number of subtransformation classes within any given transformation class is to be counted.

Suppose the subtransformation classes within the σ-transformation class containing the Latin object $\mathcal{O}$, say $\mathcal{C}$, are to be enumerated, and let $A_\sigma(\mathcal{O})$ be the σ-autotransformation group of $\mathcal{O}$. Since the $\bar{\sigma}$-transformation classes are orbits on $\mathcal{C}$, it follows by the Cauchy-Frobenius Lemma (see Lemma A.2.2) that the number of $\bar{\sigma}$-transformation classes in $\mathcal{C}$ equals the sum of the number of $\bar{\sigma}$-autotransformations of each element in $\mathcal{C}$ divided by the size of the $\bar{\sigma}$-transformation group. The key to the proof of the following theorem is to represent each σ-autotransformation of each element of the class in terms of the elements of $A_\sigma(\mathcal{O})$, and to count those which are $\bar{\sigma}$-autotransformations.

If $\mathcal{O}' \in \mathcal{C}$ then there exists some σ-transformation θ such that $\mathcal{O}^\theta = \mathcal{O}'$, and Figure 4.4 illustrates how $\theta\alpha\theta^{-1}$ is an σ-autotransformation of $\mathcal{O}'$ for any $\alpha \in A_\sigma(\mathcal{O})$. This is true since

$$(\mathcal{O}')^{\theta\alpha\theta^{-1}} = (\mathcal{O}^\theta)^{\theta\alpha\theta^{-1}} = \mathcal{O}^{\theta\alpha} = \mathcal{O}^\theta = \mathcal{O}'.$$

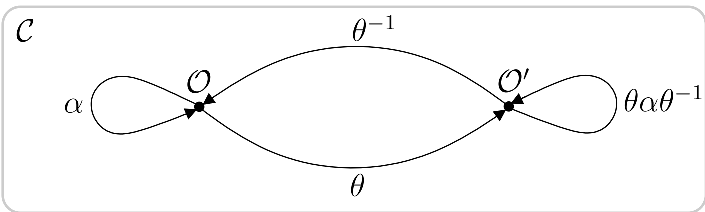

FIGURE 4.4: *Suppose θ is a σ-transformation, that $\mathcal{O}$ and $\mathcal{O}' = \mathcal{O}^\theta$ are both in the σ-transformation class $\mathcal{C}$ and that α is a σ-autotransformation of $\mathcal{O}$. The directed cycle starting at $\mathcal{O}'$ following the arcs labelled θ^{-1}, α and θ (in that order) terminates at $\mathcal{O}'$, and therefore the product $\theta\alpha\theta^{-1}$ of these three transformations is a σ-autotransformation of $\mathcal{O}'$.*

Hence it is necessary, for all $\alpha \in A_\sigma(\mathcal{O})$, to count the number of ways in which $\theta\alpha\theta^{-1}$ is a $\bar{\sigma}$-autotransformation of some Latin object in $\mathcal{C}$ for all σ-transformations θ. Denote the σ-transformation group by G_σ. Let $\alpha, \beta \in A_\sigma(\mathcal{O})$ and let $\mathcal{O}^\theta = \mathcal{O}^\eta = \mathcal{O}'$ for $\theta, \eta \in G_\sigma$. If $\theta\alpha\theta^{-1} = \eta\beta\eta^{-1}$, then this σ-autotransformation is counted twice. The following lemma helps to overcome this obstacle.

Lemma 4.5.1 *Let $A_\sigma(\mathcal{O})$ be the σ-autotransformation group of a Latin object $\mathcal{O}$ and let G_σ be the σ-transformation group. Define an equivalence relation $\sim$ such that $(\theta, \alpha) \sim (\eta, \beta)$ if and only if $\theta\alpha\theta^{-1} = \eta\beta\eta^{-1}$ and $\mathcal{O}^\theta = \mathcal{O}^\eta$ for some $\theta, \eta \in G_\sigma$ and $\alpha, \beta \in A_\sigma(\mathcal{O})$. Then each equivalence class induced by this relation has cardinality $|A_\sigma(\mathcal{O})|$.*

Proof: Let (θ, α) be a pair for which $\theta \in G_\sigma$ and $\alpha \in A_\sigma(\mathcal{O})$. For any $\lambda \in A_\sigma(\mathcal{O})$, let $\eta = \theta\lambda$ and $\beta = \lambda^{-1}\alpha\lambda$. Then $\eta\beta\eta^{-1} = \theta\lambda\lambda^{-1}\alpha\lambda\lambda^{-1}\theta^{-1} = \theta\alpha\theta^{-1}$. Furthermore, $\beta \in A_\sigma(\mathcal{O})$, $\eta \in G_\sigma$ and $\mathcal{O}^\eta = \mathcal{O}^{\theta\lambda} = \mathcal{O}^\theta$, and therefore $(\theta, \alpha) \sim (\eta, \beta)$. Hence for any element of $A_\sigma(\mathcal{O})$ there exists a unique pair (η, β) such that $(\theta, \alpha) \sim (\eta, \beta)$ and so the equivalence classes induced by $\sim$ has cardinality at least $|A_\sigma(\mathcal{O})|$.

Suppose $(\eta', \beta') \sim (\theta, \alpha)$ is not in the set of $|A_\sigma(\mathcal{O})|$ pairs equivalent to (θ, α) counted above, for some $\eta' \in G_\sigma$ and $\beta' \in A_\sigma(\mathcal{O})$. Then $\theta^{-1}\eta' = \lambda$, for some $\lambda \in A_\sigma(\mathcal{O})$, and

$$\theta\alpha\theta^{-1} = \eta'\beta'\eta'^{-1} = \theta\lambda\beta'\lambda^{-1}\theta^{-1}.$$

Hence $\beta' = \lambda\alpha\lambda^{-1}$ and $\eta' = \theta\lambda$, and so (η', β') has already been counted above. The equivalence classes therefore also have cardinality at most $|A_\sigma(\mathcal{O})|$. ■

Utilising the above lemma, the following theorem enumerates the $\bar{\sigma}$-transformation classes in any σ-transformation class.

Theorem 4.5.2 *Let $A_\sigma(\mathcal{O})$ be the σ-autotransformation group of a Latin object $\mathcal{O}$ with parameters (n, m) and suppose there are k σ-permissible n-permutations. Then the number of $\bar{\sigma}$-transformation classes in the σ-transformation class of $\mathcal{O}$ is*

$$\sum_{\alpha \in A_\sigma(\mathcal{O})} \frac{\psi(\alpha)^{k-1}}{|A_\sigma(\mathcal{O})|},$$

where

$$\psi(\alpha) = \begin{cases} \prod_{i=1}^{n} a_i! i^{a_i}, & \text{if all } n\text{-permutations in } \alpha \text{ are of the same type,} \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Let $\hat{D}_3^{(i)}$ be the subgroup of D_3 from which the σ-permissible conjugate operations for $\boldsymbol{L}_i \in \mathcal{O}$ are taken. Then the transformation group of a $\bar{\sigma}$-transformation is $S_n \times \hat{D}_3^{(1)} \times \ldots \times \hat{D}_3^{(m)}$, henceforth simply denoted by $G_{\bar{\sigma}}$. Also, let $\mathcal{C}$ denote the σ-transformation class containing $\mathcal{O}$ and let G_σ denote the σ-transformation group.

As noted before, it is necessary to count, for all $\alpha \in A_\sigma(\mathcal{O})$ and $\beta \in G_\sigma$, the number of ways in which $\theta\alpha\theta^{-1}$ is a $\bar{\sigma}$-autotransformation. There is no restriction on the conjugate operations of θ, and they may be chosen in $\prod_{i=1}^{m} |\hat{D}_3^{(i)}|$ distinct ways. In order for $\theta\alpha\theta^{-1}$ to be a $\bar{\sigma}$-autotransformation, all n-permutations in $\theta\alpha\theta^{-1}$ should be equal, and, by Proposition A.1.2, all n-permutations in α should therefore be of the same type. One of the n-permutations of θ may be chosen in $n!$ ways, but the remaining $k-1$ have to be chosen in such a way that all n-permutations of $\theta\alpha\theta^{-1}$ are equal. But this can only be true if all n-permutations of α are of the same type. If they are of the same type, say $(a_1, a_2, \ldots, a_n)$, then by Proposition A.1.3 there are $\prod_{i=1}^{n} a_i! i^{a_i}$ distinct ways of selecting each of the remaining $k-1$ permutations of θ. Otherwise there are zero ways of selecting the n-permutations of θ.

Define, for any $\alpha \in A_\sigma(\mathcal{O})$, the function $\psi(\alpha) = \prod_{i=1}^{n} a_i! i^{a_i}$ if all n-permutations in α are of type $(a_1, a_2, \ldots, a_n)$, or zero otherwise. Then there are

$$\psi(\alpha)^{k-1} \prod_{i=1}^{m} \left|\hat{D}_3^{(i)}\right|$$

choices of θ for which $\theta\alpha\theta^{-1}$ is an $\bar{\sigma}$-autotransformation of some Latin object, for some $\alpha \in A_\sigma(\mathcal{O})$.

Since any $\bar{\sigma}$-autotransformation of any Latin object in $\mathcal{C}$ may be written in the form $\theta\alpha\theta^{-1}$ for some σ-transformation θ and some $\alpha \in A_\sigma(\mathcal{O})$, the number

$$n! \sum_{\alpha \in A_\sigma(\mathcal{O})} \psi(\alpha)^{k-1} \prod_{i=1}^{m} \left|\hat{D}_3^{(i)}\right|$$

counts all $\bar{\sigma}$-autotransformations of each element in $\mathcal{C}$ at least once. As noted before, it is not guaranteed that no $\bar{\sigma}$-autotransformation has been counted more than once, and Lemma 4.5.1 may therefore be employed to remove these redundancies. It is easy to see that the type of the elements of $A_\sigma(\mathcal{O})$ are invariant under the equivalence classes considered in Lemma 4.5.1, and the equivalence classes consisting of $\bar{\sigma}$-autotransformations therefore have cardinality $|A_\sigma(\mathcal{O})|$. Hence there are exactly

$$\frac{n!}{|A_\sigma(\mathcal{O})|} \sum_{\alpha \in A_\sigma(\mathcal{O})} \psi(\alpha)^{k-1} \prod_{i=1}^{m} \left|\hat{D}_3^{(i)}\right|$$

$\bar{\sigma}$-autotransformations of the elements of $\mathcal{C}$. By the Cauchy-Frobenius Lemma (see Lemma A.2.2), this number has to be divided by $|G_{\bar{\sigma}}| = n! \prod_{i=1}^{m} |\hat{D}_3^{(i)}|$, thereby delivering the desired result. ■

Consider, for example, the set $\mathcal{C}((\pi_r, \pi_c, \pi_s), 2) = \{\boldsymbol{L}_{4.15}, \boldsymbol{L}_{4.16}\}$ containing two non-isotopic Latin squares of order 4. Previously in this subsection the autotopy groups of these Latin squares were computed in MATHEMATICA using Algorithm 4.2. By Theorem 4.5.2, if $A(\boldsymbol{L}_{4.15})$ and $A(\boldsymbol{L}_{4.16})$ are the isotopy groups of $\boldsymbol{L}_{4.15}$ and $\boldsymbol{L}_{4.16}$ respectively and since an isomorphism is a subtransformation of an isotopism, the number of isomorphism classes of Latin squares of order 4 is

$$\sum_{\alpha \in A(\boldsymbol{L}_{4.15})} \frac{\psi(\alpha)^2}{96} + \sum_{\alpha \in A(\boldsymbol{L}_{4.16})} \frac{\psi(\alpha)^2}{32}.$$

The values for $\psi(\alpha)$ may be calculated in MATHEMATICA by using the function `PermutationType`, from which it follows that $\sum_{\alpha \in A(\boldsymbol{L}_{4.15})} \psi(\alpha)^2 = 1\,440$ and $\sum_{\alpha \in A(\boldsymbol{L}_{4.16})} \psi(\alpha)^2 = 640$. Hence the number of isomorphism classes of Latin squares of order 4 is $1\,440/96 + 640/32 = 35$.

4.6 Chapter summary

In §4.1 the notion of a transformation class of Latin squares was defined. Such a class is the equivalence class of Latin squares induced by the group action of a transformation group on the set of all Latin squares of a certain order. The elements of such a transformation group are combinations of various operations that may be applied to Latin squares without destroying their defining property. Notation was introduced in order for various results on the enumeration of these transformation classes to be established in general (*i.e.* for any given transformation group) and so that various algorithms which may be utilised for enumeration purposes may also be described in general. A number of special types of equivalence classes of Latin squares were also introduced in this section, namely isomorphism classes, isotopy classes, main classes, RC-paratopism classes, transpose-isomorphism classes, as well as equivalents of the latter two.

A brief historical account of various attempts by researchers to enumerate Latin squares and various classes of Latin squares of orders $1 \leq n \leq 11$ was given in §4.2. A table of enumeration results for various classes of Latin squares was also provided in this section.

In §4.3 a backtracking tree-search approach towards enumerating any σ-transformation class of Latin squares was presented. Before branching on a partially completed Latin square, this method ensures that the square has the potential to be completed to the class leader of a σ-transformation class, where a class leader is defined uniquely for each class. This method therefore generates a class representative from each σ-transformation class, thereby enumerating the total number of σ-transformation classes. The working of the method was illustrated by an enumeration of the isomorphism classes generated by reduced N_2-squares (Latin squares without 2×2-subsquares) of order 5, and an application of this method to the enumeration of RC-paratopism classes of Latin squares and to the enumeration of main classes of MOLS was also discussed in detail.

In §4.4 it was illustrated how a graph may be constructed from a given Latin square $\boldsymbol{L}$ and a given transformation type σ in such a way that the σ-autotransformation group of $\boldsymbol{L}$ is isomorphic to the automorphism group of the graph. This is useful for the computation of autotransformation groups of Latin squares since the well-known computer program `nauty` [96] may be used to determine the automorphism group of any graph. Once the σ-autotransformation group of a Latin square $\boldsymbol{L}$ is determined, results from group theory (in particular, the orbit-stabiliser theorem and the Cauchy-Frobenius Lemma) may be used to compute the size of the σ-transformation class of which $\boldsymbol{L}$ is a member, as well as various special types of subclasses of this class, and methods for achieving these computations were presented in §4.5. An illustrative example was also presented in this section in which it was shown how the autotopy groups of the two non-isotopic Latin squares of order 4 may be used to count the total number of Latin squares in each of these classes, as well as the number of isomorphism classes within each class.

CHAPTER 5

Enumeration results

Contents

In this chapter the enumeration methodology presented in Chapter 4 is applied to the problem of enumerating SOLS (in §5.2), SOLSSOMs (in §5.3) and MOLS (in §5.4) of various orders, a task that in the literature on Latin squares has only been partly addressed for SOLS and MOLS, and not at all for SOLSSOMs. Two approaches to this problem are compared in §5.1, and some motivation is given as to why one approach may prove to be more efficient than the other in terms of the required enumeration computing time. In §5.2.1 the RC-paratopism classes of SOLS of orders $4 \leq n \leq 10$ are enumerated (the trivial cases of $n = 2, 3$ are omitted), while §5.2.2 contains enumeration results on isomorphism classes and transpose-isomorphism classes generated by SOLS, as well as the number of distinct and idempotent SOLS of various orders. In §5.3.1 the RC-paratopism classes of SOLSSOMs of orders $4 \leq n \leq 10$ are enumerated using two independent methods, and in §5.3.2 a method is described by which it may be shown that there is no SOLSSOM of order 10. The number of distinct SOLSSOMs, standard SOLSSOMS and transpose-isomorphism classes of SOLSSOMs are thereafter determined in §5.3.3. In §5.4.1 the main classes of k-MOLS of orders $3 \leq n \leq 8$ are enumerated for $2 \leq k \leq 7$, and in §5.4.2 the number of reduced and distinct k-MOLS of these orders are determined. Computing times are reported where methods performed on a computer required more than one second to complete, and computations were performed on two computing resources, namely on 3GHz Intel(R) dual core processors, each with 4GB RAM (henceforth referred to as *Computing Resource 1*), and on Stellenbosch University's *Rasatsha High Performance Computer* [132], which consists of 168

2.83GHz processors, each with 336GB RAM (henceforth referred to as *Computing Resource 2*). Implementations of the methods in this chapter were done in parallel on both computing resources.

5.1 Two enumeration approaches for orthogonal Latin squares

In §4.3 an algorithm was presented for the enumeration of classes of Latin squares using a backtracking tree-search which branches on the inclusion of rows in a partially completed Latin square. When enumerating orthogonal Latin squares using this method there are two approaches to restricting the rows included in order for the Latin squares eventually generated to be orthogonal to one another, one of which is equivalent to branching on the inclusion of universals (as was the case in the algorithm described in §4.3.2). In what follows each of these two approaches are discussed, and their efficiency in terms of the required enumeration computing times are compared.

Let $\boldsymbol{L}_0$ and $\boldsymbol{L}_1$ be Latin squares of order n which have been obtained via the backtracking tree-search described in §4.3, where, for every pair of permutations r_1 and r_2 which were considered for inclusion as the m-th rows (for some $m < n$) of $\boldsymbol{L}_0$ and $\boldsymbol{L}_1$, respectively, a restriction has been enforced which requires that the sets of pairs $\{(r_0(i), r_1(i)) \mid i \in \mathbb{Z}_n\}$ and $\{(\boldsymbol{L}'_0(i,j), \boldsymbol{L}'_1(i,j)) \mid i \in \mathbb{Z}_m, j \in \mathbb{Z}_n\}$ are disjoint. Since this restriction ensures that the pairs $(\boldsymbol{L}'_0(i,j), \boldsymbol{L}'_1(i,j))$ are unique as i and j vary over $\mathbb{Z}_n$, $\boldsymbol{L}_0$ and $\boldsymbol{L}_1$ are orthogonal. Hence in this approach rows are inserted as the search progresses, subject to the restriction that every partial universal formed in the one square must intersect (*i.e.* have an entry in common with) each partial universal in the other square at most once.

Now let $\boldsymbol{L}_0$, $\boldsymbol{L}_1$, r_0 and r_1 assume the same roles as above, but where a different restriction has been enforced, namely one which requires that, for any $i < m$, there exists exactly one element $j_0 \in \mathbb{Z}_n$ such that $r_0(j_0) = \boldsymbol{L}_1(i, j_0)$, exactly one element $j_1 \in \mathbb{Z}_n$ such that $r_1(j_1) = \boldsymbol{L}_0(i, j_1)$, and exactly one element $k \in \mathbb{Z}_n$ such that $r_0(k) = r_1(k)$. This restriction therefore ensures that, for each pair $(i_0, i_1) \in \mathbb{Z}_n^2$, there exists exactly one element $j \in \mathbb{Z}_n$ such that $\boldsymbol{L}_1(i_0, j) = \boldsymbol{L}_1(i_1, j)$, which implies that the pair $(({}^{-1}\boldsymbol{L}_0)^T(i,j), ({}^{-1}\boldsymbol{L}_1)^T(i,j))$ is unique as i and j vary ${\mathbb{Z}_n}$[1]. Hence $({}^{-1}\boldsymbol{L}_0)^T$ and $({}^{-1}\boldsymbol{L}_1)^T$ are orthogonal. Since the universal permutations of $({}^{-1}\boldsymbol{L}_0)^T$ represent the rows of $\boldsymbol{L}_0$, this approach is equivalent to branching on the inclusion of universals, while ensuring that each universal included in one Latin square intersects each universal already included in the other Latin square exactly once.

The difference between the two approaches described above lies in the fact that in the first approach one entry of each universal is included on each level of the tree, while in the second approach all entries of one universal are included on each level of the tree. Furthermore, in the first approach every two universals that do not appear in the same Latin square must intersect at most once, while in the second approach every two universals that do not appear in the same Latin square must intersect exactly once. Hence the first approach is less restrictive (especially on the lower levels of the tree) than the second.

This phenomenon may be observed from Table 5.1, which gives the number of branches on each level of the search tree for reduced k-MOLS of order n for both the above approaches. These numbers were obtained by utilising the backtracking algorithm described in §4.3 subject to the restrictions above together with an additional restriction which ensures that the k-MOLS generated are reduced. As may be seen from the table, the first approach gives rise to more

[1] Recall that $\boldsymbol{L}(i,j) = k$ implies that $({}^{-1}\boldsymbol{L})^T(j,k) = i$.

branches in the search tree than the second, as expected. Furthermore, the required computing time for finding these numbers is negligible for the second approach, whereas for the first approach it is negligible for $n < 6$ only, while for $n = 6$ the search already requires 11 seconds, 65 seconds, 20 seconds and 2 seconds for $k = 2$, 3, 4 and 5, respectively.

	First approach (rows)						Second approach (universals)					
	Level						Level					
(n,k)	1	2	3	4	5	6	1	2	3	4	5	6
$(4,2)$	1	8	8	2			2	2	2	2		
$(4,3)$	1	8	2	2			2	2	2	2		
$(5,2)$	1	138	660	18	18		9	42	24	18	18	
$(5,3)$	1	336	36	36	36		24	48	36	36	36	
$(5,4)$	1	336	36	36	36		24	48	36	36	36	
$(6,2)$	1	4 256	564 608	965 844	39 600	0	44	6 312	24 396	2 304	0	0
$(6,3)$	1	78 624	2 897 532	421 728	5 280	0	552	10 512	36	0	0	0
$(6,4)$	1	225 792	237 600	10 560	9 360	0	1 344	432	0	0	0	0
$(6,5)$	1	225 792	0	0	0	0	1 344	432	0	0	0	0

TABLE 5.1: *The number of branches on each level of the search tree for each of the two approaches to enumerating reduced k-MOLS of order n, namely branching on the inclusion of rows and branching on the inclusion of universals.*

By the discussions above and from the findings summarised in Table 5.1 it is clear that branching on the inclusion of universals is a more efficient approach to the enumeration of orthogonal Latin squares than branching on the inclusion of rows, and for this reason the enumeration algorithms in this dissertation for SOLS, SOLSSOMs and MOLS all follow this approach.

5.2 Enumeration of self-orthogonal Latin squares

For the purpose of enumerating classes of SOLS it is necessary to identify the transformations under which the property of self-orthogonality is invariant. In §2.2 it was shown that in order for a transformation to preserve the property of orthogonality between two Latin squares, any permutation applied to the rows (columns, respectively) of the one Latin square must also be applied to the rows (columns, respectively) of the other. Since a SOLS is orthogonal to its transpose, it therefore follows that any permutation applied to the rows of a SOLS must also be applied to the columns of the SOLS in order to guarantee that the resulting Latin square is again self-orthogonal. Furthermore, a permutation on the symbols may be performed independently of the permutation applied to the rows of the SOLS. It may also be noted that the only conjugate operation that necessarily preserves orthogonality is τ (the operation of transposition). Consider, for example, the SOLS

$$\boldsymbol{L}_{5.1} = \begin{bmatrix} 0&2&1&4&3&6&5\\ 3&1&6&0&5&2&4\\ 4&5&2&6&0&3&1\\ 5&6&4&3&1&0&2\\ 6&3&5&2&4&1&0\\ 2&4&0&1&6&5&3\\ 1&0&3&5&2&4&6 \end{bmatrix}$$

of order 7. Since $\boldsymbol{L}_{5.1}(1,5) = 2$ and $\boldsymbol{L}_{5.1}(2,6) = 1$, it follows that $\boldsymbol{L}_{5.1}^{-1}(1,2) = 5$ and $\boldsymbol{L}_{5.1}^{-1}(2,1) = 6$. Similarly, since $\boldsymbol{L}_{5.1}(2,5) = 3$ and $\boldsymbol{L}_{5.1}(3,6) = 2$, it follows that $\boldsymbol{L}_{5.1}^{-1}(2,3) = 5$ and $\boldsymbol{L}_{5.1}^{-1}(3,2) = 6$, contradicting the property of self-orthogonality in $\boldsymbol{L}_{5.1}^{-1}$. Since $\boldsymbol{L}_{5.1}(6,0) = 1$

and $\boldsymbol{L}_{5.1}(6,1)=0$, it follows that ${}^{-1}\boldsymbol{L}_{5.1}(1,0)=6={}^{-1}\boldsymbol{L}_{5.1}(0,1)$, and hence ${}^{-1}\boldsymbol{L}_{5.1}$ cannot also be self-orthogonal. Finally, since the operation of transposition preserves orthogonality, neither $(\boldsymbol{L}_{5.1}^{-1})^T$ nor $({}^{-1}\boldsymbol{L}_{5.1})^T$ is self-orthogonal, and so $\boldsymbol{L}_{5.1}^T$ is the only conjugate of $\boldsymbol{L}_{5.1}$ which is also self-orthogonal.

Hence the only specifications that may be included in the type of a transformation of a SOLS are π_{rc}, π_s, π_{rcs} and τ. Three classes which therefore preserve self-orthogonality include (π_{rcs})-transformation classes (*i.e.* isomorphism classes), (π_{rcs},τ)-transformation classes (*i.e.* transpose-isomorphism classes), as well as (π_{rc},π_s,τ)-transformation classes (*i.e.* RC-paratopism classes), the former two of which also preserve idempotency (as was mentioned in §4.3).

The problem of enumerating SOLS was first considered by Graham and Roberts [66] in 2006. They gave the numbers of distinct SOLS, idempotent SOLS and isomorphism classes generated by idempotent SOLS of orders $n \leq 9$ using a backtracking tree-search approach. They also considered complete sets of mutually orthogonal self-orthogonal Latin squares, and provided information on the sizes of the isomorphism classes and whether or not an isomorphism class contains a SOLS and its transpose. Their results are shown in Table 5.2.

n	Distinct SOLS	Idempotent SOLS	Isomorphism classes generated by idempotent SOLS
4	48	2	1
5	1 440	12	2
6	0	0	0
7	19 353 600	3 840	8
8	4 180 377 600	103 680	8
9	25 070 769 561 600	69 088 320	283

TABLE 5.2: *The numbers of distinct SOLS, idempotent SOLS and isomorphism classes of idempotent SOLS of orders* $4 \leq n \leq 9$ *[66].*

It was noted by Graham and Roberts that the number of distinct SOLS of order n is $n!$ times the number of idempotent SOLS of order n, a fact that follows immediately from Theorem 3.3.1 and Corollary 4.5.1, and which may be observed in Table 5.2. Graham and Roberts also reported that all SOLS of order 4 are isomorphic to their transposes, while no SOLS of order $n \in \{5,7,8\}$ is isomorphic to its transpose. It is easy to see that if $\boldsymbol{L}$ and $\boldsymbol{L}^T$ are isomorphic, then $\boldsymbol{L}^\alpha$ and $(\boldsymbol{L}^\alpha)^T$ are isomorphic for any isomorphism α. In other words, an isomorphism class of SOLS either contains the transposes of each SOLS in the class, or the transposes of no SOLS in the class. For $n=9$, Table 5.3 gives the number of isomorphism classes of idempotent SOLS (categorised according to cardinality) containing SOLS and their transposes and the number of classes not containing transposes.

Cardinality	5 040	45 360	60 480	90 720	120 960	181 440	362 880
Number of classes containing transpose	2	4	4	8	2	36	11
Number of classes not containing transpose	2	20	6	12	0	50	126

TABLE 5.3: *The numbers of isomorphism classes of idempotent SOLS of order 9 either containing or not containing the transposes of the SOLS in the class, categorised according to the cardinality of the class [66].*

Graham and Roberts were not able to extend their search in order to enumerate SOLS of order 10. It is, however, possible to enumerate various classes of SOLS of order 10 utilising the methods discussed in §4, as will be done in the following subsections. The numbers of various other classes of SOLS not enumerated by Graham and Roberts are also given in these subsections for orders $4 \leq n \leq 10$. The methods and results of §5.2.1 and §5.2.2 were published in [33] and [32] respectively, while the methods and results of §5.3 have been submitted for publication [34]. All computations referred to in the following subsections were performed on Computing Resource 1.

5.2.1 Enumeration of RC-paratopism classes of SOLS

In §4.3 it was noted that the number of RC-paratopism classes generated by diagonal Latin squares of order n is equal to the number of transpose-isomorphism classes generated by idempotent Latin squares of order n, and the same holds when these classes are generated by SOLS or idempotent SOLS, respectively.

It follows that the number of transpose-isomorphism classes generated by idempotent SOLS may be derived from the information given on the number of classes containing/not containing transposes. This may be achieved by noting that the isomorphism class generated by a SOLS $\boldsymbol{L}$ which also contains $\boldsymbol{L}^T$ is the transpose-isomorphism class generated by $\boldsymbol{L}$, while the transpose-isomorphism class generated by a SOLS $\boldsymbol{L}$ which is not isomorphic to $\boldsymbol{L}^T$ is the union of the isomorphism classes generated by $\boldsymbol{L}$ and $\boldsymbol{L}^T$, respectively. Hence the number of transpose-isomorphism classes of SOLS equals the number of isomorphism classes containing SOLS and their transposes plus half the number of isomorphism classes not containing transposes. From Table 5.2 the number of transpose-isomorphism classes generated by idempotent SOLS (*i.e.* RC-paratopism classes generated by SOLS) may be derived as 1 for $n = 4$ (since all SOLS of order 4 are isomorphic to their transposes), and 1, 4 and 4 for $n = 5$, 7 and 8, respectively (since none of these SOLS is isomorphic to its transpose). It follows from Table 5.3 that there are

$$(2 + 1) + (4 + 10) + (4 + 3) + (8 + 6) + (2 + 0) + (36 + 25) + (11 + 63) = 175$$

RC-paratopism classes generated by SOLS of order $n = 9$.

These numbers may be verified, and the search extended to include $n = 10$, using the orderly generation backtracking tree-search approach described in §4.3 and §5.1. Since self-orthogonality requires each universal in a Latin square to be a transversal in the transpose of the Latin square, branching on the inclusion of universals in a partially completed SOLS is potentially more restrictive than branching on the inclusion of rows and columns. Theorem 3.3.1, for instance, states that the universal permutation of a universal in a SOLS has exactly one fixed point and no two-cycles. Furthermore, to ensure that the insertion of a universal does not destroy the property of self-orthogonality when inserted into a partially completed SOLS, it is sufficient to verify that the universal forms at least a partial transversal in the transpose of the SOLS.

A complete methodology for the enumeration of row-isomorphism classes generated by idempotent Latin squares was presented in §4.3, and it was also noted that enumerating row-isomorphism classes by inserting rows is equivalent to enumerating transpose-isomorphism classes by inserting universals. Together with the restrictions placed on universals discussed above (where the one fixed point in the universal permutation of the universal of element k should fix k in order for the SOLS to be idempotent), this method therefore enumerates transpose-isomorphism classes generated by idempotent SOLS (*i.e.* RC-paratopism classes of SOLS).

As noted in §4.3, the first universal (the universal of the element 0) must be a cycle structure representative, and for $n = 4$ the only permutations which have only one fixed point and no two-cycles have cycle structure $z_1^1 z_3^1$. The first level of the search tree for $n = 4$ therefore has only one node corresponding to the universal permutation $\binom{0\,1\,2\,3}{0\,2\,3\,1}$. It is easy to then verify that there is only one possible universal for each of the elements 1, 2 and 3, resulting in the SOLS

$$\begin{bmatrix} 0 & 2 & 3 & 1 \\ 3 & 1 & 0 & 2 \\ 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 3 \end{bmatrix},$$

which is the smallest SOLS (when lexicographically comparing the universal permutations in natural order) in the only RC-paratopism class generated by SOLS of order 4.

For $n = 5$ the only permutations which have only one fixed point and no two-cycles have cycle structure $z_1^1 z_4^1$, and once again there is only one possible universal for each element in $\mathbb{Z}_5$, resulting in the SOLS

$$\begin{bmatrix} 0 & 4 & 1 & 2 & 3 \\ 3 & 1 & 0 & 4 & 2 \\ 4 & 3 & 2 & 0 & 1 \\ 1 & 2 & 4 & 3 & 0 \\ 2 & 0 & 3 & 1 & 4 \end{bmatrix},$$

which is the smallest SOLS (when lexicographically comparing the universal permutations in natural order) in the only RC-paratopism class generated by SOLS of order 5.

For $n = 6$ the only permutations which have only one fixed point and no two-cycles conform to the cycle structure $z_1^1 z_5^1$, and hence the first universal permutation is $\binom{0\,1\,2\,3\,4\,5}{0\,2\,3\,4\,5\,1}$. There are two possible universal permutations for the element 1, namely $\binom{0\,1\,2\,3\,4\,5}{2\,1\,4\,5\,3\,0}$ and $\binom{0\,1\,2\,3\,4\,5}{3\,1\,0\,5\,2\,4}$. With the insertion of the former there is only one possible universal for the element 2, but no possible universals for the element 3, while for the latter there is not even a possible universal for the element 2. The search tree therefore produces no SOLS of order 6, as expected.

For $n = 7$ the universal permutations may admit two distinct cycle structures, namely $z_1^1 z_3^2$ and $z_1^1 z_6^1$. The search tree for this case is not as trivial as for the previous cases discussed above, but is still small enough to present in its entirety; this search tree is shown in Figure 5.1. For each branch the universal to be inserted and its cycle structure is given in a shorthand notation where the universal permutation $\binom{0\,1\,2\,3\,4\,5\,6}{a\,b\,c\,d\,e\,f\,g}$ is written simply as *abcdefg* and where the cycle structure $z_i^{a_i}$ is written as i^{a_i}. The two partial SOLS are shown in which only the first universal have been inserted, and the four SOLS that were found by the search are shown at the four leaves of the tree on the seventh level, verifying the number derived above from the results of Graham and Roberts. A SOLS is also shown in which universals for all but one element have been inserted, and where the only possible universal permutation for the remaining element is $\binom{0\,1\,2\,3\,4\,5\,6}{2\,3\,5\,4\,1\,0\,6}$. This universal is not inserted, however, as its cycle structure $z_1^1 z_3^2$ is smaller than that of the first universal, which is $z_1^1 z_6^1$. Finally, for the leaves of the tree that are not on the seventh level it is either indicated [a] that there are no possible universals that would have preserved the property of orthogonality, or [b] that the insertion of any further universals would have resulted in a SOLS which cannot be completed to a class leader.

For $n = 8$ the universal permutations also admit two distinct cycle structures, namely $z_1^1 z_3^1 z_4^1$ and $z_1^1 z_7^1$. The tree in this case is significantly larger than for the case of $n = 7$ (surprisingly so in spite of the fact that there are the same number of RC-paratopism classes for both these cases), and it is therefore not shown here. For the branch on the first level which inserts the universal permutation with cycle structure $z_1^1 z_3^1 z_4^1$ there are 26 branches on the second level,

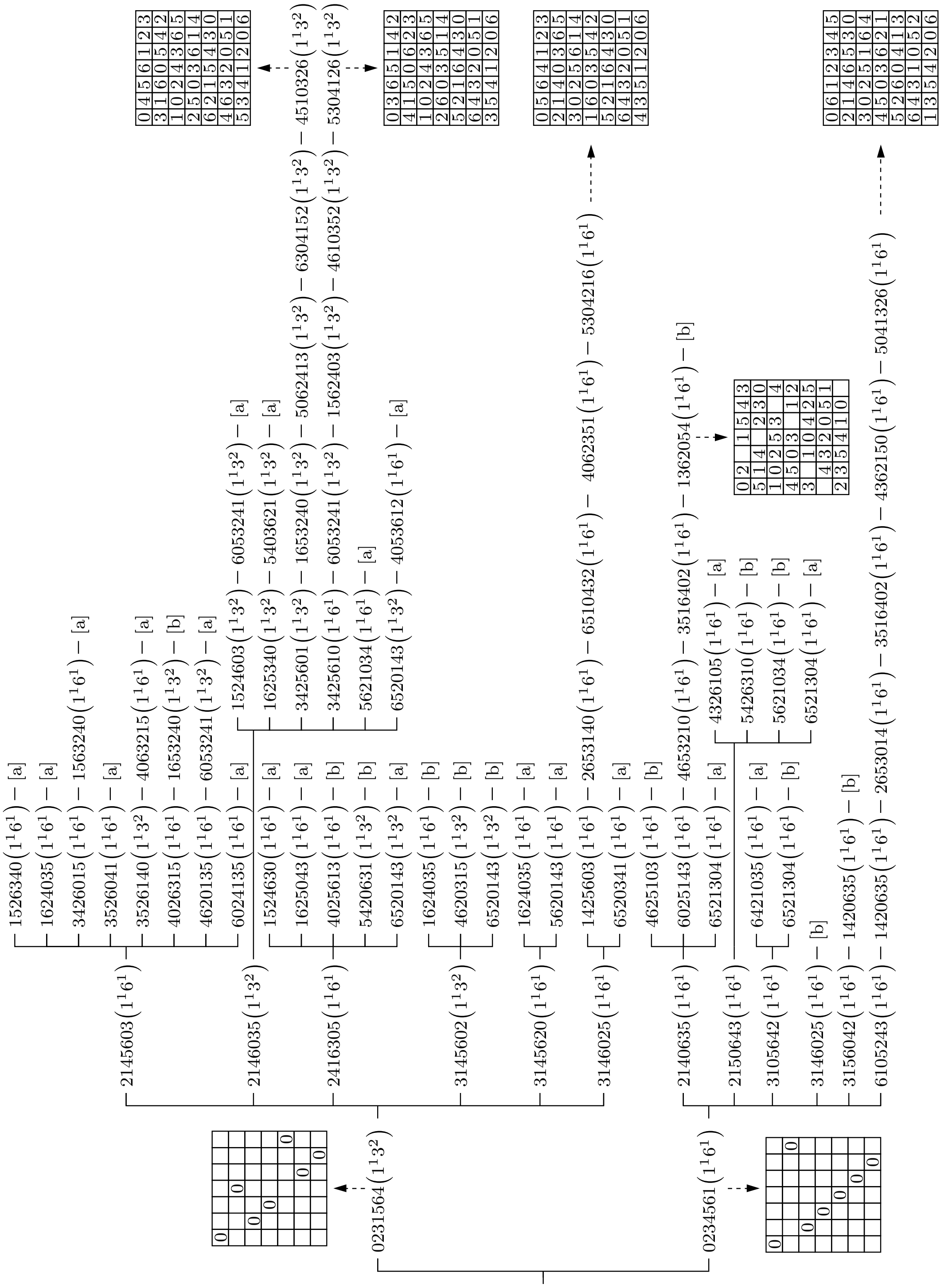

FIGURE 5.1: *The orderly generation search tree for transpose-isomorphism classes generated by idempotent SOLS of order 7. Partial SOLS are shown with only the first universal inserted for the first two branches, as well as a partial SOLS which cannot be completed since the empty entries form a universal permutation with cycle structure smaller than that of the first universal permutation. For each leaf of the tree either the class leader generated is given, or else it is either indicated [a] that there are no possible universals that would have preserved the property of orthogonality, or [b] that the insertion of any further universals would have resulted in a SOLS which cannot be completed to a class leader.*

of which only the third branch eventually produces a SOLS (where the branches are ordered according to the lexicographical ordering of the universal permutations associated with them). For the branch on the first level which inserts the universal permutation with cycle structure $z_1^1 z_7^1$ there are 32 branches on the second level, of which the sixth, fifteenth and twenty-seventh branches each eventually produces one SOLS. This results in a total of four RC-paratopism classes, as also found by Graham and Roberts.

For $n = 9$ the universal permutations admit three distinct cycle structures, namely $z_1^1 z_3^1 z_5^1$, $z_1^1 z_4^2$ and $z_1^1 z_8^1$, and the branches corresponding to these cycle structures result in 148, 115 and 207 branches on the second level, respectively. The number of SOLS found among the 148 branches on the second level corresponding to the cycle structure $z_1^1 z_3^1 z_5^1$ (which amounts to a total of 138 SOLS) is given in Table 5.4. Here the branch number is given, together with the number of SOLS eventually found in that branch as well as the computing time in seconds required to traverse the subtree induced by the branch. Branches that produced no SOLS are not shown in the table.

Branch	2	3	4	5	6	7	8	9	10	11	12	13	14	16	17	19	21	22
SOLS	2	7	3	6	4	5	2	2	1	4	1	4	2	2	1	1	1	7
Time (s)	4	2	2	2	4	3	4	3	4	3	4	3	3	3	2	3	2	2
Branch	23	24	25	27	29	30	31	33	34	35	38	41	44	47	50	52	57	58
SOLS	2	2	2	1	3	4	6	1	2	5	2	3	1	1	2	2	3	2
Time (s)	2	3	2	2	2	3	2	2	1	2	2	2	2	1	2	1	1	2
Branch	61	69	75	77	83	86	87	88	89	90	100	101	106	107	123	128	130	139
SOLS	2	12	1	1	1	1	6	4	1	1	1	1	1	1	1	1	2	1
Time (s)	2	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0

TABLE 5.4: *The number of SOLS of order 9 eventually found for each branch on the second level of the subtree of the search tree corresponding to the cycle structure $z_1^1 z_3^1 z_5^1$ together with the required computing time in seconds. This section of the tree produced 138 SOLS in 93 seconds.*

The number of SOLS found among the 115 branches on the second level corresponding to the cycle structure $z_1^1 z_4^2$ (which amounts to a total of 19 SOLS) is given in Table 5.5, while the same information for the 207 branches on the second level corresponding to the cycle structure $z_1^1 z_8^1$ is given in Table 5.6.

Branch	3	8	10	11	27	35	36	92	98	105	107	110	113
SOLS	3	1	1	1	1	2	1	1	1	4	1	1	1
Time(s)	2	1	1	1	1	0	1	0	0	0	0	0	0

TABLE 5.5: *The number of SOLS of order 9 eventually found for each branch on the second level of the subtree of the search tree corresponding to the cycle structure $z_1^1 z_4^2$ together with the required computing time in seconds. This section of the tree produced 19 SOLS in 7 seconds.*

Branch	2	8	18	19	21	25	38	47	59	66	83	109
SOLS	2	1	2	2	1	2	1	3	1	1	1	1
Time(s)	1	1	1	0	0	0	0	0	0	0	0	0

TABLE 5.6: *The number of SOLS of order 9 eventually found for each branch on the second level of the subtree of the search tree corresponding to the cycle structure $z_1^1 z_8^1$ together with the required computing time in seconds. This section of the tree produced 18 SOLS in 3 seconds.*

Hence a total of $138+19+18 = 175$ RC-paratopism classes of SOLS of order 9 were counted in 257 seconds, verifying the number derived from the results of Graham and Roberts. It should be noted that the 257 seconds includes the $93 + 3 + 7 = 103$ seconds reported in the tables above, which is only the total computing time required for transversing the tree from level 3 onwards. The remaining computing time of 138 seconds was required in order to generate the universals on the second level.

For $n = 10$ the universal permutations admit four distinct cycle structures, namely $z_1^1 z_3^3$, $z_1^1 z_3^1 z_6^1$, $z_1^1 z_4^1 z_5^1$ and $z_1^1 z_9^1$, and the branches corresponding to these cycle structures resulted in 362, 1 005, 869 and 1 589 branches on the second level, respectively. For each of the four branches on the first level, Table 5.7 gives the number of SOLS found, together with the required computing time, in each of a number of subsets of the branches on the second level. As may be seen from the table, 121 642 RC-paratopism classes of SOLS of order 10 were counted in 6 219 149 seconds (approximately 72 days).

$z_1^1 z_3^3$			$z_1^1 z_3^1 z_6^1$			$z_1^1 z_4^1 z_5^1$			$z_1^1 z_9^1$		
Branches	SOLS	Time	Branches	SOLS	Time	Branches	SOLS	Time	Branches	SOLS	Time
$[1, 18]$	9 698	304 891	$[1, 50]$	27 771	614 642	$[1, 43]$	2 451	198 222	$[1, 79]$	115	95 917
$[19, 36]$	6 607	297 067	$[51, 100]$	18 298	518 376	$[44, 86]$	1 357	169 886	$[80, 158]$	20	60 879
$[37, 54]$	3 922	216 956	$[101, 150]$	12 713	437 095	$[87, 129]$	654	121 036	$[159, 237]$	3	42 924
$[55, 72]$	2 600	189 530	$[151, 200]$	8 382	355 696	$[130, 172]$	411	100 776	$[238, 316]$	2	29 371
$[73, 90]$	1 252	125 293	$[201, 250]$	6 823	343 787	$[173, 215]$	244	85 123	$[317, 395]$	0	17 984
$[91, 108]$	1 073	134 017	$[251, 300]$	4 738	281 390	$[216, 258]$	150	61 984	$[396, 474]$	0	10 435
$[109, 126]$	580	101 888	$[301, 350]$	3 269	223 119	$[259, 301]$	75	45 122	$[475, 553]$	0	5 615
$[127, 144]$	309	81 087	$[351, 400]$	2 426	188 832	$[302, 344]$	52	32 205	$[554, 632]$	0	3 433
$[145, 162]$	188	58 965	$[401, 450]$	1 605	132 719	$[345, 387]$	41	23 423	$[633, 711]$	0	2 005
$[163, 180]$	128	40 693	$[451, 500]$	1 056	90 017	$[388, 430]$	36	23 588	$[712, 790]$	0	1 204
$[181, 198]$	50	31 118	$[501, 550]$	677	65 138	$[431, 473]$	25	13 884	$[791, 869]$	0	702
$[199, 216]$	27	21 052	$[551, 600]$	574	52 668	$[474, 516]$	8	8 913	$[870, 948]$	0	598
$[217, 234]$	9	13 283	$[601, 650]$	405	39 774	$[517, 559]$	6	5 386	$[949, 1\,027]$	0	371
$[235, 252]$	3	10 292	$[651, 700]$	269	26 627	$[560, 602]$	1	2 104	$[1\,028, 1\,106]$	0	159
$[253, 270]$	3	5 652	$[701, 750]$	212	18 102	$[603, 645]$	1	1 005	$[1\,107, 1\,185]$	0	89
$[271, 288]$	2	2 649	$[751, 800]$	152	13 476	$[646, 688]$	1	534	$[1\,186, 1\,264]$	0	58
$[289, 306]$	0	1 071	$[801, 850]$	85	8 007	$[689, 731]$	1	342	$[1\,265, 1\,343]$	0	30
$[307, 324]$	0	653	$[851, 900]$	55	5 049	$[732, 774]$	0	156	$[1\,344, 1\,422]$	0	14
$[325, 342]$	1	237	$[901, 950]$	20	2 225	$[775, 817]$	0	75	$[1\,423, 1\,501]$	0	8
$[343, 360]$	0	43	$[951, 1\,000]$	6	390	$[818, 860]$	0	19	$[1\,502, 1\,580]$	0	3
$[361, 362]$	0	0	$[1\,001, 1\,005]$	0	0	$[861, 869]$	0	1	$[1\,581, 1\,589]$	0	0
	26 452	1 636 437		89 536	3 417 129		5 514	893 784		140	271 799

TABLE 5.7: *The number of SOLS of order 10 found in a given range of branches on the second level of the search tree for each cycle structure type admitted by the first universal in a SOLS of order 10. A total of* 121 642 *SOLS of order 10 were found in* 6 219 149 *seconds.*

The exponential growth of the computing times (less than a second for orders $n \leq 8$, 257 seconds for $n = 9$ and approximately 72 days for $n = 10$) provides strong circumstantial evidence that the case of $n = 11$ is not resolvable within a realistic time frame using the current methodology and computing power. It is not even necessary to traverse the tree at a deeper level than the second level in order to obtain some form of quantifiable measure that this is indeed the case. For $n = 11$ the universal permutations admit five cycle structures, namely $z_1^1 z_3^1 z_4^1$, $z_1^1 z_3^1 z_7^1$, $z_1^1 z_4^1 z_6^1$, $z_1^1 z_5^2$ and $z_1^1 z_9^1$, and for each of these five branches on the first level there are 5 043, 8 131, 7 137, 6 121 and 13 891 branches on the second level, respectively. Furthermore, it was found that the average time to traverse the subtree induced by a node on the second level for $n = 9$ was approximately 0.6 seconds, and for $n = 10$ the same average time was determined as approximately 1 626 seconds. If these average times are linearly extrapolated, a conservative lower bound on the average time required to traverse the subtree induced by a node on the second level of the tree for $n = 11$ is 4 406 460 seconds (approximately 51 days), which aggregates to approximately 5 634 years as a conservative lower bound on the traversal of the entire tree for $n = 11$.

5.2.2 Enumeration of other classes of SOLS

In order to enumerate the isomorphism classes of SOLS (Graham and Roberts only enumerated the isomorphism classes of idempotent SOLS), transpose-isomorphism classes of SOLS, as well as distinct and idempotent SOLS, the methods discussed in §4.4 and §4.5 may be used. In §4.4 a method was discussed for computing the autotransformation groups of Latin squares using `nauty` [96], and this method was used to compute the transpose-automorphism groups of the idempotent SOLS enumerated in the previous section. These groups may then be used to enumerate the various other classes of SOLS using the methods described in §4.5.

By the discussions of §4.4 the RC-paratopism graph of a Latin square $\boldsymbol{L}$ is a graph G with vertex set

$$V(G) = \{\ell_{ij} \mid i,j \in \mathbb{Z}_n\} \cup \{r_i \mid i \in \mathbb{Z}_n\} \cup \{c_i \mid i \in \mathbb{Z}_n\} \cup \{s_i \mid i \in \mathbb{Z}_n\} \cup \{R, C\}$$

and edge set

$$\begin{aligned} E(G) \;=\; & \{r_i\ell_{ij} \mid i,j \in \mathbb{Z}_n\} \cup \{c_j\ell_{ij} \mid i,j \in \mathbb{Z}_n\} \cup \{s_{\boldsymbol{L}(i,j)}\ell_{ij} \mid i,j \in \mathbb{Z}_n\} \\ & \cup\{r_ic_i \mid i \in \mathbb{Z}_n\} \cup \{r_iR \mid i \in \mathbb{Z}_n\} \cup \{c_iC \mid i \in \mathbb{Z}_n\}. \end{aligned}$$

It should be noted that the RC-autoparatopism group of an idempotent SOLS is also its transpose-automorphism group, and hence either the RC-paratopism graph or the transpose-isomorphism graph may be used. Using `nauty`, the automorphism group of this graph was calculated for each class representative of RC-paratopism classes of SOLS generated in the previous section (all of which are idempotent), and the orders of these groups thus found are summarised in Table 5.8. For each order and for each group size, the number of RC-paratopism classes whose members have RC-autoparatopism groups of the specified order are given in this table[2]. The required computing time for determining these groups was less than a second for $n = 4, 5, 7, 8$, while it required one second for $n = 9$ and 1 859 seconds for $n = 10$.

n	4	5	7		8				9									10		
Group order	24	20	6	42	1	7	8	56	1	2	4	6	8	12	16	72	144	1	3	9
Number of classes	1	1	2	2	1	1	1	1	63	36	42	5	18	4	4	1	2	121 456	176	10

TABLE 5.8: *The various orders exhibited by RC-autoparatopism groups of SOLS of various orders, as well as the number of RC-paratopism classes containing SOLS with RC-autoparatopism groups of the given orders.*

Let $\mathcal{P}(n)$ denote a set of idempotent class-representatives, one from each class, of RC-paratopism classes of SOLS of order n, and let $A(\boldsymbol{L})$ denote the RC-autoparatopism group of a SOLS $\boldsymbol{L}$. From Theorem 4.5.1 it follows that there are

$$\sum_{\boldsymbol{L} \in \mathcal{P}(n)} \frac{2(n!)^2}{|A(\boldsymbol{L})|}$$

[2]It follows by Lemma A.2.1 that the RC-autoparatopism groups of the members of an RC-paratopism class have the same size.

distinct SOLS of order n, and from Corollary 4.5.1 it follows that there are

$$\sum_{\boldsymbol{L}\in\mathcal{P}(n)} \frac{2n!}{|A(\boldsymbol{L})|}$$

idempotent SOLS of order n. Furthermore, from Theorem 4.5.2 it follows that there are

$$\sum_{\boldsymbol{L}\in\mathcal{P}(n)} \sum_{\alpha\in A(\boldsymbol{L})} \frac{\psi(\alpha)}{|A(\boldsymbol{L})|}$$

transpose-isomorphism classes of SOLS of order n, where $\psi(\alpha) = \prod_{i=1}^{n} a_i! i^{a_i}$ if the row and column permutation of the RC-paratopism α has the same type as the symbol permutation of α (which is always the case, since an RC-autoparatopism of an idempotent SOLS is a transpose-automorphism). Enumerating the number of isomorphism classes of SOLS of order n may once again be performed by utilising information on which RC-paratopism classes contain SOLS and their transposes and which do not. Let $\mathcal{P}'(n) \subset \mathcal{P}(n)$ be the subset of SOLS class-representatives which are isomorphic to their transposes, and let $\mathcal{P}''(n) = \mathcal{P}(n)\backslash\mathcal{P}'(n)$. These sets may be determined by utilising the following lemma.

Lemma 5.2.1 *An idempotent SOLS $\boldsymbol{L}$ is isomorphic to its transpose if an only if it admits a transpose-automorphism which transposes $\boldsymbol{L}$.*

Proof: Let $\boldsymbol{L}$ be an idempotent SOLS of order n and let $\alpha \in |A(\boldsymbol{L})|$ be an RC-autoparatopism that transposes $\boldsymbol{L}$. Hence α is of the form (p, p, τ) for some $p \in S_n$ (since $\boldsymbol{L}$ is idempotent). Since $(p, p, \tau) \in S_n^2 \times S_2$, it is the product of (e, e, τ) and (p, p, ι), where ι is the identity conjugate operation and e is the identity permutation. Therefore,

$$\boldsymbol{L} = \boldsymbol{L}^{(p,p,\tau)} = \left(\boldsymbol{L}^{(e,e,\tau)}\right)^{(p,p,\iota)} = \left(\boldsymbol{L}^{T}\right)^{(p,p,e)},$$

and $\boldsymbol{L}$ is isomorphic to its transpose via the isomorphism p. Conversely, let $\boldsymbol{L} = \left(\boldsymbol{L}^{T}\right)^{p}$ for some isomorphism $p \in S_n$. Since p is a special case of an RC-paratopism, it may be written as (p, p, ι), and since

$$\boldsymbol{L}^{(p,p,\tau)} = (\boldsymbol{L}^{T})^{(p,p,\iota)} = (\boldsymbol{L}^{T})^{p} = \boldsymbol{L},$$

(p, p, τ) is an RC-autoparatopism that transposes $\boldsymbol{L}$. ∎

The sets $\mathcal{P}'(n)$ and $\mathcal{P}''(n)$ may be determined via the RC-autoparatopism groups of the elements of $\mathcal{P}(n)$ since all these SOLS are idempotent. The following theorem gives the number of isomorphism classes of SOLS of order n.

Theorem 5.2.1 *The number of isomorphism classes of SOLS of order n is*

$$\sum_{\boldsymbol{L}\in\mathcal{P}'(n)} \frac{1}{|A'(\boldsymbol{L})|} \sum_{\boldsymbol{\alpha}\in A'(\boldsymbol{L})} \psi(\alpha) + \sum_{\boldsymbol{L}\in\mathcal{P}''(n)} \frac{2}{|A(\boldsymbol{L})|} \sum_{\boldsymbol{\alpha}\in A(\boldsymbol{L})} \psi(\alpha),$$

where $A'(\boldsymbol{L}) \subset A(\boldsymbol{L})$ is the set of the transpose-automorphisms of $\boldsymbol{L}$ which do not transpose $\boldsymbol{L}$.

Proof: Let $\boldsymbol{L} \in \mathcal{P}'(n)$ and let $\boldsymbol{L}' = \boldsymbol{L}^{(q,r,\tau)}$ for some RC-paratopism (q, r, τ). Since $\boldsymbol{L} \in \mathcal{P}'(n)$, there exists some RC-autoparatopism $(p, p, \tau) \in S_n \times S_2$ such that $\boldsymbol{L}^{(p,p,\tau)} = \boldsymbol{L}$, or equivalently $\boldsymbol{L}^{(p,p,\iota)} = \boldsymbol{L}^T$, which implies that

$$\boldsymbol{L}' = \boldsymbol{L}^{(q,r,\tau)} = \left(\boldsymbol{L}^T\right)^{(q,r,\iota)} = \left(\boldsymbol{L}^{(p,p,\iota)}\right)^{(q,r,\iota)} = \boldsymbol{L}^{(pq,pr,\iota)}.$$

Hence any SOLS in the RC-paratopism class of $\boldsymbol{L}$ may be mapped to $\boldsymbol{L}$ via an RC-paratopism that does not utilise the operation of transposition. Therefore the RC-paratopism class generated by $\boldsymbol{L} \in \mathcal{P}'(n)$ is a (π_{rc}, π_s)-transformation class, and $A'(\boldsymbol{L})$ is the (π_{rc}, π_s)-autotransformation group of $\boldsymbol{L}$. By Theorem 4.5.2 it follows that there are

$$\sum_{\alpha \in A'(\boldsymbol{L})} \frac{\psi(\alpha)}{|A'(\boldsymbol{L})|}$$

(π_{rcs})-transformation classes (*i.e.* isomorphism classes) in the (π_{rc}, π_s)-transformation class generated by $\boldsymbol{L}$ (*i.e.* the RC-paratopism class generated by $\boldsymbol{L}$).

Next suppose $\boldsymbol{L} \in \mathcal{P}''(n)$ and let $\boldsymbol{L}' = \left(\boldsymbol{L}'^T\right)^p$ where p is an isomorphism. If $\boldsymbol{L} = \boldsymbol{L}'^{(q,r,t)}$ for some RC-paratopism $(q, r, t) \in S_n \times S_2$, then

$$\boldsymbol{L} = \boldsymbol{L}'^{(q,r,t)} = \left(\left(\boldsymbol{L}'^T\right)^p\right)^{(q,r,t)} = \left(\left(\boldsymbol{L}^T\right)^{(q^{-1},r^{-1},t^{-1})}\right)^{(pq,pr,t)} = \left(\boldsymbol{L}^T\right)^{(q^{-1}pq,r^{-1}pr,\iota)}.$$

Since both $\boldsymbol{L}$ and $\boldsymbol{L}^T$ are idempotent, they are isomorphic, which contradicts the property of the elements of $\mathcal{P}''(n)$. Hence no SOLS in the RC-paratopism class of $\boldsymbol{L}$ is isomorphic to its transpose, and therefore each transpose-isomorphism class in the RC-paratopism class of $\boldsymbol{L}$ is a union of two disjoint isomorphism classes, one containing the transposes of the SOLS in the other. Consequently there are twice as many isomorphism classes as transpose-isomorphism classes in the RC-paratopism class of $\boldsymbol{L}$. The desired result follows by taking the sum of the number of transpose-isomorphism classes over the sets $\mathcal{P}'(n)$ and $\mathcal{P}''(n)$. ■

In summary, Table 5.9 gives the numbers of the various classes of SOLS of orders $4 \leq n \leq 10$ as enumerated by the methods discussed in this and the preceding section. Class representatives of RC-paratopism classes generated by SOLS of orders $4 \leq n \leq 9$ are available in Appendix B.1, and these SOLS, together with the class representatives of order 10, are also available on the compact disc accompanying this dissertation.

5.3 Enumeration of SOLSSOMs

Once again it is necessary to first establish which transformations may be applied to a SOLSSOM in order for the resulting pair of Latin squares to remain a SOLSSOM. As was noted in the previous section, any (π_{rc}, π_s, τ)-transformation may be applied to SOLS in order to guarantee that the resulting Latin square is also a SOLS. However, if such a transformation is applied to a SOLS $\boldsymbol{L}$ which forms part of a SOLSSOM $(\boldsymbol{L}, \boldsymbol{S})$, then in order for the resulting pair of Latin squares to remain orthogonal, the permutation applied to the rows and columns of $\boldsymbol{L}$ must also be applied to the rows and columns of $\boldsymbol{S}$. Furthermore, it may be noted that if a permutation p is applied to the rows and columns of $\boldsymbol{S}$, then since $\boldsymbol{S}(i, j) = \boldsymbol{S}(j, i)$, $\boldsymbol{S}^p(p(i), p(j)) = \boldsymbol{S}^p(p(j), p(i))$, and hence $\boldsymbol{S}^p$ is also symmetric. In addition to the permutation applied to the rows and columns of $\boldsymbol{S}$, an independent permutation may be applied to the

n	Distinct SOLS	Distinct idempotent SOLS	Isomorphism classes generated by idempotent SOLS	Isomorphism classes generated by all SOLS	Transpose-isomorphism classes generated by all SOLS	RC-paratopism classes generated by all SOLS
4	48	2	1	6	5	1
5	1 440	12	2	22	11	1
6	0	0	0	0	0	0
7	19 353 600	3 840	8	3 972	1 986	4
8	4 180 377 600	103 680	8	104 120	52 060	4
9	25 070 769 561 600	69 088 320	283	69 112 956	34 564 884	175
10	3 200 285 563 453 440 000	881 912 908 800	243 284	881 912 947 656	440 956 473 828	121 642

TABLE 5.9: *Enumeration of various classes of SOLS of orders* $4 \leq n \leq 10$.

symbols of $\boldsymbol{S}$ neither destroying the orthogonality between $\boldsymbol{S}$ and $\boldsymbol{L}$ nor the symmetry of $\boldsymbol{S}$. In other words, any $(\pi_{rc}^{(1,2)}, \pi_s^{(1)}, \pi_s^{(2)}, \tau^{(1)})$-transformation applied to a SOLSSOM will result in a pair of orthogonal Latin squares which also forms a SOLSSOM.

Furthermore, the only conjugate operation which necessarily preserves the symmetry of a Latin square is τ, which for a symmetric Latin square is equivalent to the identity conjugate operation ι. The symmetric Latin square

$$\boldsymbol{L}_{5.2} = \begin{bmatrix} 0&4&3&1&2\\4&1&0&2&3\\3&0&2&4&1\\1&2&4&3&0\\2&3&1&0&4 \end{bmatrix}, \quad \text{for which} \quad \boldsymbol{L}_{5.2}^{-1} = \begin{bmatrix} 0&3&4&2&1\\2&1&3&4&0\\1&4&2&0&3\\4&0&1&3&2\\3&2&0&1&4 \end{bmatrix} \quad \text{and} \quad {}^{-1}\boldsymbol{L}_{5.2} = \begin{bmatrix} 0&2&1&4&3\\3&1&4&0&2\\4&3&2&1&0\\2&4&0&3&1\\1&0&3&2&4 \end{bmatrix},$$

has, for example, non-symmetric conjugates since neither $\boldsymbol{L}_{5.2}^{-1}$ nor ${}^{-1}\boldsymbol{L}_{5.2}$ is symmetric. In fact, $\boldsymbol{L}_{5.2}^{-1} = \left({}^{-1}\boldsymbol{L}_{5.2}\right)^T$, and hence the only conjugate of $\boldsymbol{L}_{5.2}$ that is symmetric is $\boldsymbol{L}_{5.2}^T$.

Since a $(\pi_{rc}^{(1,2)}, \pi_s^{(1)}, \pi_s^{(2)}, \tau^{(1)})$-transformation applied to a SOLSSOM $(\boldsymbol{L}, \boldsymbol{S})$ constitutes two RC-paratopisms applied to $\boldsymbol{L}$ and $\boldsymbol{S}$ respectively, a $(\pi_{rc}^{(1,2)}, \pi_s^{(1)}, \pi_s^{(2)}, \tau^{(1)})$-transformation applied to a SOLSSOM is henceforth also referred to as an *RC-paratopism*, which should cause no confusion since it will be clear from the context whether an RC-paratopism is applied to one or two Latin squares. Similarly, a $(\pi_{rcs}^{(1,2)}, \tau^{(1)})$-transformation applied to a SOLSSOM is henceforth referred to as a *transpose-isomorphism*. In the following subsections methods are presented for enumerating these two classes of SOLSSOMs, as well as methods for enumerating distinct and standard SOLSSOMs.

5.3.1 Enumeration of RC-paratopism classes of SOLSSOMs

It is useful to note that any SOLSSOM may be mapped to a standard SOLSSOM by two permutations on the symbol sets of the SOLS and the symmetric Latin square, respectively. Hence any RC-paratopism class generated by SOLSSOMs contains a standard SOLSSOM, and so only standard SOLSSOMs are considered in this section.

RC-paratopism classes of SOLSSOMs may be enumerated by utilising existing repositories of SOLS and symmetric Latin squares. Two distinct enumeration methods may be employed, namely generating symmetric Latin square mates for a maximal set of SOLS, or generating SOLS mates for a maximal set of symmetric Latin squares. In what follows, let $\mathcal{P}(n)$ again denote a set of SOLS class representatives, one from each RC-paratopism class generated by SOLS, and let $\mathcal{Q}(n)$ denote a set of symmetric Latin square class representatives, one from each RC-paratopism class generated by symmetric Latin squares.

Let $\boldsymbol{S}$ be a symmetric Latin square of order n and let $A(\boldsymbol{S})$ denote the RC-autoparatopism group of $\boldsymbol{S}$. Furthermore, let $(\boldsymbol{L}, \boldsymbol{S})$ and $(\boldsymbol{L}', \boldsymbol{S})$ be standard SOLSSOMs in the same RC-paratopism class. Then, for any RC-paratopism $(p, q, r, t) \in S_n^3 \times S_2$ which maps $(\boldsymbol{L}, \boldsymbol{S})$ to $(\boldsymbol{L}', \boldsymbol{S})$, it must hold that $(p, r) \in A(\boldsymbol{S})$. Furthermore, since $\boldsymbol{L}$ and $\boldsymbol{L}'$ are idempotent, $p = q$, and in order to test whether two standard SOLSSOMs $(\boldsymbol{L}, \boldsymbol{S})$ and $(\boldsymbol{L}', \boldsymbol{S})$ which share the same symmetric mate are RC-paratopic, it is sufficient to test for each $(p, r) \in A(\boldsymbol{S})$ whether p (taken as an isomorphism) maps $\boldsymbol{L}$ to $\boldsymbol{L}'$. If no element of $A(\boldsymbol{S})$ maps $\boldsymbol{L}$ to $\boldsymbol{L}'$, then $(\boldsymbol{L}, \boldsymbol{S})$ and $(\boldsymbol{L}', \boldsymbol{S})$ are not RC-paratopic. Hence for each $(p, r) \in A(\boldsymbol{S})$, the isomorphism p may also be used to test whether $(\boldsymbol{L}, \boldsymbol{S})$ is the standard SOLSSOM containing the smallest SOLS in the RC-paratopism class generated by all SOLSSOMs containing $\boldsymbol{S}$. This test may then replace the test for RC-paratopism class leadership (of RC-paratopism classes generated by SOLS) in the orderly generation backtracking tree-search approach for enumerating RC-paratopism classes generated by SOLS discussed in §5.2.1. Together with the additional restriction that a universal may only be inserted in a partially completed SOLS if it forms a transversal in $\boldsymbol{S}$, this method then generates one SOLSSOM from each RC-paratopism class of SOLSSOMs containing $\boldsymbol{S}$. If this method is repeated for each element of $\mathcal{Q}(n)$, one SOLSSOM from each RC-paratopism class will therefore be generated.

Let $\boldsymbol{L}$ be an idempotent SOLS of order n and let $A(\boldsymbol{L})$ denote the RC-autoparatopism group of $\boldsymbol{L}$. Consider testing whether two standard SOLSSOMs $(\boldsymbol{L}, \boldsymbol{S})$ and $(\boldsymbol{L}, \boldsymbol{S}')$ are RC-paratopic. Once again an RC-paratopism from $(\boldsymbol{L}, \boldsymbol{S})$ to $(\boldsymbol{L}, \boldsymbol{S}')$ will be of the form $(p, p, r, t) \in S_n^3 \times S_2$, where $(p, p, t) \in A(\boldsymbol{L})$. If (p, p, r, t) is applied to $(\boldsymbol{L}, \boldsymbol{S})$, then $\boldsymbol{S}^{(p,r)}(0) = r \circ \boldsymbol{S}(p^{-1}(0)) \circ p^{-1}$ (see §2.3). However, $\boldsymbol{S}^{(p,r)}$ must be reduced in order for $(\boldsymbol{L}, \boldsymbol{S})$ and $(\boldsymbol{L}, \boldsymbol{S}')$ to be RC-paratopic, and hence $\boldsymbol{S}^{(p,r)}(0) = r \circ \boldsymbol{S}(p^{-1}(0)) \circ p^{-1} = e$ (where e is the identity permutation), and it follows that $r = p \circ \boldsymbol{S}(p^{-1}(0))^{-1}$. Hence in order to test whether two standard SOLSSOMs $(\boldsymbol{L}, \boldsymbol{S})$ and $(\boldsymbol{L}, \boldsymbol{S}')$ which share the same SOLS are RC-paratopic, it is sufficient to test, for each $(p, p, t) \in A(\boldsymbol{L})$, whether the RC-paratopism $(p, p \circ \boldsymbol{S}(p^{-1}(0))^{-1})$ maps $\boldsymbol{S}$ to $\boldsymbol{S}'$. Once again $(p, p \circ \boldsymbol{S}(p^{-1}(0))^{-1})$ may also be used to test whether $(\boldsymbol{L}, \boldsymbol{S})$ is the standard SOLSSOM containing the smallest symmetric Latin square in the RC-paratopism class generated by all SOLSSOMs containing $\boldsymbol{L}$.

An orderly backtracking tree search may also be used in this case to generate RC-paratopism class representatives of SOLSSOMs containing a fixed SOLS $\boldsymbol{L}$. Since symmetric Latin squares are generated in this case, only universal permutations consisting of one and two cycles are considered, and a universal is inserted into a partially completed symmetric Latin square only if it forms a transversal in $\boldsymbol{L}$. The method described above may then be used to test whether a partially completed symmetric Latin square may be mapped to a smaller partially completed Latin square which is also orthogonal to $\boldsymbol{L}$. If this method is repeated for each element of $\mathcal{P}(n)$, one SOLSSOM from each RC-paratopism class will be generated.

The two methods discussed above are completely independent of one another, and therefore provides a means of validation of the results. The set $\mathcal{P}(n)$ is available from the output of the backtracking tree-search discussed in §5.2.1, while the set $\mathcal{Q}(n)$ is only partially available in the literature. The only enumeration work in the literature which is related to symmetric Latin squares is the enumeration of non-isomorphic 1-factorisations of the complete graph K_{2n}, where two 1-factorisations $\{F_1, F_2, \ldots, F_{2n-1}\}$ and $\{F'_1, F'_2, \ldots, F'_{2n-1}\}$ are *isomorphic* if there exists a permutation p such that $\{p(F_1), p(F_2), \ldots, p(F_{2n-1})\} = \{F'_1, F'_2, \ldots, F'_{2n-1}\}$, where $p(F_i)$ contains $\{p(a), p(b)\}$ if F_i contains $\{a, b\}$. These numbers are given in Table 5.10, and details on the methods used to obtain these numbers are provided by Dinitz *et al.* [46].

$2n$	2	4	6	8	10	12
Number of classes	1	1	1	6	396	526 915 620

TABLE 5.10: *The number of isomorphism classes of 1-factorisations of K_{2n}.*

In §3.1 it was shown that a 1-factorisation of K_{2n} is equivalent to a symmetric unipotent Latin square of order $2n$. The following theorem shows that the number of isomorphism classes of 1-factorisations of K_{2n} is equal to the number of RC-paratopism classes of symmetric unipotent Latin squares of order $2n$.

Theorem 5.3.1 *Two symmetric unipotent Latin squares are RC-paratopic if and only if their corresponding 1-factorisations are isomorphic.*

Proof: Let $\{F_1, F_2, \ldots, F_{2n-1}\}$ and $\{F'_1, F'_2, \ldots, F'_{2n-1}\}$ be two 1-factorisations of K_{2n} and let $\boldsymbol{L}$ and $\boldsymbol{L}'$ be symmetric unipotent Latin squares such that $\boldsymbol{L}(i,j) = \boldsymbol{L}(j,i) = k$ if $\{i,j\} \in F_k$ and $\boldsymbol{L}'(i,j) = \boldsymbol{L}'(j,i) = k$ if $\{i,j\} \in F'_k$, for all $1 \leq k \leq 2n-1$ and all $i, j \in \mathbb{Z}_n$. Assume that there exists some permutation p such that $\{p(F_1), p(F_2), \ldots, p(F_{2n-1})\} = \{F'_1, F'_2, \ldots, F'_{2n-1}\}$. Hence there also exists some permutation q of order $2n$ such that $p(F_i) = F'_{q(i)}$ for all $1 \leq i \leq 2n-1$ and $q(0) = 0$. Therefore, if $\{i,j\} \in F_k$, then $\{p(i), p(j)\} \in F'_{q(k)}$, which is equivalent to stating that if $\boldsymbol{L}(i,j) = k$, then $\boldsymbol{L}'(p(i), p(j)) = q(k)$. Consequently the RC-paratopism $(p, q, t) \in S_{2n}^2 \times S_2$ maps $\boldsymbol{L}$ to $\boldsymbol{L}'$ (where t may either be ι or τ since $\boldsymbol{L}$ and $\boldsymbol{L}'$ are symmetric).

Conversely, suppose that some RC-paratopism $(p, q, t) \in S_{2n}^2 \times S_2$ maps $\boldsymbol{L}$ to $\boldsymbol{L}'$. If $\boldsymbol{L}(i,j) = \boldsymbol{L}(j,i) = k$, then $\boldsymbol{L}'(p(i), p(j)) = \boldsymbol{L}'(p(j), p(i)) = q(k)$, which is equivalent to stating that if $\{i,j\} \in F_k$, then $\{p(i), p(j)\} \in F'_{q(k)}$. Since q is a bijection, $\{p(F_1), p(F_2), \ldots, p(F_{2n-1})\} = \{F'_1, F'_2, \ldots, F'_{2n-1}\}$, and the two 1-factorisations are therefore isomorphic. ■

The unipotent members of the set $\mathcal{Q}(2n)$ for $n = 2, 3, 4$ are therefore available (see, for instance, Andersen [5]), and these symmetric Latin squares may be used to validate the enumeration results for unipotent SOLSSOMs of even order. It seems, however, that no attempts have been made to enumerate symmetric Latin squares of odd order, and so the orderly generation method was used here in order to achieve this. Since the universal permutations of a symmetric Latin square only contains one- and two-cycles, it follows that for odd order each universal permutation must have at least one fixed point (it cannot only have two-cycles). Each universal in a symmetric Latin square therefore necessarily contains a diagonal entry, and hence each universal contains exactly one diagonal entry. This implies that all symmetric Latin squares of odd order are diagonal (as are SOLS), and therefore that the orderly generation method used to enumerate RC-paratopism classes generated by SOLS in §5.2.1 may also be used to enumerate RC-paratopism classes generated by symmetric Latin squares of odd order. The test for orthogonality may simply be removed and a restriction introduced which ensures that each universal has only two-cycles and exactly one fixed point. The number of RC-paratopism classes of symmetric Latin squares of odd order are given in Table 5.11, and the members of the set $\mathcal{Q}(2n+1)$ for $n = 2$, 3 and 4 are therefore available. The required computing time for the enumeration of these symmetric Latin squares was less than a second for orders 5 and 7, while 58 seconds of computing time was required for order 9.

n	5	7	9
Number of classes	1	7	3 460

TABLE 5.11: *The number of RC-paratopism classes of symmetric Latin squares of odd order.*

The search tree for symmetric Latin squares of order 11 has five branches on the second level, and these branches gave rise to 15, 26, 49, 56 and 80 branches on the third level, respectively. Furthermore, on the fourth level these five branches gave rise to a total of 2 341, 5 028, 3 569, 2 667 and 2 084 branches, respectively, while the very first branch on the fourth level gives rise to 108 branches on the fifth level. It was found that the first of these 108 branches results in 17 938 symmetric Latin squares in 1 492 seconds. The fact that these results were found in only one branch out of 108, which in turn emanates from only one branch out of 15 689, is an indication that it would not be possible to enumerate the RC-paratopism classes of symmetric Latin squares of order 11 within a realistic time frame using the current methodology and computing power.

For $n = 4$ there is only one RC-paratopism class of symmetric Latin squares (all of which are unipotent), and using the methods discussed above only one SOLS mate was found for this square. Also, for the only SOLS of order 4 only one symmetric mate was found, and hence exactly one RC-paratopism class is generated by SOLSSOMs of order 4.

For $n = 5$ again only one SOLS mate and one symmetric mate were found for the only symmetric Latin square and the only SOLS of order 5, respectively. Hence only one RC-paratopism class is generated by SOLSSOMs of order 5. Figures 5.2 and 5.3 show the search trees for finding SOLS mates for the symmetric Latin square

$$\boldsymbol{L}_{5.3} = \begin{bmatrix} 0 & 4 & 3 & 1 & 2 \\ 4 & 1 & 0 & 2 & 3 \\ 3 & 0 & 2 & 4 & 1 \\ 1 & 2 & 4 & 3 & 0 \\ 2 & 3 & 1 & 0 & 4 \end{bmatrix}$$

of order 5 and symmetric mates for the SOLS

$$\boldsymbol{L}_{5.4} = \begin{bmatrix} 0 & 2 & 1 & 4 & 3 \\ 3 & 1 & 4 & 0 & 2 \\ 4 & 3 & 2 & 1 & 0 \\ 3 & 4 & 0 & 3 & 1 \\ 1 & 0 & 3 & 2 & 4 \end{bmatrix}$$

of order 5, respectively. In Figure 5.2 the universals inserted preserve the self-orthogonality of the partially completed SOLS, but where a partially completed SOLS does not give rise to any further branches the last universal inserted destroys the orthogonality between the partially completed SOLS and the symmetric Latin square. Similarly, in Figure 5.3 the universals inserted preserve the symmetry of the partially completed symmetric Latin square, but where one does not give rise to any further branches the last universal inserted destroys the orthogonality between the partially completed symmetric Latin square and the SOLS. Two completed SOLS are shown in Figure 5.2; they are, however, transposes of one another, and thus RC-paratopic.

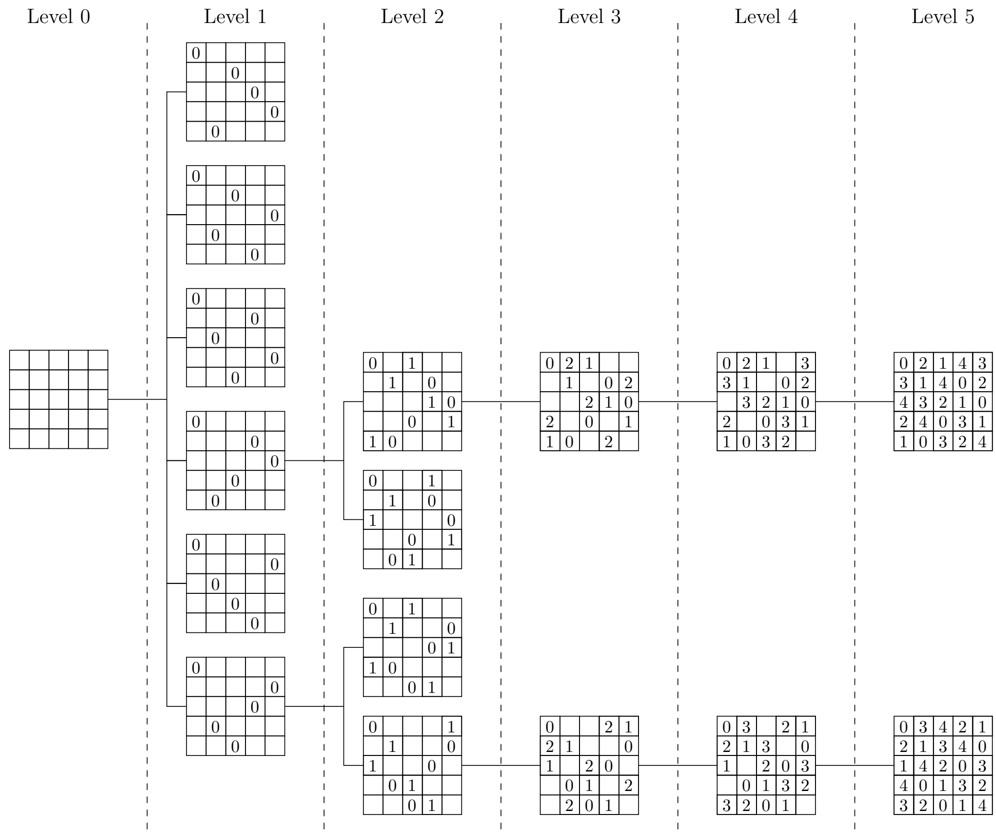

FIGURE 5.2: *The backtracking search tree for SOLSSOMs of order 5, where the search branches on the inclusion of universals in a partially completed SOLS of order 5. Where a partially completed SOLS does not give rise to any further branches, the last universal inserted destroys the orthogonality between the partially completed SOLS and the symmetric Latin square* $\boldsymbol{L}_{5.4}$.

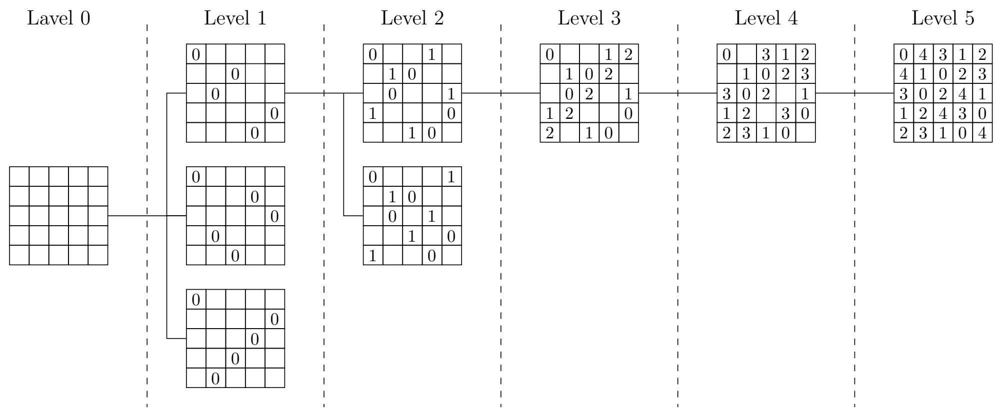

FIGURE 5.3: *The backtracking search tree for SOLSSOMs of order 5, where the search branches on the inclusion of universals in a partially completed symmetric Latin square of order 5. Where a partially completed symmetric Latin square does not give rise to any further branches, the last universal inserted destroys the orthogonality between the partially completed symmetric Latin square and the SOLS* $\boldsymbol{L}_{5.3}$.

For $n = 7$ SOLS mates were found for only one of the seven symmetric Latin squares, namely the seventh[3] symmetric Latin square, and two SOLS mates were found for this Latin square.

[3]The SOLS and symmetric Latin squares that are used here to enumerate SOLSSOMs are available in a

Furthermore, there are four SOLS of order 7, and one symmetric mate each was found for the first and fourth of these SOLS. Hence two RC-paratopism classes are generated by SOLSSOMs of order 7.

For $n = 8$ two SOLS mates were found (requiring one second of computing time) for each of the first, second and third symmetric unipotent Latin squares, and one SOLS mate was found for the fifth symmetric unipotent Latin square, resulting in seven RC-paratopism class generated by unipotent SOLSSOMs of order 8. For the second SOLS of order 8 fourteen symmetric mates were found, two of which are unipotent, six are of type[4] 2^4, four are of type $2^2 4^1$ and two are of type 4^2. For the fourth SOLS of order 8 eighteen symmetric mates were found, five of which are unipotent while thirteen are of type 4^2. This therefore results in seven RC-paratopism classes generated by unipotent SOLSSOMs of order 8, and 32 RC-paratopism classes generated by SOLSSOMs of order 8 in general (including unipotent SOLSSOMS).

For $n = 9$ the number of SOLS mates found for each of the 3 460 symmetric Latin squares of order 9 which have SOLS orthogonal to them are given in Table 5.12, and 76 seconds of computing time was required to generate these SOLS. Interestingly only eight of the 3 460 symmetric Latin squares of order 9 have SOLS that are orthogonal to them.

Symmetric Latin square	116	341	364	426	428	484	1 744	2 765
Number of classes	1	11	2	1	5	3	1	2

TABLE 5.12: *For each symmetric Latin square of order 9 which admits orthogonal SOLS mates, the number of RC-paratopism classes generated by SOLSSOMs containing this symmetric Latin square is given.*

Among the 175 SOLS of order 9, only one symmetric mate was found for the i-th SOLS, where $i \in \{38, 68, 73, 86, 88, 92, 101, 102, 133, 135, 137, 139, 140, 141, 144, 155, 158, 163, 165, 169, 171, 173\}$, while two symmetric mates where found each for the 172-nd and 175-th SOLS, in total requiring two seconds of computing time. In both the above cases, 26 RC-paratopism classes are therefore generated by SOLSSOMs of order 9.

Class representatives of RC-paratopims classes of SOLSSOMs of orders $4 \leq n \leq 9$ are available in Appendix B.2, as well as on the compact disc accompanying this dissertation.

5.3.2 The non-existence of SOLSSOMs of order 10

Since it was not known at the time that work towards this dissertation commenced whether a SOLSSOM of order 10 exists, a filtering method was employed that determines which of the 121 642 SOLS of order 10 satisfies two necessary (but not sufficient) conditions for having symmetric orthogonal mates (rather than attempting to enumerate something that possibly does not exist). This method utilises a simple backtracking procedure which, given a set of k Latin squares, finds all possible n-sets of entries which form transversals in each of these k Latin squares, a method which may, in general, be extremely useful in looking for sets of orthogonal Latin squares. This procedure is given in pseudocode form in Algorithm 5.1.

number of text files on the compact disc accompanying this dissertation. Latin squares are referred to in the text above in the order in which they appear in these text files.

[4] A Latin square is of *diagonal type* $1^{d_1} 2^{d_2} \dots n^{d_n}$ if it contains d_i symbols that each appear i times on the diagonal of the Latin square, where the term i^{d_i} is omitted if $d_i = 0$. A unipotent Latin square of order n, for example, is of type n^1, while an idempotent Latin square of order n is of type 1^n.

Algorithm 5.1 GetTransversals

Input: A set of Latin squares $\{\boldsymbol{L}_1, \boldsymbol{L}_2, \ldots, \boldsymbol{L}_k\}$.

Output: A set $\mathcal{V}$ such that if V is a transversal of $\boldsymbol{L}_i$ for all $1 \leq i \leq k$, then $V \in \mathcal{V}$.

$V \leftarrow \varnothing$
$r \leftarrow 0$
$c \leftarrow 0$
while $r \geq 0$ **do**
    if $r = n$ or $c = n$ **then**
        if $r = n$ **then** Print V
        $r \leftarrow r - 1$
        $c \leftarrow V(r) + 1$
    else
        if $(r, c) \notin V$ and $\boldsymbol{L}_i(a, b) \neq \boldsymbol{L}_i(r, c)$ for all $1 \leq i \leq k$ and all $(a, b) \in V$ **then**
            $V \leftarrow V \cup \{(r, c)\}$
            $r \leftarrow r + 1$
            $c \leftarrow 0$
        else
            $c \leftarrow c + 1$
        end if
    end if
end while

In this algorithm r and c denote the current row and columns respectively (both of which are zero initially), and at any stage of the procedure it is attempted to insert the entry (r, c) into the current partial transversal. This insertion is only performed if the resulting set of entries is still a transversal in each of the given Latin squares. If not, then the next column is considered, and if the last column is reached the procedure backtracks to the previous row. If a Latin square may be constructed using any n of the transversals generated by this procedure, then this Latin square is orthogonal to each Latin square in the given set of Latin squares.

For each of the 121 642 RC-paratopism class representatives of SOLS of order 10, the SOLS and its transpose are given as input to Algorithm 5.1, and a total of 143 seconds of computing time was required in order to calculate all possible transversals for all of these SOLS and their transposes. One necessary condition for a SOLS and its transpose to have a common orthogonal mate is certainly that at least 10 transversals is found by Algorithm 5.1, and 119 288 of the 121 642 SOLS did not even satisfy this condition. Another necessary condition is that each pair $(i, j) \in \mathbb{Z}^2$ must be part of at least one transversal (*i.e.* each entry of the SOLS must lie on at least one transversal), otherwise it is impossible to construct a complete Latin square using these transversals. Of the remaining 2 354 SOLS, only four SOLS satisfied this condition (the 34 641-st, 120 857-th, 121 427-th and the 121 642-nd SOLS); these four SOLS are

$$\begin{bmatrix} 0&5&8&1&9&4&3&6&7&2\\ 9&1&6&0&8&2&5&4&3&7\\ 1&0&2&7&5&3&8&9&6&4\\ 4&9&0&3&7&6&1&8&2&5\\ 7&3&1&6&4&8&2&5&9&0\\ 3&8&7&9&0&5&4&2&1&6\\ 5&7&9&2&3&0&6&1&4&8\\ 8&2&3&4&6&9&0&7&5&1\\ 2&6&4&5&1&7&9&0&8&3\\ 6&4&5&8&2&1&7&3&0&9 \end{bmatrix}, \begin{bmatrix} 0&8&6&5&7&9&2&1&4&3\\ 7&1&9&8&0&3&5&4&6&2\\ 1&0&2&7&9&4&3&6&5&8\\ 4&5&0&3&8&6&1&9&2&7\\ 2&6&3&0&4&7&8&5&9&1\\ 8&7&1&9&6&5&4&2&3&0\\ 5&9&8&2&1&0&6&3&7&4\\ 9&2&5&4&3&8&0&7&1&6\\ 3&4&7&6&2&1&9&0&8&5\\ 6&3&4&1&5&2&7&8&0&9 \end{bmatrix}, \begin{bmatrix} 0&5&6&9&3&2&8&4&1&7\\ 9&1&7&4&0&8&2&3&5&6\\ 8&0&2&5&9&7&1&6&3&4\\ 1&7&0&3&8&4&9&2&6&5\\ 6&9&8&0&4&1&7&5&2&3\\ 4&2&1&8&6&5&3&9&7&0\\ 7&3&4&2&5&0&6&1&9&8\\ 5&8&9&6&2&3&0&7&4&1\\ 3&6&5&7&1&9&4&0&8&2\\ 2&4&3&1&7&6&5&8&0&9 \end{bmatrix} \text{ and } \begin{bmatrix} 0&9&6&1&8&4&2&3&5&7\\ 3&1&8&9&5&7&4&6&2&0\\ 1&0&2&7&6&8&9&5&3&4\\ 4&7&0&3&2&9&1&8&6&5\\ 7&6&3&0&4&1&5&2&9&8\\ 8&2&9&6&0&5&3&4&7&1\\ 5&3&4&8&7&0&6&9&1&2\\ 2&8&1&5&9&6&0&7&4&3\\ 9&4&5&2&1&3&7&0&8&6\\ 6&5&7&4&3&2&8&1&0&9 \end{bmatrix}.$$

It is easy to verify by hand that the transversals found for these four SOLS cannot form a Latin square. For the first SOLS, for example, 19 transversals were found, and although each entry of the SOLS lies on at least one of these transversals, the entry $(0,1)$ lies on only one transversal, namely

$$\{(0,1),(1,0),(2,2),(3,4),(4,3),(5,6),(6,5),(7,9),(8,8),(9,7)\}.$$

Furthermore, the entry $(1,2)$ also lies on only one transversal, namely

$$\{(0,3),(1,2),(2,1),(3,0),(4,6),(5,5),(6,4),(7,7),(8,8),(9,9)\}.$$

However, both these transversals contain the entry $(8,8)$, and therefore they cannot both be part of the same Latin square. Hence the first SOLS and its transpose have no common orthogonal mates. In a similar manner it may be shown that the remaining three SOLS and their transposes also do not have common orthogonal mates.

Hence not only do the findings discussed above show that a SOLS of order 10 cannot have a symmetric Latin square orthogonal to it, they also establish a more general result related to the hitherto unsolved problem of whether a 3-MOLS of order 10 exists, as summarised in the following theorem.

Theorem 5.3.2 *If a 3-MOLS of order 10 exists, it does not contain a SOLS and its transpose.*

The following corollary follows naturally from the above theorem.

Corollary 5.3.1 *A SOLSSOM of order 10 does not exist.*

Theorem 5.40 in Colbourn *et al.* [38] may therefore be updated to the following result.

Theorem 5.3.3 *A SOLSSOM exists for any $n \notin \{2,3,6,10\}$ and possibly $n \neq 14$.*

5.3.3 Enumeration of other classes of SOLSSOMs

In order to enumerate distinct SOLSSOMs, standard SOLSSOMs and transpose-isomorphism classes of SOLSSOMs, the methods of §4.5 may once again be employed. In order to determine the RC-autoparatopism group of a SOLSSOM $(\boldsymbol{L},\boldsymbol{S})$, the RC-paratopism graphs of $\boldsymbol{L}$ and $\boldsymbol{S}$ may be used. Let the edges and colour classes of these graphs be defined as in §5.2.2, where the RC-paratopism graph of $\boldsymbol{L}$ has vertices ℓ_{ij}, r_i, c_i, s_i, R and C for all $i,j \in \mathbb{Z}_n$, while the RC-paratopism graph of $\boldsymbol{S}$ has vertices ℓ'_{ij}, r'_i, c'_i, s'_i, R' and C' for all $i,j \in \mathbb{Z}_n$. If the edges $\{r_i, r'_i\}$ and $\{c_i, c'_i\}$ are used to connect the two graphs, then this will ensure that the elements of the RC-autoparatopism group of $(\boldsymbol{L},\boldsymbol{S})$ permutes the rows and columns of both Latin squares using the same permutation. It should also be ensured that no vertex from the one graph is in the same colour class as any vertex from the other graph. The automorphism groups of these graphs may then be calculated, as before, using `nauty`. The various group orders determined for SOLSSOMs of orders $4 \leq n \leq 9$ are given in Table 5.13.

Let $\mathcal{R}(n)$ denote a set of idempotent class-representatives, one from each class, of RC-paratopism classes of SOLSSOMs of order n, and let $A((\boldsymbol{L},\boldsymbol{S}))$ denote the RC-autoparatopism group of a SOLSSOM $(\boldsymbol{L},\boldsymbol{S})$. From Theorem 4.5.1 it follows that there are

$$\sum_{(\boldsymbol{L},\boldsymbol{S})\in\mathcal{R}(n)} \frac{2(n!)^3}{|A((\boldsymbol{L},\boldsymbol{S}))|}$$

n	4	5	7	8			9							
Group order	24	20	42	4	8	56	2	4	6	8	12	16	72	144
Number of classes	1	1	2	6	25	1	4	6	3	2	4	4	1	2

TABLE 5.13: *The various orders that RC-autoparatopism groups of SOLSSOMs may exhibit for various orders, as well as the number of RC-paratopism classes containing SOLSSOMs with RC-autoparatopism groups of the given orders.*

distinct SOLSSOMs of order n, and the following lemma (which is similar to Corollary 4.5.1) may be used to enumerate standard SOLSSOMs.

Lemma 5.3.1 *The number of distinct SOLSSOMs is $(n!)^2$ times the number of standard SOLSSOMs.*

Proof: It is easy to see that any $(\pi_s^{(1)}, \pi_s^{(2)})$-transformation class generated by SOLSSOMs contains exactly one standard SOLSSOM, and that the $(\pi_s^{(1)}, \pi_s^{(2)})$-autotransformation-group of a SOLSSOM has order one. Hence the number of $(\pi_s^{(1)}, \pi_s^{(2)})$-transformation classes generated by SOLSSOMs of order n is equal to the number of standard SOLSSOMs of order n, and since the $(\pi_s^{(1)}, \pi_s^{(2)})$-transformation group has order $(n!)^2$, the desired result follows from Theorem 4.5.1. ■

It therefore follows that there are

$$\sum_{(\boldsymbol{L},\boldsymbol{S})\in\mathcal{R}(n)} \frac{2n!}{|A((\boldsymbol{L},\boldsymbol{S}))|}$$

standard SOLSSOMs of order n. Furthermore, it follows by Theorem 4.5.2 that there are

$$\sum_{(\boldsymbol{L},\boldsymbol{S})\in\mathcal{R}(n)} \sum_{\alpha\in A((\boldsymbol{L},\boldsymbol{S}))} \frac{\psi(\alpha)^2}{|A((\boldsymbol{L},\boldsymbol{S}))|}$$

transpose-isomorphism classes of SOLS of order n, where $\psi(\alpha) = \prod_{i=1}^{n} a_i! i^{a_i}$ if the row and column permutation of the RC-paratopism α has the same type as both the symbol permutations of α. The final enumeration results for SOLSSOMs of orders $4 \leq n \leq 10$ are given in Table 5.14.

5.4 Enumeration of MOLS

As mentioned in §4.2, existing work in the literature on the enumeration of k-MOLS of order n include the enumeration of 8-MOLS of order 9 by Owens and Preece [113]. They determined that there are 19 isotopy classes[5] of 8-MOLS of order 9 utilising the fact that an $(n-1)$-MOLS of order n exists if and only if a *projective plane* of order n exists [41, p. 160], while projective planes have already been enumerated for $n = 9$ by Lam *et al.* [86]. Colbourn *et al.* [38, pp. 172–175] provide 19 isotopy class representatives from the isotopy classes of 8-MOLS of order

[5]An *isotopy* class of k-MOLS of order n is a $(\pi_r^{(0,1,\ldots,k-1)}, \pi_c^{(0,1,\ldots,k-1)}, \pi_s^{(0)}, \pi_s^{(1)}, \ldots, \pi_s^{(k-1)})$-transformation class.

n	Distinct	Standard	Transpose-isomorphism classes	(Row,column)-paratopism classes
4	1 152	2	31	1
5	172 800	12	749	1
6	0	0	0	0
7	12 192 768 000	480	1 210 622	2
8	608 662 978 560 000	374 400	7 547 904 042	32
9	464 573 723 443 200 000	3 528 000	640 121 719 688	26
10	0	0	0	0

TABLE 5.14: *Enumeration of various classes of SOLSSOMs of order* $4 \leq n \leq 10$.

9, and by performing paratopism testing utilising **nauty**[6] [96] it follows that there are 7 main classes of 8-MOLS of order 9.

To the best knowledge of the author no other published work exists on the enumeration of k-MOLS of order n. Brendan McKay provides main class representatives of pairs of orthogonal Latin squares of orders 3, 4, 5, 7 and 8 on his website [98], without reference, however, to how these squares were obtained. According to this repository there is one main class of 2-MOLS of orders 3, 4 and 5, while there are 7 main classes of 2-MOLS of order 7 and 2 165 main classes of 2-MOLS of order 8.

5.4.1 Enumeration of main classes of MOLS

The relative cycle structures of the universals in a 2-MOLS of order 3 permit only one cycle structure, namely $z_1^1 z_2^1$ (since the relative cycle structure of two universals in a k-MOLS of order n has exactly one fixed point), and the first universal permutation of the second Latin square in a main class leader of 2-MOLS of order 3 therefore is the cycle structure representative $\binom{0\,1\,2}{0\,2\,1}$ (according the the algorithm described in §4.3.2). Furthermore, the first universal of the first Latin square is the identity permutation and both Latin squares are reduced. It is easy to verify that the resulting partial 2-MOLS of order 3

$$\left(\begin{bmatrix} 0 & 1 & 2 \\ & 0 & \\ & & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ & & 0 \\ & 0 & \end{bmatrix}\right)$$

has only one feasible completion to a 2-MOLS of order 3, namely

$$\left(\begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}\right).$$

Hence there is only one main class of 2-MOLS of order 3.

For $n = 4$ the relative cycle structures of the universals also permit only one cycle structure, namely $z_1^1 z_3^1$. Hence the first universal permutation of the second Latin square is $\binom{0\,1\,2\,3}{0\,2\,3\,1}$, and

[6] Another tool provided by the computer program **nauty** allows the user to test whether or not two graphs are isomorphic. By Theorem 4.4.1 this tool may be used to test whether two Latin squares are in the same σ-transformation class for any transformation type σ.

it is also easy to verify that for both $k = 2$ and $k = 3$ there is only one completion to a reduced k-MOLS of order 4 if the first universal permutation of the first Latin square is the identity permutation. Hence there is only one main class of k-MOLS of order 4 for $k = 2$ and $k = 3$, and a main class representative for $k = 3$ is

$$\left(\begin{bmatrix} 0&1&2&3\\ 1&0&3&2\\ 2&3&0&1\\ 3&2&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&2&3\\ 2&3&0&1\\ 3&2&1&0\\ 1&0&3&2 \end{bmatrix}, \begin{bmatrix} 0&1&2&3\\ 3&2&1&0\\ 1&0&3&2\\ 2&3&0&1 \end{bmatrix}\right),$$

whereas the first two Latin squares of this 3-MOLS form a main class representative for $k = 2$.

For $n = 5$ two relative cycle structures are admitted by universals in a k-MOLS of order 5, namely $z_1^1 z_2^2$ and $z_1^1 z_4^1$. For $k = 2$ the branch in the search tree (as discussed in §4.3.2) corresponding to the cycle structure $z_1^1 z_2^2$ for the first universal permutation of the second Latin square gives rise to two branches on the second level, two branches on the third level, and then one branch each on the fourth and fifth levels. This section of the search tree therefore produces one 2-MOLS of order 5. The branch corresponding to the cycle structure $z_1^1 z_4^1$, on the other hand, also has two branches on the second level, but has only one branch on the third and fourth levels, and no branches on the fifth level. This section of the tree therefore produces no MOLS, and consequently there is only one main class of 2-MOLS of order 5.

The backtracking search tree for 2-MOLS of order 5 is shown in Figure 5.4. On each level of the tree two partially completed Latin squares (referred to as Members 1 and 2, respectively) are shown, and in cases where a universal was only found for Member 1 only this partially completed Latin square is shown. Where branches are pruned (*i.e.* where there are no feasible universals that may be included in any of the members), it is either indicated [a] that there are no possible universals that would have preserved the orthogonality of the two members, or [b] that the current partially completed 2-MOLS cannot be completed to a class leader.

Two completed pairs of orthogonal Latin squares of order 5 are shown in Figure 5.4, but it can be shown that one of them is not a class leader, namely the pair

$$\mathcal{M}_{5.1} = \left(\begin{bmatrix} 0&1&2&3&4\\ 3&0&1&4&2\\ 4&3&0&2&1\\ 1&2&4&0&3\\ 2&4&3&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4\\ 4&3&0&2&1\\ 1&2&4&0&3\\ 2&4&3&1&0\\ 3&0&1&4&2 \end{bmatrix}\right).$$

of orthogonal Latin squares of order 5. This may be achieved by considering the conjugate of $\mathcal{M}_{5.1}$ which is obtained by applying the permutation $\binom{0123}{0213}$ to the elements of $T(\mathcal{M}_{5.1})$. This conjugate is given by the pair

$$\mathcal{M}_{5.2} = \left(\begin{bmatrix} 0&1&2&3&4\\ 1&2&4&0&3\\ 2&4&3&1&0\\ 3&0&1&4&2\\ 4&3&0&2&1 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4\\ 3&0&1&4&2\\ 4&3&0&2&1\\ 1&2&4&0&3\\ 2&4&3&1&0 \end{bmatrix}\right)$$

of orthogonal Latin squares of order 5. It may be noted that the relative cycle structure of the universals of the element 0 in $\mathcal{M}_{5.2}$ is $z_1^1 z_2^2$, whereas the relative cycle structure of the universals of the element 0 in $\mathcal{M}_{5.1}$ is $z_1^1 z_4^1$. Hence $\mathcal{M}_{5.2}$ may be mapped via a paratopism to a 2-MOLS of order 5 which is lexicographically smaller than $\mathcal{M}_{5.1}$.

For $n = 5$ and for each of the two cases $k = 3$ and $k = 4$ there are two branches on the first level of the search tree, both corresponding to the case where the first universal permutation of the

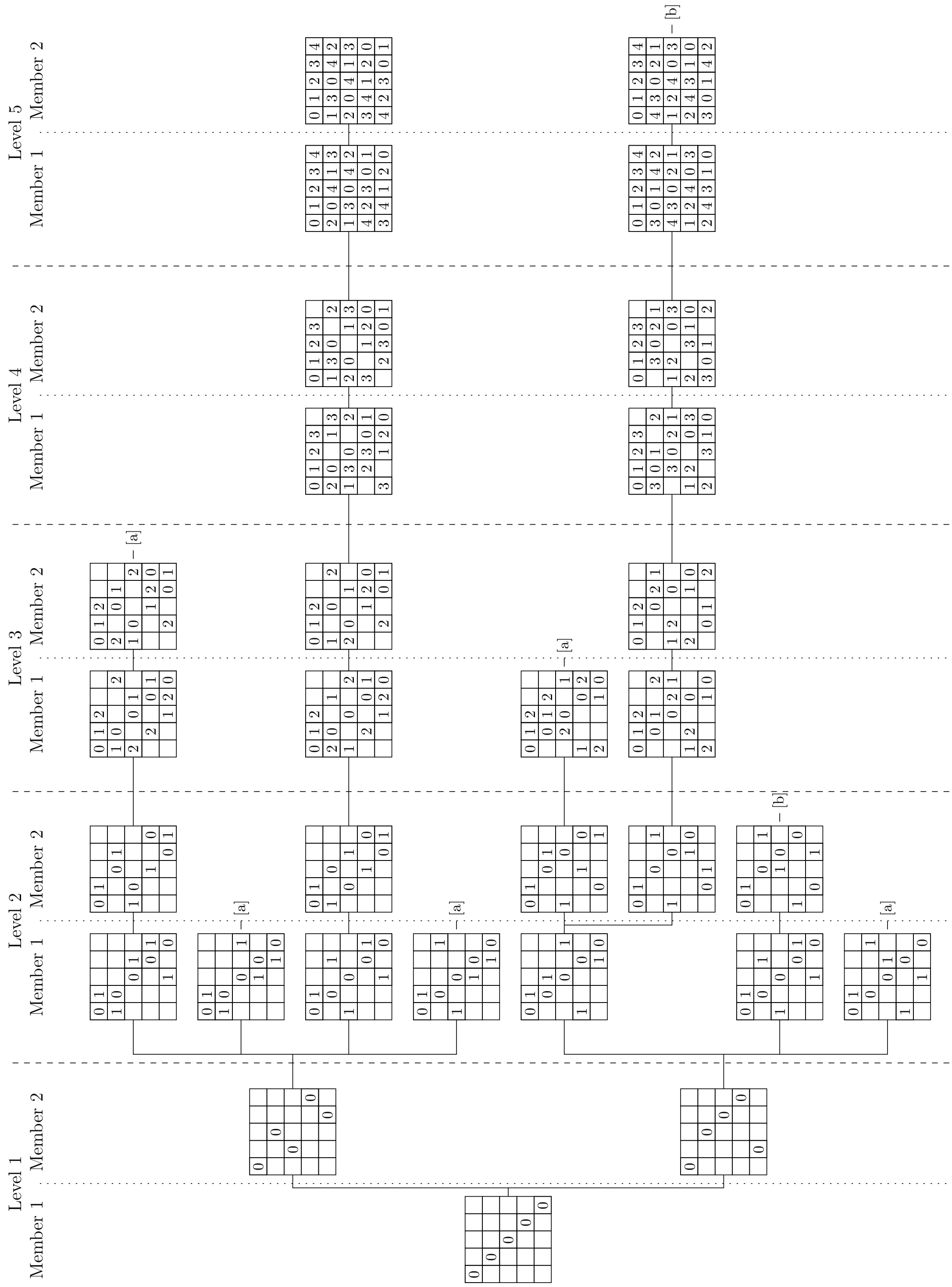

FIGURE 5.4: *The orderly generation search tree for main classes generated by 2-MOLS of order 5. Both members of a partially completed 2-MOLS are shown for each branch in the tree, except in cases where a universal was found for only one of the members of the partially completed 2-MOLS. For each leaf of the tree the main class leader generated is given, or else it is either indicated [a] that there are no possible universals that would have preserved the orthogonality of the two members, or [b] that the current partially completed 2-MOLS cannot be completed to a class leader.*

second Latin square has cycle structure $z_1^1 z_2^2$, and in the case where this universal permutation has cycle structure $z_1^1 z_4^1$ there are no feasible universals of the element 0 for the third Latin square (and in the case of $k = 4$, the fourth Latin square). Furthermore, on the second level of each of the two trees there are two branches, while the remaining levels of the trees have only one branch each, eventually producing one 3-MOLS of order 5 and one 4-MOLS of order 5, respectively.

Finally, for $k = 2, 3, 4$ a main class representative of the only main class of k-MOLS of order 5 is given by the first k Latin squares in the 4-MOLS of order 5,

$$\left(\begin{bmatrix} 0&1&2&3&4 \\ 2&0&4&1&3 \\ 1&3&0&4&2 \\ 4&2&3&0&1 \\ 3&4&1&2&0 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4 \\ 1&3&0&4&2 \\ 2&0&4&1&3 \\ 3&4&1&2&0 \\ 4&2&3&0&1 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4 \\ 4&2&3&0&1 \\ 3&4&1&2&0 \\ 1&3&0&4&2 \\ 2&0&4&1&3 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4 \\ 3&4&1&2&0 \\ 4&2&3&0&1 \\ 2&0&4&1&3 \\ 1&3&0&4&2 \end{bmatrix} \right).$$

For $n = 6$, only two relative cycle structures are admitted by universals, namely $z_1^1 z_2^1 z_3^1$ and $z_1^1 z_5^1$. For $2 \leq k \leq 5$ Table 5.15 gives the number of branches on each level of the search tree corresponding to each of these two cycle structures, and as expected no MOLS of order 6 is found.

		Level					
k	Cycle structure	1	2	3	4	5	6
2	$z_1^1 z_2^1 z_3^1$	1	27	38	11	0	0
	$z_1^1 z_5^1$	1	9	8	1	0	0
3	$z_1^1 z_2^1 z_3^1$	1	14	0	0	0	0
	$z_1^1 z_5^1$	2	6	0	0	0	0
4	$z_1^1 z_2^1 z_3^1$	1	0	0	0	0	0
	$z_1^1 z_5^1$	2	1	0	0	0	0
5	$z_1^1 z_2^1 z_3^1$	1	0	0	0	0	0
	$z_1^1 z_5^1$	1	1	0	0	0	0

TABLE 5.15: *For each cycle structure that the first universal of the second Latin square in a k-MOLS of order 6 may admit, the number of branches on each level of the search tree for k-MOLS of order 6 are given for all $k \in \{2, 3, 4, 5\}$.*

For $n = 7$, four relative cycle structures are admitted by the universals in a k-MOLS of order 7, namely $z_1^1 z_2^3$, $z_1^1 z_2^1 z_4^1$, $z_1^1 z_3^2$ and $z_1^1 z_6^1$. For $k = 2$ Table 5.16 gives the number of branches on each level corresponding to each of these four cycle structures. The search tree produced seven 2-MOLS of order 7 in 14 seconds, thereby verifying the number found by McKay [98].

For $n = 7$ and $k = 3$, there are three possible universals of the element 0 for the third Latin square if the first universal of the second Latin square has cycle structure $z_1^1 z_2^3$, and this section of the tree produces one 3-MOLS of order 7. For the cycle structures $z_1^1 z_2^1 z_4^1$ and $z_1^1 z_3^2$ there are five and six possible universals of the element 0 for the third Latin square, respectively. However, this section of the search tree produces no 3-MOLS. If the first universal of the second Latin square has cycle structure $z_1^1 z_6^1$, then there are no feasible universals of the element 0 for the third Latin square. Hence there is only one main class of 3-MOLS of order 7, and Table 5.17 provides more detail on the number of branches in various sections of the search tree for 3-MOLS of order 7. Each row in this table corresponds to a branch on the first level of the tree, and it gives the corresponding cycle structure, the number of branches on every other level, and the required computing time.

	Level						
Cycle structure	2	3	4	5	6	7	Time (s)
$z_1^1 z_2^3$	241	11 371	11 653	381	10	5	10
$z_1^1 z_2^1 z_4^1$	388	9 467	6 141	118	3	1	4
$z_1^1 z_3^2$	98	296	7	3	1	0	0
$z_1^1 z_6^1$	95	492	37	5	2	1	0
Total	822	21 626	17 838	507	16	7	14

TABLE 5.16: *The number of branches on each level of the search tree for 2-MOLS of order 7 for each cycle structure admitted by the first universal of the second Latin square in a k-MOLS of order 7 together with the required computing time. Level 1 is omitted since this level trivially has only one branch corresponding to each cycle structure, and the branches on Level 7 give the number of 2-MOLS of order 7 found in the corresponding section of the search tree.*

	Level						
Cycle structure	2	3	4	5	6	7	Time (s)
	1 719	844	1	1	1	1	2
$z_1^1 z_2^3$	1 459	592	0	0	0	0	2
	3 167	1 854	0	0	0	0	4
	315	117	0	0	0	0	1
	1 098	219	0	0	0	0	1
$z_1^1 z_2^1 z_4^1$	1 279	72	0	0	0	0	0
	860	74	0	0	0	0	0
	592	25	0	0	0	0	1
	10	2	1	1	1	0	1
	3	0	0	0	0	0	0
$z_1^1 z_3^2$	14	0	0	0	0	0	0
	11	0	0	0	0	0	0
	1	1	1	1	1	0	0
	1	0	0	0	0	0	0
	10 529	3 800	3	3	3	1	12

TABLE 5.17: *The number of branches on every other level of the search tree for 3-MOLS of order 7 for each cycle structure that the first universal of the second Latin square in a k-MOLS of order 7 may admit and each branch on the first level of the search tree corresponding to that cycle structure, together with the required computing time. Level 7 also gives the number of 3-MOLS of order 7 found in the corresponding section of the search tree.*

The cases of $k = 4$, 5 and 6 (for $n = 7$) are similar in that for the cycle structure $z_1^1 z_6^1$ there are no feasible pairs of universals of the element 0 for the third Latin square (hence the cycle structure $z_1^1 z_6^1$ does not give rise to any first level branches), while the cycle structure $z_1^1 z_3^2$ does not give rise to any second level branches. Table 5.18 gives the number of branches on the first level of each of the three search trees corresponding to the cycle structures $z_1^1 z_2^3$, $z_1^1 z_2^1 z_4^1$ and $z_1^1 z_3^2$, while Table 5.19 gives the number of branches on the second level of each of the three search trees corresponding to the cycle structures $z_1^1 z_2^3$ and $z_1^1 z_2^1 z_4^1$.

For $k = 4$ and for the cycle structure $z_1^1 z_2^3$ only a few first level branches give rise to branches on the third level, and Table 5.20 gives the number of branches on levels lower than the second for these first level branches. For $k = 5$ and 6 only the very first branch of the search tree gives rise to branches on the third level and lower, and this branch gives rise to exactly one branch on each of the lower levels in both cases.

Consequently only one main class of k-MOLS of order 7 was counted for $k = 4, 5, 6$, and the

	k		
Cycle Structure	4	5	6
$z_1^1 z_2^3$	18	15	11
$z_1^1 z_2^1 z_4^1$	19	13	5
$z_1^1 z_3^2$	7	5	1

TABLE 5.18: *The number of branches on the first level of the search tree for k-MOLS of order 7 corresponding to each of the cycle structures $z_1^1 z_2^3$, $z_1^1 z_2^1 z_4^1$ and $z_1^1 z_3^2$ for $k = 4, 5, 6$.*

	Cycle	First level branch																		
k	structure	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
4	$z_1^1 z_2^3$	16	142	170	56	75	112	77	27	106	93	175	38	91	80	121	104	168	121	
	$z_1^1 z_2^1 z_4^1$	29	45	44	16	42	42	45	50	10	28	12	10	3	7	7	5	9	3	2
5	$z_1^1 z_2^3$	4	3	0	0	2	2	4	3	3	1	3	8	4	3	4				
	$z_1^1 z_2^1 z_4^1$	7	4	7	4	0	0	1	0	1	0	0	0	0						
6	$z_1^1 z_2^3$	3	2	0	2	2	2	3	4	4	3	4								
	$z_1^1 z_2^1 z_4^1$	2	2	0	1	0														

TABLE 5.19: *The number of branches on the second level of the tree for $k = 4, 5, 6$ and for each branch on the first level of the search tree for k-MOLS of order 7 corresponding to the cycle structures $z_1^1 z_2^3$ and $z_1^1 z_2^1 z_4^1$ respectively.*

	Level				
First level branch	3	4	5	6	7
1	3	1	1	1	1
4	2	1	1	1	0
7	1	1	1	1	0
8	1	0	0	0	0
11	2	0	0	0	0
13	9	0	0	0	0
15	2	0	0	0	0

TABLE 5.20: *The number of branches on the third to seventh levels of the search tree for each of the branches on the first level of the search tree for 4-MOLS of order 7 corresponding to the cycle structure $z_1^1 z_2^3$ that give rise to branches on levels lower than the second.*

required computing time was approximately five seconds for $k = 4, 5$ and 32 seconds for $k = 6$ (utilising Computing Resource 1 in all cases). For $k = 3, 4, 5, 6$ a main class representative of the only main class of k-MOLS of order 7 is given by the first k Latin squares in the 6-MOLS of order 7

$$\left(\begin{bmatrix} 0&1&2&3&4&5&6\\ 2&0&4&1&5&6&3\\ 1&3&0&6&2&4&5\\ 4&2&5&0&6&3&1\\ 3&6&1&5&0&2&4\\ 6&5&3&4&1&0&2\\ 5&4&6&2&3&1&0 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6\\ 1&3&0&6&2&4&5\\ 2&0&4&1&5&6&3\\ 3&6&1&5&0&2&4\\ 4&2&5&0&6&3&1\\ 5&4&6&2&3&1&0\\ 6&5&3&4&1&0&2 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6\\ 4&2&5&0&6&3&1\\ 3&6&1&5&0&2&4\\ 6&5&3&4&1&0&2\\ 5&4&6&2&3&1&0\\ 2&0&4&1&5&6&3\\ 1&3&0&6&2&4&5 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6\\ 3&6&1&5&0&2&4\\ 4&2&5&0&6&3&1\\ 5&4&6&2&3&1&0\\ 6&5&3&4&1&0&2\\ 1&3&0&6&2&4&5\\ 2&0&4&1&5&6&3 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6\\ 6&5&3&4&1&0&2\\ 5&4&6&2&3&1&0\\ 2&0&4&1&5&6&3\\ 1&3&0&6&2&4&5\\ 4&2&5&0&6&3&1\\ 3&6&1&5&0&2&4 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6\\ 5&4&6&2&3&1&0\\ 6&5&3&4&1&0&2\\ 1&3&0&6&2&4&5\\ 2&0&4&1&5&6&3\\ 3&6&1&5&0&2&4\\ 4&2&5&0&6&3&1 \end{bmatrix}\right).$$

For $n = 8$ four relative cycle structures are admitted by the universals in a k-MOLS of order 8, namely $z_1^1 z_2^2 z_3^1$, $z_1^1 z_2^1 z_5^1$, $z_1^1 z_3^1 z_4^1$ and $z_1^1 z_7^1$. For $k = 2, 3, 4$ Table 5.21 gives the number of branches on every level of the tree corresponding to each of the four cycle structures $z_1^1 z_2^2 z_3^1$, $z_1^1 z_2^1 z_5^1$, $z_1^1 z_3^1 z_4^1$ and $z_1^1 z_7^1$, together with the required computing time. The search tree counted 2 165 main classes of 2-MOLS of order 8 in approximately 38 days (once again verifying the number found by McKay [98]), 39 main classes of 3-MOLS of order 8 in approximately 36 days and one main class of 4-MOLS of order 8 in approximately $4\frac{1}{2}$ days (in the first two cases Computing Resource 2 was utilised, while in the last case Computing Resource 1 was utilised).

k	Cycle structure	Level 1	2	3	4	5	6	7	8	Time (s)
2	$z_1^1 z_2^2 z_3^1$	1	12 095	21 661 780	870 780 093	541 480 115	5 213 158	10 182	2 033	2 969 152
	$z_1^1 z_2^1 z_5^1$	1	11 598	10 228 732	204 152 431	46 047 326	139 706	5 887	129	283 347
	$z_1^1 z_3^1 z_4^1$	1	4 001	681 424	1 050 327	20 172	370	132	0	2 352
	$z_1^1 z_7^1$	1	2 163	205 429	333 755	10 712	756	426	3	1 130
	Total	4	29 857	32 777 365	1 076 316 606	587 558 325	5 353 990	16 627	2 165	3 255 981
3	$z_1^1 z_2^2 z_3^1$	17	12 501 028	1 484 518 094	18 814 494	55	23	22	20	2 980 679
	$z_1^1 z_2^1 z_5^1$	14	3 358 273	61 708 802	63 157	97	92	84	17	160 494
	$z_1^1 z_3^1 z_4^1$	5	52 059	5 283	1	0	0	0	0	169
	$z_1^1 z_7^1$	9	37 403	9 079	82	64	53	53	2	353
	Total	45	15 948 763	1 546 241 258	18 877 734	216	168	159	39	3 141 695
4	$z_1^1 z_2^2 z_3^1$	419	86 064 551	3 028 409	1	0	0	0	0	380 634
	$z_1^1 z_2^1 z_5^1$	322	5 000 070	2 940	1	0	0	0	0	12 757
	$z_1^1 z_3^1 z_4^1$	37	1 314	0	0	0	0	0	0	8
	$z_1^1 z_7^1$	30	1 419	2	2	2	2	2	0	13
	Total	808	91 067 354	3 031 351	3	2	2	2	1	393 412

TABLE 5.21: *The number of branches on each level of the search tree for k-MOLS of order 8 corresponding to each cycle structure that the first universal of the second Latin square in a k-MOLS of order 8 may admit for $k = 2, 3, 4$, together with the required computing time. The branches on Level 8 give the number of k-MOLS of order 8 found in the corresponding section of the search tree.*

For $n = 8$ and $k = 5, 6, 7$ only the very last branch on the first level corresponding to the cycle structure $z_1^1 z_7^1$ gave rise to any branches on the third levels and lower, and this branch gave rise to exactly one branch on level ℓ for $3 \leq \ell \leq 8$. Table 5.22 gives the number of branches on levels 1 and 2 of the tree for $k = 5, 6, 7$ corresponding to each of the four cycle structures $z_1^1 z_2^2 z_3^1$, $z_1^1 z_2^1 z_5^1$, $z_1^1 z_3^1 z_4^1$ and $z_1^1 z_7^1$, together with the required computing time. The search tree counted one main class of 5-MOLS of order 8 in approximately 1 day, one main class of 6-MOLS of order 8 in approximately 2 hours and 20 minutes, and one main class of 7-MOLS of order 8 in approximately 3 hours (in all three cases Computing Resource 1 was utilised). For $k = 4, 5, 6, 7$ a class representative of the only main class of k-MOLS of order 8 is given by the first k Latin squares in the 7-MOLS of order 8

$$\left(\begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 1&0&4&7&2&6&5&3 \\ 2&4&0&5&1&3&7&6 \\ 3&7&5&0&6&2&4&1 \\ 4&2&1&6&0&7&3&5 \\ 5&6&3&2&7&0&1&4 \\ 6&5&7&4&3&1&0&2 \\ 7&3&6&1&5&4&2&0 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 2&4&0&5&1&3&7&6 \\ 3&7&5&0&6&2&4&1 \\ 4&2&1&6&0&7&3&5 \\ 5&6&3&2&7&0&1&4 \\ 6&5&7&4&3&1&0&2 \\ 7&3&6&1&5&4&2&0 \\ 1&0&4&7&2&6&5&3 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 3&7&5&0&6&2&4&1 \\ 4&2&1&6&0&7&3&5 \\ 5&6&3&2&7&0&1&4 \\ 6&5&7&4&3&1&0&2 \\ 7&3&6&1&5&4&2&0 \\ 1&0&4&7&2&6&5&3 \\ 2&4&0&5&1&3&7&6 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 4&2&1&6&0&7&3&5 \\ 5&6&3&2&7&0&1&4 \\ 6&5&7&4&3&1&0&2 \\ 7&3&6&1&5&4&2&0 \\ 1&0&4&7&2&6&5&3 \\ 2&4&0&5&1&3&7&6 \\ 3&7&5&0&6&2&4&1 \end{bmatrix}, \right.$$

$$\left. \begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 5&6&3&2&7&0&1&4 \\ 6&5&7&4&3&1&0&2 \\ 7&3&6&1&5&4&2&0 \\ 1&0&4&7&2&6&5&3 \\ 2&4&0&5&1&3&7&6 \\ 3&7&5&0&6&2&4&1 \\ 4&2&1&6&0&7&3&5 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 6&5&7&4&3&1&0&2 \\ 7&3&6&1&5&4&2&0 \\ 1&0&4&7&2&6&5&3 \\ 2&4&0&5&1&3&7&6 \\ 3&7&5&0&6&2&4&1 \\ 4&2&1&6&0&7&3&5 \\ 5&6&3&2&7&0&1&4 \end{bmatrix}, \begin{bmatrix} 0&1&2&3&4&5&6&7 \\ 7&3&6&1&5&4&2&0 \\ 1&0&4&7&2&6&5&3 \\ 2&4&0&5&1&3&7&6 \\ 3&7&5&0&6&2&4&1 \\ 4&2&1&6&0&7&3&5 \\ 5&6&3&2&7&0&1&4 \\ 6&5&7&4&3&1&0&2 \end{bmatrix} \right).$$

k	Cycle Structure	Level 1	Level 2	Time (s)
5	$z_1^1 z_2^2 z_3^1$	2 567	6 401 104	86 508
	$z_1^1 z_2^1 z_5^1$	1 071	41 313	2 298
	$z_1^1 z_3^1 z_4^1$	38	0	1
	$z_1^1 z_7^1$	36	3	8
	Total	3 712	6 442 420	88 815
6	$z_1^1 z_2^2 z_3^1$	1 565	6 499	8 330
	$z_1^1 z_2^1 z_5^1$	321	4	123
	$z_1^1 z_3^1 z_4^1$	3	0	0
	$z_1^1 z_7^1$	6	2	28
	Total	1 895	6 505	8 481
7	$z_1^1 z_2^2 z_3^1$	290	1101	19 823
	$z_1^1 z_2^1 z_5^1$	31	0	99
	$z_1^1 z_3^1 z_4^1$	1	0	0
	$z_1^1 z_7^1$	2	2	472
	Total	324	1 103	20 394

TABLE 5.22: *The number of branches on the first and second levels of the search tree for k-MOLS of order 8 corresponding to each cycle structure that the first universal of the second Latin square in a k-MOLS of order 8 may admit for $k = 5, 6, 7$, together with the required computing time.*

5.4.2 Enumeration of distinct and reduced MOLS

The number of reduced k-MOLS of order n and the number of distinct k-MOLS of order n may be determined utilising the methods presented in §4.5. Since a paratopism of a k-MOLS $\mathcal{M}$ of order n consists of a permutation applied to the rows of all the Latin squares in $\mathcal{M}$, a permutation applied to the columns of all Latin squares in $\mathcal{M}$, k permutations each applied to the symbols of some Latin square in $\mathcal{M}$ and $(k+2)!$ conjugate operations, the transformation group of a main class of k-MOLS of order n, namely $S_n \wr S_{k+2}$, has order $(k+2)!(n!)^{k+2}$. Therefore it follows by Theorem 4.5.1 that there are

$$\frac{(k+2)!(n!)^{k+2}}{|A(\mathcal{M})|}$$

k-MOLS of order n in the main class containing the k-MOLS $\mathcal{M}$ of order n, where $A(\mathcal{M})$ denotes the autoparatopism group of $\mathcal{M}$. Furthermore, it follows by Corollary 4.5.3 that there are

$$\frac{1}{(n!)^k(n-1)!}\left(\frac{(k+2)!(n!)^{k+2}}{|A(\mathcal{M})|}\right) = \frac{(k+2)!(n!)^2}{|A(\mathcal{M})|(n-1)!}$$

reduced k-MOLS of order n in the main class containing $\mathcal{M}$.

The autoparatopism groups for the class leaders generated, as discussed in the previous section, may be determined using `nauty` [96] and the method described in §4.4. The orders of the autoparatopism groups of k-MOLS of order n for which there is only one main class is given in Table 5.23.

The seven main classes of 2-MOLS of order 7 exhibit autoparatopism group orders of 6, 6, 126, 48, 2 352, 24 and 3 528, respectively, while Table 5.24 gives the number of main classes of 2- and 3-MOLS of order 8 which admit certain autoparatopism group orders.

Finally, the number of main classes of k-MOLS of order n, the number of reduced k-MOLS of order n and the number of distinct k-MOLS of order n are given in Tables 5.25, 5.26 and 5.27, respectively. Class representatives of main classes of k-MOLS of orders $3 \leq n \leq 8$ are available in Appendix B.3 for $2 \leq k \leq n-1$ (except for 2-MOLS of order 8).

		k					
		2	3	4	5	6	7
n	3	432					
	4	1 152	5 760				
	5	800	2 000	12 000			
	7	—	1 764	3 528	12 348	98 784	
	8	—	—	8 064	18 816	75 264	677 376

TABLE 5.23: *The orders of the autoparatopism groups of k-MOLS of order n for which there is exactly one main class for $n = 3, 4, 5, 7, 8$.*

	Group order																		
n	1	2	3	4	6	8	12	16	24	32	48	64	84	96	128	192	256	3 840	5 376
2	434	852	18	419	34	229	7	109	10	31	2	12	1	1	0	4	1	0	1
3	0	0	0	0	0	0	0	2	2	10	0	10	0	3	5	3	2	1	1

TABLE 5.24: *The number of main classes of 2 and 3-MOLS of order 8 which admit various autoparatopism group orders.*

		k					
	n	2	3	4	5	6	7
Main classes	3	1					
	4	1	1				
	5	1	1	1			
	6	0	0	0	0		
	7	7	1	1	1	1	
	8	2 165	39	1	1	1	1
Reduced	3	1					
	4	2	2				
	5	18	36	36			
	6	0	0	0	0		
	7	342 480	2 400	7 200	14 400	14 400	
	8	7 850 589 120	29 854 080	28 800	86 400	172 800	172 800

TABLE 5.25: *The number of main classes of k-MOLS of order n and the number of reduced k-MOLS of order n for $3 \leq n \leq 8$ and $2 \leq k \leq 7$.*

		k		
	n	2	3	4
Distinct	3	72		
	4	6 912	165 888	
	5	6 220 800	1 492 992 000	179 159 040 000
	6	0	0	0
	7	6 263 668 776 960 000	221 225 582 592 000 000	3 344 930 808 791 040 000 000
	8	64 324 116 731 941 355 520 000	9 862 699 452 850 608 537 600 000	383 623 424 598 626 795 520 000 000

TABLE 5.26: *The number distinct k-MOLS of order n for $3 \leq n \leq 8$ and $2 \leq k \leq 4$.*

5.5 Chapter summary

In this chapter distinct SOLS, idempotent SOLS, isomorphism classes of SOLS, transpose-isomorphism classes generated by SOLS and RC-paratopism classes generated by SOLS have been enumerated for orders $4 \leq n \leq 10$, where the numbers of only some of these classes were previously known, and only for $n \leq 9$. The numbers of distinct SOLSSOMs, standard SOLSSOMS, transpose-isomorphism classes generated by SOLSSOMs and RC-paratopism classes

(n, k)	Distinct
$(6, 5)$	0
$(7, 5)$	33 716 902 552 613 679 978 774 528
$(7, 6)$	169 933 188 865 172 974 512 094 838 784
$(8, 5)$	46 403 089 439 449 893 034 343 293 517 824
$(8, 6)$	3 741 945 132 397 240 250 509 786 690 481 029 120
$(8, 7)$	150 875 227 738 256 708 086 646 531 607 528 562 753 536

TABLE 5.27: *The number distinct k-MOLS of order n for $3 \leq n \leq 8$ and $5 \leq k \leq 7$.*

generated by SOLSSOMs have also been established for $4 \leq n \leq 10$, and none of these numbers was previously known. In particular, it was shown that no SOLS of order 10 satisfies even the most basic of necessary conditions for having a common orthogonal mate with its transpose, which in turn establishes both the non-existence of a SOLSSOM of order 10 and of a 3-MOLS of order 10 containing a SOLS and its transpose. Both these non-existence results relate to the infamous problem of determining whether or not a 3-MOLS of order 10 exists. Finally, distinct k-MOLS of order n, reduced k-MOLS of order n as well as main classes of k-MOLS of orders $3 \leq n \leq 8$ have also been enumerated in this chapter for $2 \leq k \leq 7$.

The Latin squares generated by the methods in this chapter are available online at the repository [82] in a compact text file format. Computer code for all the algorithms and procedures presented and applied in this chapter is available on the compact disc accompanying this dissertation, as are repositories (in the form of text files) containing RC-paratopism class representatives of SOLS, symmetric Latin squares and SOLSSOMs of orders $4 \leq n \leq 10$, and main class representatives of k-MOLS of orders $3 \leq n \leq 8$ for $2 \leq k \leq 7$.

CHAPTER 6

Conclusion

Contents

The dissertation closes here with a summary of the work contained therein, an appraisal of the contributions of the dissertation as well as a discussion on possibilities for future work in the area of Latin square subclass enumeration.

6.1 Summary of work contained in this dissertation

In this dissertation the numbers of various classes of SOLS and SOLSSOMs of orders $4 \leq n \leq 10$ and various classes of k-MOLS of orders $3 \leq n \leq 8$ for $2 \leq k \leq 7$ have been established. For this purpose, a number of preliminary mathematical definitions were required, and these were reviewed in Chapter 2 for the sake of completeness and self-containment. This chapter contains a general overview of the theory of Latin squares, and also provides a useful introduction to the theory of Latin squares for those not familiar with the field.

A number of important applications of Latin squares to sports tournament scheduling were described in Chapter 3. Two applications, in particular, were highlighted, namely *mixed doubles table tennis tournaments*, where two teams, each consisting of men and women, participate in a mixed doubles round-robin fashion, and *spouse-avoiding mixed doubles round-robin tournaments*, where married couples participate in a mixed doubles round-robin fashion in such a way that no person opposes or partners his/her spouse. It was shown that the former tournament may be scheduled using a 3-MOLS, while the latter tournament may be scheduled using a SOLSSOM. A review was also given on the efforts of various researchers to obtain constructions for these designs, and three unsolved problems were highlighted, namely the question of whether a 3-MOLS of order 10 exists, as well as whether SOLSSOMs of orders 10 and 14 exist.

In Chapter 4 a backtracking tree-search algorithm for enumerating σ-transformation classes of Latin squares was presented for any transformation of type σ. Before branching on the inclusion of universal into a partially completed Latin square, this algorithm verifies whether the partially completed Latin square has the potential to be completed to a well-defined class representative of a σ-transformation class. In this way it is ensured that only one Latin square from each class is generated by the algorithm, thereby determining the total number of classes as well as building a repository of class representatives in the process. A method for determining the σ-autotransformation group of a Latin square associated with any transformation of type σ was also presented in this chapter, and methods were reviewed which use these groups in order to determine class sizes and to enumerate special subclasses.

The main results of this dissertation are contained in Chapter 5, where the enumeration algorithms presented in Chapter 4 were utilised for the purpose of enumerating various subclasses of SOLS, SOLSSOMs and k-MOLS. In particular, distinct SOLS, idempotent SOLS, isomorphism classes generated by SOLS, transpose-isomorphism classes generated by SOLS and RC-paratopism classes generated by SOLS of orders $4 \leq n \leq 10$ were enumerated using the backtracking tree-search algorithm presented in the preceding chapter. Repositories of SOLS and symmetric Latin squares were then utilised in order to enumerate distinct SOLSSOMs, standard SOLSSOMs, transpose-isomorphism classes generated by SOLSSOMs and RC-paratopism generated by SOLSSOMs of orders $4 \leq n \leq 9$. Finally, distinct k-MOLS, reduced k-MOLS and main classes of k-MOLS of orders $3 \leq n \leq 8$ were enumerated for $2 \leq k \leq n-1$, where these numbers were previously known only for $k = 2$.

Furthermore, it was shown via a computerised filtering process that only four of the 121 642 RC-paratopism class representatives of SOLS of order 10 satisfy a necessary condition for admitting a common orthogonal mate with its transpose. It was easy to then verify by hand that these four SOLS of order 10 do not allow any common orthogonal mates with their transposes. This led to not only the establishment of the non-existence of a SOLSSOM of order 10, but also the non-existence of a set of three mutually orthogonal Latin squares of order 10 containing a SOLS and its transpose.

6.2 An appraisal of the contributions of this dissertation

The main contributions of this dissertation are threefold. The first contribution involves the extension of the work by Graham and Roberts [66] in 2006, who enumerated distinct SOLS, idempotent SOLS and isomorphism classes generated by idempotent SOLS of orders $4 \leq n \leq 9$. In this dissertation three additional classes of SOLS of orders $4 \leq n \leq 9$ were enumerated, namely isomorphism classes generated by all SOLS, transpose-isomorphism classes generated by all SOLS and RC-paratopism classes generated by all SOLS. This contribution was published in [32].

The second contribution involved the enumeration of all of the above-mentioned classes for SOLS of order 10, which was not previously possible to achieve within a realistic time frame. For this purpose the backtracking tree-search approach described in §4.3 was implemented on 12 computers in parallel in order to enumerate the RC-paratopism classes of SOLS of order 10. The search was, however, still not trivial to execute, as it required approximately 72 days of computing time. It was also shown that the next step in the enumeration of SOLS, namely the enumeration of SOLS of order 11, will not be possible to resolve using the current enumeration methods and computing power. This contribution was published in [33].

Another contribution involves the enumeration of SOLSSOMs of orders $4 \leq n \leq 9$ as well as the establishment of the non-existence of a SOLSSOM of order 10. SOLSSOMs were enumerated using existing repositories of SOLS and symmetric Latin squares, and the non-existence of

SOLSSOMs of order 10 was established using the SOLS of order 10 generated as mentioned above, and determining by computer which of them have the potential to admit a common orthogonal mate with their transposes. As it was found that no SOLS of order 10 can have a common orthogonal mate with its transpose, which not only shows that a SOLSSOM of order 10 does not exist (thereby settling a 32-year old existence question), but also that if a set of three mutually orthogonal Latin squares of order 10 exists, then it does not contain a SOLS and its transpose. This result therefore represents a necessary condition to the celebrated problem of determining whether a set of three mutually orthogonal Latin squares of order 10 exists, and it may be used in future to reduce the search space for such a set of Latin squares. This contribution has been submitted for publication in [34].

The final contribution of this dissertation involves the enumeration of k-MOLS of orders $3 \leq n \leq 8$ for $2 \leq k \leq n-1$. Three classes of k-MOLS of these orders were enumerated, namely distinct k-MOLS, reduced k-MOLS and main classes of k-MOLS utilising the backtracking tree-search approach described in §4.3.2. Of these results, only the number of main classes of 2-MOLS of orders $3 \leq n \leq 8$ had previously been established, and these numbers were verified in this dissertation.

The numbers of the various classes of SOLS and SOLSSOMs enumerated in this dissertation have been contributed as sequences to the *Online Encyclopedia of Integer Sequences* (OEIS) [129], and the reference numbers of these sequences together with the corresponding class descriptions are given in Table 6.1.

Reference number	Class
#A160368	Distinct SOLS
#A160367	Idempotent SOLS
#A181592	Isomorphism classes of idempotent SOLS
#A181593	Isomorphism classes of SOLS
#A160366	Transpose-isomorphism classes of SOLS
#A160365	RC-paratopism classes of SOLS
#A166490	Distinct SOLSSOMs
#A166489	Standard SOLSSOMs
#A166488	Transpose-isomorphism classes of SOLSSOMs
#A166487	RC-paratopism classes of SOLSSOMs

TABLE 6.1: *Reference numbers to new sequences in the Online Encyclopedia of Integer Sequences (OEIS) [129] which contain the enumeration results of this dissertation.*

6.3 Future work

This section contains a number of suggestions for possible future work in the area of Latin square enumeration with applications to sports tournament scheduling that emerged while research towards this dissertation was conducted. Two important areas are highlighted in what follows, namely open problems in the realm of enumeration of Latin squares and open problems centred around the existence and construction of Latin squares.

6.3.1 Proposals regarding enumeration

Due to the fact that obtaining an explicit formula for the number of Latin squares of any order is extremely unlikely, the enumeration of Latin squares is a step-by-step process where the numbers for each order have to be determined individually (possibly using the same methods). It therefore follows that once any enumeration work has been conducted, a next step to be taken will always present itself. The first proposal follows naturally from this observation.

Proposal 1 *Determine the number of RC-paratopism classes of SOLS of order 11.*

It was shown in §5.3.1 that enumerating SOLS of order 11 is not within realistic reach using the methods presented in this dissertation and the current computer processing power. Another method is therefore required for this purpose, and one improvement may be to include additional operations in the definition of an RC-paratopism. This will allow for larger classes which, in turn, would decrease their numbers and possibly result in a traversable search space. Alternative representations of SOLS may also be considered, such as representations using graphs or orthogonal arrays.

If the number of RC-paratopism classes of SOLS may be enumerated, and class representatives generated, then the other classes of SOLS mentioned in this dissertation may be enumerated by determining the RC-autoparatopism groups of these class representatives. It was shown in Chapter 5 that the required time for computing these groups using the computer program `nauty` was one second for order 9 and 1 859 seconds for order 10. It therefore follows that computing the RC-autoparatopism groups of SOLS of order 11 may provide a further hurdle that needs to be overcome.

The same observation above may be made for SOLSSOMs, as follows.

Proposal 2 *Determine the number of RC-paratopism classes of SOLSSOMs of order 11.*

Using the methods presented in this dissertation, this enumeration problem may be solved only once SOLS or symmetric Latin squares of order 11 have been enumerated. As in the case of SOLS, it has also been shown that the current methods would not render the enumeration of RC-paratopism classes of symmetric Latin squares of order 11 feasible within a realistic time frame. One may instead consider forming SOLSSOMs by generating the SOLS and symmetric mates simultaneously, rather than first generating one square and thereafter searching for possible orthogonal mates.

In this dissertation k-MOLS have only been enumerated up to and including order 8, and it was mentioned in §5.4 that 8-MOLS of order 9 have also been enumerated (in a theoretical fashion) in the literature. The next step in the enumeration of k-MOLS is therefore as follows.

Proposal 3 *Determine the number of main classes of k-MOLS of order 9, for $2 \leq k \leq 7$.*

6.3.2 Proposals regarding existence and construction

There are still a large number of unsolved problems in the theory of Latin squares with applications to sports tournament scheduling. In particular, it was noted in this dissertation that, although the case of order 10 has now been settled, the existence of SOLSSOMs of order 14 is still undecided, and this gives rise to the following natural proposal for future work.

Proposal 4 *Determine whether a SOLSSOM of order 14 exists.*

Since no 3-MOLS of order 10 has yet been found (despite a large number of attempts by researchers), it was an expected result that no SOLSSOM of order 10 can be found. For the case of order 14, however, a construction of a 3-MOLS of order 14 has been given in the literature, and this provides some circumstantial evidence that a SOLSSOM of order 14 may possibly exist. To the practical sports tournament scheduler the fact that no SOLSSOM of order 10 exists, on the other hand, is of little use. Since it is known that a SOLS of order 10 exists, it follows that the matches of a *spouse-avoiding mixed doubles round-robin (SAMDRR) tournament* may be obtained for ten couples. However, it was shown that there exists no partition of these matches into 9 rounds so that no player plays twice in any round. Hence, in order to obtain a schedule for such a tournament, it is necessary to consider relaxations on some of the requirements of an SAMDRR tournament, as was done by Burger and Van Vuuren [35] in 2009 for the purpose of obtaining good schedules for (unbalanced) SAMDRR tournaments of orders 6, 10 and 14. The authors did not, however, prove the optimality (in some sense) of their schedules, and the following proposal is therefore put forward.

Proposal 5 *Determine the smallest number of rounds in which a spouse-avoiding mixed doubles round-robin tournament may be scheduled for six, ten and fourteen married couples, or determine an optimal schedule (in some sense) for such a tournament where a number of the requirements have been relaxed.*

The problem of balancing carry-over effects in round-robin tournaments was briefly mentioned in §3.1, and a number of references to work done in this area was given. In particular, it has been shown that a balanced tournament of order n (one in which each player receives a carry-over effect from each other player at most once) exists if n is a power of two or if $n = 20$ or $n = 22$ [80]. For all other orders, however, the existence of a balanced tournament is undecided, and this interesting problem is proposed for future work.

Proposal 6 *Determine whether a round-robin tournament of order n which is balanced with respect to carry-over effects exists if $n \neq 2^r, 20, 22$, for some $r \in \mathbb{N}$.*

It was also been found that existence and construction problems in the theory of Latin squares may be formulated as integer programming problems and solved using standard solution techniques and/or software from the operations research literature. This has proved to be useful in, for example, establishing the non-existence of a pair of orthogonal Latin squares of order 6 in the approach adopted by Appa *et al.* [10]. Such construction approaches may be especially useful since quasigroup identities may be used as constraints in an integer programming model in order to construct special Latin squares with applications to sports tournament scheduling, a connection that seems not yet to have been made in the literature. The following proposal is therefore put forward.

Proposal 7 *Investigate integer programming formulations for the construction of special types of Latin squares with applications to sports tournament scheduling.*

Bibliography

[1] ABEL RJR, BENNET FE, ZHANG H & ZHU L, 2000. *A few more incomplete self-orthogonal Latin squares and related designs*, Australasian Journal of Combinatorics, **21**, pp. 85–94.

[2] ACKETA DM & MATIĆ-KEKIĆ S, 1995. *An attempt for construction of a triple of pairwise mutually orthogonal Latin squares on 10 elements*, Zbornik Radova Prirodno-Matematički Fakulteta Serija Matematika, **25**, pp. 141–153.

[3] ADAMSON IT, 1964. *Introduction to field theory*, Oliver and Boyd, Edinburgh.

[4] ALLENBY RBJT, 1983. *Rings, fields and groups*, Edward Arnold, London.

[5] ANDERSEN LD, 2007. *Factorisation of graphs*, pp. 740–755 in COLBOURN CJ & DINITZ JH (EDS), *The handbook of combinatorial designs*, 2nd Edition, CRC Press, Boca Raton (FL).

[6] ANDERSEN LD, 2007. *The history of Latin squares*, (Unpublished) Technical Report R-2007-32, Aalborg University, Aalborg.

[7] ANDERSON I, 1999. *Balancing carry-over effects in round robin tournaments*, pp. 1–16 in HOLROYD FC, QUINN KAS, ROWLEY C & WEBB BS (EDS) ,*Combinatorial designs and their applications*, CRC Press, Boca Raton (FL).

[8] ANDERSON I & FINIZIO NJ, 2007. *Whist tournaments*, pp. 663–668 in COLBOURN CJ & DINITZ JH (EDS), *The handbook of combinatorial designs*, 2nd Edition, CRC Press, Boca Raton (FL).

[9] ANDERSON I, COLBOURN CJ, DINITZ JH & GRIGGS TS, 2007. *Design theory: Antiquity to 1950*, pp. 11–22 in COLBOURN CJ & DINITZ JH (EDS), *The handbook of combinatorial designs*, 2nd Edition, CRC Press, Boca Raton (FL).

[10] APPA G, MAGOS D & MOURTOS I, 2004. *An LP-based proof for the non-existence of a pair of orthogonal Latin squares of order 6*, Operations Research Letters, **32**, pp. 336–344.

[11] ARMSTRONG MA, 1988. *Groups and symmetry*, Springer-Verlag, New York (NY).

[12] BALL WWR, 1914. *Mathematical recreations and essays*, Macmillan and Company Limited, London.

[13] BAMMEL SF & ROTHSTEIN J, 1975. *The number of* 9×9 *Latin squares*, Discrete Mathematics, **11**, pp. 93–95.

[14] Barra JR, 1963. *A propos d'un théorème de R.C. Bose*, Comptes Rendus de l'Académie des Sciences, **256**, pp. 5502–5504.

[15] Bennet FE & Zhu L, 1992. *Conjugate orthogonal Latin squares and related structures*, pp. 41–96 in Dinitz JH & Stinson DR (Eds), *Contemporary design theory: A collection of surveys*, John Wiley & Sons, New York (NY).

[16] Bennet FE & Zhu L, 1996. *Further results on the existence of HSOLSSOM*(h^n), Australasian Journal of Combinatorics, **14**, pp. 207–220.

[17] Bennet FE & Zhu L, 1996. *The spectrum of HSOLSSOM*(h^n) *where h is even*, Discrete Mathematics, **158**, pp. 11–25.

[18] Beth T, Jungnickel D & Lenz H, 1999. *Design theory*, 2nd Edition, Cambridge University Press, Cambridge.

[19] Biggs NL, 1985. *Discrete mathematics*, Oxford University Press, New York (NY).

[20] Bóna M, 2004. *Combinatorics of permutations*, CRC Press, Boca Raton (FL).

[21] Bose RC, 1938. *On the application of the properties of Galois fields to the problem of construction of hyper-Graeco-Latin squares*, Sankhyā: The Indian Journal of Statistics, **3(4)**, pp. 323–338.

[22] Bose RC & Shrikhande SS, 1959. *On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order* $4t + 2$, Proceedings of the National Academy of Sciences of the United States of America, **45(5)**, pp. 734–737.

[23] Bose RC, Shrikhande SS & Parker ET, 1960. *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture,* Canadian Journal of Mathematics, **7(2)**, pp. 189–203.

[24] Brayton RK, Coppersmith D & Hoffman AJ, 1974. *Self orthogonal Latin squares of all orders* $n \neq 2, 3, 6$, Bulletin of the American Mathematical Society, **80(1)**, pp. 116–118.

[25] Brown JW, 1968. *Enumeration of Latin squares with application to order 8*, Journal of Combinatorial Theory, **5**, pp. 177–184.

[26] Brown JW, 1972. *An extension of Mann's theorem to a triple of mutually orthogonal Latin squares of order 10*, Journal of Combinatorial Theory, Series A, **12(3)** pp. 316–318.

[27] Brown JW & Parker ET, 1982. *A try for three order-10 orthogonal Latin squares*, Congressus Numerantium, **36**, pp. 143–144.

[28] Brown JW & Parker ET, 1984. *Some attempts to construct orthogonal Latin squares*, Congressus Numerantium, **43**, pp. 201–202.

[29] Bruck RH, 1944. *Some results in the theory of quasigroups*, Transactions of the American Mathematical Society, **55(1)**, pp. 19–52.

[30] Budden FJ, 1972. *The fascination of groups*, Cambridge University Press, Cambridge.

[31] Burger AP, Kidd MP & Van Vuuren JH, 2010. *A graph-theoretic proof of the non-existence of a self-orthogonal Latin square of order 6*, Discrete Mathematics, **311(13)**, pp. 1 223–1 228.

[32] Burger AP, Kidd MP & Van Vuuren JH, 2010. *Enumeration of isomorphism classes self-orthogonal Latin squares*, Ars Combinatoria, **97**, pp. 143–152.

[33] Burger AP, Kidd MP & Van Vuuren JH, 2010. *Enumerasie van self-ortogonale Latynse vierkante van orde 10*, LitNet Akademies (Natuurwetenskappe), **7(3)**, pp. 1–22.

[34] Burger AP, Kidd MP & Van Vuuren JH, 2011. *Enumerasie van self-ortogonale Latynse vierkante met simmetriese ortogonale maats*, submitted to Die Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie.

[35] Burger AP & van Vuuren JH, 2009. *Skedulering van gade-vermydende gemengde-dubbels rondomtalie-tennistoernooie*, Die Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie, **28(1)**, pp. 35–63.

[36] Cayley A, 1877. *On the theory of groups*, Proceedings of the London Mathematical Society, **9**, pp. 126–133.

[37] Cayley A, 1890. *On Latin squares*, Oxford, Cambridge and Dublin Messenger of Mathematics, **19**, pp. 85–239.

[38] Colbourn CJ, Dinitz JH & Wanless IM, 2007. *Part III: Latin squares*, pp. 133–228 in Colbourn CJ & Dinitz JH (Eds), *The handbook of combinatorial designs*, 2nd Edition, CRC Press, Boca Raton (FL).

[39] Colbourn CJ & Rosa A, 1999. *Triple systems*, Clarendon Press, Oxford.

[40] Chein O, Pflugfelder HO & Smith JDH, 1990. *Quasigroups and loops: Theory and applications*, Heldermann Verlag, Berlin.

[41] Dénes J & Keedwell AD, 1974. *Latin squares and their applications*, The English University Press Ltd, Akaémiai Kiadó, Budapest.

[42] Dénes J & Keedwell AD, 1991. *Latin squares: New developments in the theory and applications*, Elsevier Science Publishers, New York (NY).

[43] Delisle E, 2010. *The search for a triple of mutually orthogonal Latin squares of order ten: Looking through pairs of dimension thirty-five and less*, MSc Thesis, University of Victoria, Victoria.

[44] Deo N, 1974. *Graph theory with applications to engineering and computer science*, Prentice–Hall, Englewood Cliffs (NJ).

[45] Dinitz JH, Froneck D, Lamken ER & Wallis WD, 2007. *Scheduling a tournament*, pp. 591–606 in Colbourn CJ & Dinitz JH (Eds), *The handbook of combinatorial designs*, 2nd Edition, CRC Press, Boca Raton (FL).

[46] Dinitz JH, Garnick DK & McKay BD, 1994. *There are 526,915,620 nonisomorphic one-factorisations of K_{12}*, Journal of Combinatorial Designs, **2(4)**, pp. 273–285.

[47] Dinitz JH & Williams HC, 2007. *Number theory and finite fields*, pp. 791–818 in Colbourn CJ & Dinitz JH (Eds), *The handbook of combinatorial designs*, 2nd Edition, CRC Press, Boca Raton (FL).

[48] Dixon JD & Mortimer B, 1996. *Permutation groups*, Springer-Verlag, New York (NY).

[49] Du B, 1993. *A few more resolvable spouse-avoiding mixed-doubles round robin tournaments*, Ars Combinatoria, **36**, pp. 309–314.

[50] Edmonds J, 2008. *How to think about algorithms*, Cambridge University Press, Cambridge.

[51] Erdös P & Kaplansky I, 1946. *The asymptotic number of Latin rectangles*, American Journal of Mathematics, **68**, pp. 230–236.

[52] Euler L, 1782. *Recherches sur une nouvelle espèce de quarrés magiques*, Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen, **9**, pp. 85–239, (English translation by Ho A & Klyve D).

[53] Euler L, 1849. *De quadratis magicis*, Commentationes Arithmeticae, **2**, pp. 593–602.

[54] Faradžev IA, 1978. *Constructive enumeration of combinatorial objects*, Problèmes Combinatoires et Théorie des Graphes, CNRS, **260**, pp. 131–135.

[55] Fisher RA, 1925. *Statistical methods for research workers*, Oliver and Boyd, Edinburgh.

[56] Fisher RA, 1935. *The design of experiments*, Oliver and Boyd, Edinburgh.

[57] Fisher RA & Yates F, 1934. *The* 6×6 *Latin squares*, Proceedings of the Cambridge Philosophical Society, **30**, pp. 492–507.

[58] Franklin MF, 1984. *Cyclic generation of self orthogonal Latin squares*, Utilitas Mathematica, **25**, pp. 135–147.

[59] Frolov M, 1890. *Sur les permutations carrées*, Journal de Mathématiques Spéciales, **4**, pp. 8–11, 25–30.

[60] Gallian JA, 1993. *On the converse of Lagrange's theorem*, Mathematics Magazine, **66(1)**, p. 23.

[61] Gardner M, 2000. *Modeling mathematics with playing cards*, The College Mathematics Journal, **31(3)**, pp. 173–177.

[62] Gessel IM, 1986. *Counting three-line Latin rectangles*, pp. 106–111 in Labelle G & Leroux P (Eds), *Combinatoire énumerative*, Springer, Berlin.

[63] Gessel IM, 1987. *Counting Latin rectangles*, Bulletin of the American Mathematical Society, **16(1)**, pp. 79–82.

[64] Godsil CD & McKay BD, 1984. *Asymptotic enumeration of Latin rectangles*, Bulletin of the American Mathematical Society, **10(1)**, pp. 91–92.

[65] Goulden IP & Jackson DM, 1983. *Combinatorial enumeration*, John Wiley & Sons, New York (NY).

[66] Graham GP & Roberts CE, 2006. *Enumeration and isomorphic classification of self-orthogonal Latin squares*, Journal of Combinatorial Mathematics and Combinatorial Computing, **59**, pp. 101–118.

[67] Grimaldi RP, 1994. *Discrete and combinatorial mathematics: An applied introduction*, Addison-Wesley Publishing Company, Reading (MA).

[68] Hall M, 1945. *An existence problem for Latin squares*, Bulletin of the American Mathematical Society, **51**, pp. 387–388.

[69] Hall M, 1959. *The theory of groups*, The Macmillan Company, New York (NY).

[70] Hanani H, 1970. *On the number of orthogonal Latin squares*, Journal of Combinatorial Theory, Series A, **8**, pp. 247–271.

[71] Hedayat A, 1973. *An application of sum composition: A self orthogonal Latin square of order ten*, Journal of Combinatorial Theory, Series A, **14**, pp. 256–260.

[72] Hedayat A, 1973. *Self orthogonal Latin square designs and their importance*, Biometrics, **29**, pp. 393–395.

[73] Hedayat A, 1975. *Self orthogonal Latin square designs and their importance, II*, Biometrics, **31**, pp. 755–759.

[74] Hedayat A, 1978. *A generalization of sum composition: Self orthogonal Latin square designs with sub self orthogonal Latin square designs*, Journal of Combinatorial Theory, Series A, **24**, pp. 202–210.

[75] Herstein IN, 1975. *Topics in algebra*, John Wiley & Sons, New York (NY).

[76] Holt DF, 2005. *Handbook of computational group theory*, CRC Press, Boca Raton (FL).

[77] Horton JD, 1970. *Variations on a theme by Moore*, Proceedings of the Louisiana Conference on Combinatorics, Graph Theory and Computing, Louisiana State University, Baton Rouge (LA), pp. 146–166.

[78] Hulpke A, Kaski P & Östergård PRJ, 2010. *The number of Latin squares of order 11*, to appear in Mathematics of Computation.

[79] Kaplansky I, 1963. *Solution to the "Problème des ménages"*, Bulletin of the American Mathematical Society, **49**, pp. 784–785.

[80] Keedwell AD, 2000, *Designing tournaments with the aid of Latin squares: A presentation of old and new results*, Utilitas Mathematica, **58**, pp. 65–85.

[81] Kendall MG, 1948. *Who discovered the Latin square?*, The American Statistician, **2(4)**, p. 13.

[82] Kidd MP, 2010. *A repository of self-orthogonal Latin squares*, [Online], [Cited October 27th, 2010], Available from `http://www.vuuren.co.za` → `Repositories`

[83] Kidd MP, 2010. *A tabu-search for minimising the carry-over effects value of a round-robin tournament*, ORiON, **26(2)**, pp. 125–141.

[84] Kleiner I, 1986. *The evolution of group theory: A brief survey*, Mathematics Magazine, **59(4)**, pp. 195–215.

[85] Kolesova G, Lam CWH & Thiel L, 1990. *On the number of* 8×8 *Latin squares*, Journal of Combinatorial Theory, Series A, **54**, pp. 143–148.

[86] Lam CWH, Kolesova G & Thiel L, 1991. *A computer search for finite projective planes of order 9*, Discrete Mathematics, **92**, pp. 187–195.

[87] Laurie DP, 2004. Professor, Department of Mathematical Sciences, University of Stellenbosch, [Personal Communication], Contactable at `dpl@sun.ac.za`.

[88] Laywine CF & Mullen GL, 1998. *Discrete mathematics using Latin squares*, John Wiley & Sons, New York (NY).

[89] Ledermann W, 1949. *Introduction to the theory of finite groups*, Oliver and Boyd, Edinburgh.

[90] Lindner CC, 1971. *The generalized singular direct product for quasigroups*, Canadian Mathematical Bulletin, **14(1)**, pp. 61–63.

[91] Lindner CC, Mullin RC & Stinson DR, 1983. *On the spectrum of resolvable orthogonal arrays invariant under the Klein group* K_4, Aequationes Mathematicae, **26**, pp. 176–183.

[92] Lucas E, 1891. *Théorie des nombres*, Gauthier-Villars, Paris.

[93] MacMahon PA, 1960. *Combinatory analysis*, Chelsea Publishing Company, New York (NY).

[94] MacNeish HF, 1922. *Euler squares*, Annals of Mathematics, **23**, pp. 221–227.

[95] Martin GE, 2001. *Counting: The art of enumerative combinatorics*, Springer, New York (NY).

[96] McKay BD, 1984. `nauty`, [Online], [Cited December 3rd 2009], Available from `http://cs.anu.edu.au/~bdm/nauty/`

[97] McKay BD, 1998. *Isomorph-free exhaustive generation*, Journal of Algorithms, **26**, pp. 306–324.

[98] McKay BD, 2010. *Latin squares*, [Online], [Cited October 26th, 2010], Available from `http://cs.anu.edu.au/~bdm/data/latin.html`.

[99] McKay BD, Meynert A & Myrvold W, 2007. *Small Latin squares, quasigroups, and loops*, Journal of Combinatorial Designs, **15**, pp. 98–119.

[100] McKay BD & Rogoyski E, 1995. *Latin squares of order 10*, The Electronic Journal of Combinatorics, **2**, Note 3.

[101] McKay BD & Wanless IM, 1999. *Most Latin squares have many subsquares*, Journal of Combinatorial Theory, Series A, **86**, pp. 323–347.

[102] McKay BD & Wanless IM, 2005. *On the number of Latin squares*, Annals of Combinatorics, **9**, pp. 335–344.

[103] McLaurin SC & Smith DD, 1989. *Constructing transpose-orthogonal Latin squares*, Journal of Combinatorial Theory, Series A, **51**, pp. 221–226.

[104] Mendelsohn NS, 1971. *Combinatorial designs as models of universal algebras*, pp. 123–132 in Tutte WT (Ed), *Recent progress in combinatorics: Proceedings of the Third Waterloo Conference on Combinatorics*, Academic Press, New York (NY).

[105] Mendelsohn NS, 1971. *Latin squares orthogonal to their transposes*, Journal of Combinatorial Theory, Series A, **11**, pp. 187–189.

[106] Mills WH, 1972. *Three mutually orthogonal Latin squares*, Journal of Combinatorial Theory, Series A, **13**, pp. 79–82.

[107] Mullin RC & Németh E, 1969. *On furnishing room squares*, Journal of Combinatorial Theory, **7**, pp. 266–272.

[108] Mullin RC & Németh E, 1970. *A construction for self orthogonal Latin squares from certain room squares*, Proceedings of the Louisiana Conference on Combinatorics, Graph Theory and Computing, Louisiana State University, Baton Rouge (LA), pp. 231–226.

[109] Myrvold W, 2005. *Negative results for orthogonal Latin squares of order 10*, Journal of Combinatorial Mathematics and Combinatorial Computing, **29**, pp. 95–105.

[110] Németh E, 1969. *A study of room squares*, PhD Thesis, University of Waterloo, Waterloo.

[111] Neumann PM, 1979. *A lemma that is not Burnside's*, The Mathematical Scientist, **4**, pp. 133–141.

[112] Norton HW, 1939. *The* 7×7 *squares,* Annals of Eugenics, **9**, pp. 269–307.

[113] Owens PJ & Preece DA, 1995. *Complete sets of pairwise orthogonal Latin squares of order 9*, Journal of Combinatorial Mathematics and Combinatorial Computing, **18**, pp. 83–96.

[114] Parker ET, 1959. *Construction of some sets of mutually orthogonal Latin squares*, Proceedings of the American Mathematical Society, **10(6)**, pp. 946–949.

[115] Parker ET, 1959. *Orthogonal Latin squares*, Proceedings of the National Academy of Sciences, **45**, pp. 859–862.

[116] Parker ET, 1963. *Computer investigation of orthogonal Latin squares of order ten,* Proceedings of Symposia in Applied Mathematics, **15**, pp. 73–81.

[117] Parker ET, 1975. *Nonexistence of a triple of orthogonal Latin squares of order 10 with group of order 25 — a search made short*, Journal of Combinatorial Theory, Series A, **19**, pp. 243–244.

[118] Pflugfelder HO, 1990. *Quasigroups and loops: Introduction*, Heldermann, Berlin.

[119] Pulleyblank WR, 1975. *Mixed doubles table tennis tournaments,* Proceedings of the Fifth Manitoba Conference on Numerical Mathematics, Utilitas Mathematica Publishing Inc., Winnipeg, pp. 593–598.

[120] Read RC, 1978. *Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations,* pp. 107–120 in Alspach B, Hell P & Miller DJ (Eds), *Algorithmic aspects of combinatorics*, North-Holland Publushing Company, Amsterdam.

[121] Roberts FS & Tesman B, 2009. *Applied combinatorics*, 2nd Edition, CRC Press, Boca Raton (FL).

[122] Robinson DF, 1981. *Constructing an annual round-robin tournament played on neutral grounds*, Mathematical Chronicle, **10**, pp. 73–82.

[123] Roth RL, 2001. *A history of Lagrange's theorem on groups*, Mathematics Magazine, **74(2)**, pp. 99–108.

[124] Rotman JJ, 1984. *An introduction to the theory of groups*, Allyn and Bacon Inc., Boston (MA).

[125] Russel KG, 1980. *Balancing carry-over effects in round robin tournaments*, Biometrika, **67**, pp. 127–131.

[126] Sade A, 1951. *An omission in Norton's list of* 7×7 *squares*, Annals of Mathematical Statistics, **22**, pp. 306–307.

[127] Sade A, 1960. *Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens*, Annales de la Société Scientifique de Bruxelles. Série I, **74**, pp. 91–99.

[128] Shao JY & Wei WD, 1992. *A formula for the number of Latin squares*, Discrete Mathematics, **110**, pp. 293–296.

[129] Sloane N, 1995. *The online encyclopedia of integer sequences*, [Online], [Cited December 8th, 2009], Available from `http://oeis.org`.

[130] Stein CM, 1978. *Asymptotic evaluation of the number of Latin rectangles*, Journal of Combinatorial Theory, Series A, **25**, pp. 38–49.

[131] Stein SK, 1957. *On the foundations of quasigroups*, Transactions of the American Mathematical Society, **85(1)**, pp. 228–256.

[132] Stellenbosch University, 2011. *Rasatsha high performance computer*, [Online], [Cited October 28th, 2011], Available from `https://www0.sun.ac.za/hpc/index.php?title=Main_Page`.

[133] Stinson DR, 1984. *A short proof of the nonexistence of a pair of orthogonal Latin squares of order six*, Journal of Combinatorial Theory, Series A, **36**, pp. 373–376.

[134] Stones D, 2010. *The many formulae for the number of Latin rectangles*, Electronic Journal of Combinatorics, **17**, Article 1.

[135] Styan GPH & Boyer C, 2009. *Some comments on Latin squares and on Graeco-Latin squares, illustrated with postage stamps and old playing cards*, Statistical Papers, **50**, pp. 917–941.

[136] Tarry G, 1900. *Le probleme des 36 officiers*, Comptes Rendus Association Franqaise pour l'Advancement des Science, **29(2)**, pp. 170–203.

[137] Todorov DT, 1985. *Three mutually orthogonal Latin squares of order 14*, Ars Combinatoria, **20**, pp. 45–48.

[138] Ullrich P, 2002. *Officers, playing cards, and sheep*, Metrika, **56**, pp. 189–204.

[139] Wallis WD, 1979. *Spouse-avoiding mixed doubles tournaments*, Annals of the New York Academy of Sciences, **319**, pp. 549–554.

[140] Wallis WD, 1983. *The problem of hospitable golfers*, Ars Combinatoria, **15**, pp. 149–152.

[141] Wallis WD, 1984. *Three orthogonal Latin squares*, Congressus Numerantium, **42**, pp. 69–86.

[142] Wallis WD, 1988. *Combinatorial designs*, Marcel Dekker, Inc., New York (NY).

[143] Wang SMP, 1978. *On self-orthogonal Latin squares and partial transversals of Latin squares*, PhD Thesis, Ohio State University, Columbus (OH).

[144] Wang SMP & Wilson RM, 1978. *A few more squares II*, Congressus Numerantium, **21**, p. 688.

[145] Weisner L, 1963. *Special orthogonal Latin squares of order 10*, Canadian Mathematical Bulletin, **6(1)**, pp. 61–63.

[146] Wells MB, 1967. *The number of Latin squares of order eight*, Journal of Combinatorial Theory, **3**, pp. 98–99.

[147] Wikipedia Online Encyclopedia, 2010. *Whist*, [Online], [Cited October 29$^{\text{th}}$, 2010], Available from `http://en.wikipedia.org/wiki/Whist`.

[148] Whitelaw TA, 1988. *Introduction to abstract algebra*, 2$^{\text{nd}}$ Edition, Blackie and Son Ltd, London.

[149] Wolfram Mathworld, 2009. *Abelian*, [Online], [Cited April 30$^{\text{th}}$, 2009], Available from `http://mathworld.wolfram.com/Abelian.html`

[150] Wolfram Research, 2010. *Wolfram Mathematica 7*, [Online], [Cited October 26$^{\text{th}}$, 2010], Available from `http://www.wolfram.com/products/mathematica/index.html`

[151] Yamamoto K, 1951. *On the asymptotic number of Latin rectangles*, Japanese Journal of Mathematics, **21**, pp. 113–119.

[152] Yamamoto K, 1954. *Euler squares and incomplete Euler squares of even degrees*, Memoirs of the Faculty of Science, Kyūshū University, Series A, **8(2)** pp. 161–180.

[153] Yamamoto K, 1961. *Generation principles of Latin squares*, Bulletin de l'Institut International de Statistique, **38**, pp. 73–76.

[154] Zhu L, 1982. *A short disproof of Euler's conjecture concerning orthogonal Latin squares*, Ars Combinatoria, **14**, pp. 47–55.

[155] Zhu L, 1984. *A few more self-orthogonal Latin squares with symmetric orthogonal mates*, Congressus Numerantium, **42**, pp. 313–320.

APPENDIX A

Discrete mathematical preliminaries

Contents

This appendix contains a number of notions from the field of abstract algebra which are used throughout this dissertation, especially in the enumeration algorithms presented in Chapter 4. In §A.1 the notions of permutations, permutation cycles and conjugacy classes of permutations are reviewed. Permutation cycles allow for the classification of permutations into conjugacy classes according to their cycle structures, and the notion of conjugate permutations describe in what way permutations in the same conjugacy class may be mapped to one another. A method for determining all possible mappings between two permutations in the same conjugacy class is also presented. In §A.2 a brief introduction to the field of group theory is given together with a number of basic definitions and examples, followed by a discussion on group actions. Two well-known results concerning group actions are reviewed from the literature, and the important application of these results to enumerating classes of combinatorial objects and determining class sizes is illustrated by means of an example.

A.1 Permutations

This section contains a number of important mathematical prerequisites concerning permutations, most of which are used throughout this dissertation due to the fact that there is a strong relationship between the notions of permutations and Latin squares.

There are a number of different definitions for permutations in the combinatorial literature; see, for instance, Bóna [20, Definition 0.1], Dixon and Mortimer [48, p. 2] and Martin [95, p. 74].

Definition A.1.1 (Permutation) *Given a set S of cardinality n, a* permutation of order n *is a one-to-one mapping from S onto itself.* □

Hence a permutation of order n may be used to rearrange a set of n distinct, ordered objects [20]. Throughout this dissertation it is assumed (unless stated otherwise) that all permutations act upon the set $\mathbb{Z}_n$. The notation $p(i) \in \mathbb{Z}_n$ is used to denote the image of $i \in \mathbb{Z}_n$ under the permutation p. The image of a subset of $\mathbb{Z}_n$, say $S = \{s_1, s_2, \ldots, s_k\} \subseteq \mathbb{Z}_n$ for some $k \leq n$, is denoted by $p(S) = \{p(s_1), p(s_2), \ldots, p(s_k)\}$. A permutation p is *lexicographically smaller* than a permutation q, denoted by $p < q$, if $p(k) < q(k)$ for some $k \leq n$ and $p(i) = q(i)$ for all $i < k$.

A useful representation of a permutation p involves a $2 \times n$ array in which the first row is a listing of the elements of $\mathbb{Z}_n$ in natural order and the second row is a listing of the elements of $p(\mathbb{Z}_n)$, and in which i and $p(i)$ appear in the same column for all $i \in \mathbb{Z}_n$. It is customary (see, for instance, Dixon and Mortimer [48, p. 2] and Ledermann [89, p. 62]) to write this representation in the form

$$p = \begin{pmatrix} 0 & 1 & \ldots & n-1 \\ p(0) & p(1) & \ldots & p(n-1) \end{pmatrix}.$$

Provided that $p(i)$ is found below i in this representation, the first row may be, in fact, written in any order [89, p. 63]. A permutation p of order n for which the image of $p(i)$ is i for all $i \in \mathbb{Z}_n$ leaves the arrangement of a set of objects unchanged. This permutation is therefore called the *identity permutation* and is henceforth denoted by e.

Two notions that play especially important roles in most of the enumeration algorithms described in this dissertation is that of *permutation cycles* and *conjugacy classes* of permutations, which are discussed in detail in the next two subsections.

A.1.1 Permutation cycles

The following important definition may be found in Bóna [20, p. 74] and Martin [95, p. 76] and allows for the classification of permutations into equivalence classes, as will be described in the next subsection.

Definition A.1.2 (Permutation cycles) *A k-*cycle *of a permutation of order n is an ordered k-tuple denoted by $(c_0, c_1, \ldots, c_{k-1})$ for which $p(c_i) = c_{i+1}$ for all $0 \leq i \leq k-1$, where addition is performed modulo k.* □

For example, a 2-cycle and a 3-cycle of the permutation $p = \binom{0\,1\,2\,3\,4}{3\,4\,1\,0\,2}$ are $(0, 3)$ and $(1, 4, 2)$, respectively. No distinction is made between the cycles $(1, 4, 2)$, $(2, 1, 4)$ and $(4, 2, 1)$ since any one of these alternatives implies that the image of 1 is 4, the image of 4 is 2 and the image of 2 is 1. Hence $(0, 3)$ and $(1, 4, 2)$ are the only cycles of p and p may be written in *cycle notation* [20, p. 74] as $(0, 3)(1, 4, 2)$. An n-cycle of a permutation consists of all elements of $\mathbb{Z}_n$ and is also called a *full-cycle*, whereas a 1-cycle is sometimes called a *fixed point*. A permutation is said to be of *type* $(a_1, a_2, \ldots, a_n)$ if it has a_i cycles of length $i \in \{1, 2, \ldots, n\}$, and the *cycle structure* of a permutation of type $(a_1, a_2, \ldots, a_n)$ is denoted by $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n}$, where the symbol z is simply a place holder. For simplicity, any factor $z_i^{a_i}$ in this notation for which $a_i = 0$ is omitted for the sake of brevity. The permutation $p = \binom{0\,1\,2\,3\,4\,5\,6}{1\,0\,3\,2\,5\,6\,4}$, for example, has cycle structure $z_2^2 z_3^1$ and is of type $(0, 2, 1, 0, 0)$ since it has two 2-cycles and one 3-cycle.

The *cycle structure representative* of a cycle structure $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n}$ is the lexicographically smallest permutation that exhibits the cycle structure. If (a, b, c, d) is a cycle of a permutation, then it may be written as $\binom{a\,b\,c\,d}{b\,c\,d\,a}$ in regular permutation form. It is clear that this cycle would be represented in the lexicographically smallest way if $a < b < c < d$. Hence the elements of each cycle of a cycle structure representative must appear in non-decreasing order when cycling over all elements of the cycle from the smallest element to the largest element. It is also easy to see that the cycles should appear in order of non-decreasing length. Hence given a cycle structure, say $z_1^1 z_2^2 z_3^1$, the cycles may be written in order of non-decreasing length, *i.e*

$$(\textvisiblespace)(\textvisiblespace\,\textvisiblespace)(\textvisiblespace\,\textvisiblespace)(\textvisiblespace\,\textvisiblespace\,\textvisiblespace),$$

and the elements $0, 1, \ldots, n-1$ may be filled into the empty spaces from left to right, resulting in the permutation

$$(0)(1{,}2)(3{,}4)(5, 6, 7),$$

or

$$\begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,2\,1\,4\,3\,6\,7\,5 \end{pmatrix}$$

in regular notation.

It is also useful to define a lexicographical ordering of cycle structures. The cycle structure $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n}$ is *lexicographically smaller* than the cycle structure $z_1^{b_1} z_2^{b_2} \ldots z_n^{b_n}$, denoted by $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n} \prec z_1^{b_1} z_2^{b_2} \ldots z_n^{b_n}$, if $a_k > b_k$ for some $k \leq n$ and $a_i = b_i$ for all $1 \leq i < k$. For instance, the cycle structure $z_1^1 z_2^2 z_3^1$ is lexicographically smaller than the cycle structure $z_1^1 z_2^1 z_5^1$. All possible cycle structures of permutations of order 5 are shown in Table A.1 in lexicographical order, together with the cycle structure representative of each cycle structure.

Cycle structure	Representative
z_1^5	$\binom{0\,1\,2\,3\,4}{0\,1\,2\,3\,4}$
$z_1^3 z_2^1$	$\binom{0\,1\,2\,3\,4}{0\,1\,2\,4\,3}$
$z_1^2 z_3^1$	$\binom{0\,1\,2\,3\,4}{0\,1\,3\,4\,2}$
$z_1^1 z_2^2$	$\binom{0\,1\,2\,3\,4}{0\,2\,1\,4\,3}$
$z_1^1 z_4^1$	$\binom{0\,1\,2\,3\,4}{0\,2\,3\,4\,1}$
$z_2^1 z_3^1$	$\binom{0\,1\,2\,3\,4}{1\,0\,3\,4\,2}$
z_5	$\binom{0\,1\,2\,3\,4}{1\,2\,3\,4\,0}$

Table A.1: *The seven possible cycle structures of a permutation of order 5, together with the cycle structure representative of each cycle structure.*

It may be observed from Table A.1 that, when arranging the possible cycle structures of a permutation of a certain order lexicographically, the cycle structure representatives are also in lexicographical order. This observation is established in general in the following proposition.

Proposition A.1.1 *If p and q are the cycle structure representatives of the cycle structures $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n}$ and $z_1^{b_1} z_2^{b_2} \ldots z_n^{b_n}$ respectively, and $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n} \prec z_1^{b_1} z_2^{b_2} \ldots z_n^{b_n}$, then $p < q$.*

Proof: Since $z_1^{a_1} z_2^{a_2} \ldots z_n^{a_n} \prec z_1^{b_1} z_2^{b_2} \ldots z_n^{b_n}$, it follows that $a_k > b_k$ for some $k \leq n$ and $a_i = b_i$ for all $1 \leq i < k$. Hence (by definition of a cycle structure representative) all cycles of length i for $1 \leq i < k$ are equal for p and q, and so are the first $a_k - b_k$ cycles of length k. Hence $p(a) = q(a)$ for all $0 \leq a \leq \sum_{i=1}^{k} a_i - b_k$. The next cycle of p (the first cycle that is different from those of q) is also of length k, while the next cycle of q is of length $k+1$. Without loss of generality, these cycles may be written as $(0, 1, \ldots, k-1)$ and $(0, 1, \ldots, k)$, and for all $0 \leq a \leq k-2$ it follows that $p(a) = q(a)$. However, $p(k-1) = 0$ and $q(k-1) = k$, and therefore $p < q$. ■

A.1.2 Conjugacy classes of permutations

Consider an ordered list of objects (a, b, c, d, e) and a permutation $p = \binom{01234}{34102}$ applied to it. The resulting rearrangement of the list may be found by indexing the list by means of $\mathbb{Z}_5$ (see Figure A.1(a)), rewriting the indices as their images under p (as shown in Figure A.1(b)) and rearranging the objects in order for the indices again to be in natural order (as shown in Figure A.1(c)). From this it is clear that the object in position i moves to position $p(i)$ if p is applied to (a, b, c, d, e).

0	1	2	3	4
a	b	c	d	e

(a)

3	4	1	0	2
a	b	c	d	e

(b)

0	1	2	3	4
d	c	e	a	b

(c)

FIGURE A.1: *Applying the permutation $p = \binom{01234}{34102}$ to an ordered list (a, b, c, d, e) of objects.*

Now consider applying a second permutation, say $q = \binom{01234}{24031}$, to the list (d, c, e, a, b), delivering a third rearrangement of the list (a, b, c, d, e), namely the list (e, b, d, a, c). In effect a composition of the permutations p and q has been applied to the list (a, b, c, d, e), denoted by $q \circ p$. It is conventional to use the notation $q \circ p$ to denote the fact that p is applied first and q second (see Martin [95, p. 75]).

Since a permutation p rearranges a set of objects such that the object in position i moves to position $p(i)$, a second permutation q applied to the resulting rearrangement will move the object in position $p(i)$ to position $q(p(i))$. The object in position i of the *initial* arrangement therefore moves to position $q(p(i))$, and the composition of two permutations p and q is therefore given by

$$q \circ p = \begin{pmatrix} 0 & 1 & \ldots & n-1 \\ q(p(0)) & q(p(1)) & \ldots & q(p(n-1)) \end{pmatrix}.$$

Consider, as an example, the composition

$$q \circ p = \begin{pmatrix} 01234 \\ 24031 \end{pmatrix} \circ \begin{pmatrix} 01234 \\ 34102 \end{pmatrix} = \begin{pmatrix} 01234 \\ 31420 \end{pmatrix}$$

of the two permutations $p = \binom{01234}{34102}$ and $q = \binom{01234}{24031}$ in the above example. It may be found that 2 *goes to* 1 in p while 1 *goes to* 4 in q, and therefore 2 *goes to* 4 in $q \circ p$, and so on. Applying $q \circ p = \binom{01234}{31420}$ to the list (a, b, c, d, e) in the example above delivers the list (e, b, d, a, c), as expected.

Given a permutation p, let q be a permutation defined by $q(p(i)) = i$ for all $i \in \mathbb{Z}_n$ and define the two permutations $r = q \circ p$ and $r' = p \circ q$. Then $r(i) = q(p(i)) = i$ for any $i \in \mathbb{Z}_n$ and therefore $q \circ p = e$ (the identity permutation). Also, for any $i, j \in \mathbb{Z}_n$, let $i = p(j)$. Hence $q(i) = j$ and $r'(i) = p(q(i)) = p(j) = i$ and $p \circ q = e$. Hence q is the *inverse permutation* of p. The inverse permutation of a permutation p, denoted by p^{-1}, therefore has the property that if $p(i) = j$ for some $i, j \in \mathbb{Z}_n$, then $p^{-1}(j) = i$. It is also easy to show that $(p \circ q)^{-1} = (q^{-1} \circ p^{-1})$. This is true since if $(p \circ q)(a) = p(q(a)) = b$ for some $a, b \in \mathbb{Z}_n$, then $a = q^{-1}(p^{-1}(b)) = (q^{-1} \circ p^{-1})(b)$.

The following definition provides a means of grouping permutations into equivalence classes called *conjugacy classes*, and the definition may also be found in Bóna [20, p. 80].

Definition A.1.3 (Conjugate permutation) *A permutation p of order n is a* conjugate permutation *of a permutation q of order n if there exists a permutation r of order n such that $q = r \circ p \circ r^{-1}$, in which case p and q are in the same* conjugacy class. □

An even simpler classification of conjugate permutations is given by the following proposition.

Proposition A.1.2 ([20], Lemma 3.13) *Two permutations are in the same conjugacy class if and only if they are of the same type.*

Proof: Suppose p and q are conjugate permutations and suppose $r \circ p \circ r^{-1} = q$ for some permutation r. Let $(x_1, x_2, \ldots, x_k)$ be any cycle of p. Hence $p(x_i) = x_{i+1}$ for all $1 \leq i \leq k$, where addition is performed modulo k. Then, since $q(r(x_i)) = r(p(r^{-1}(r(x_i)))) = r(x_{i+1})$, the sequence $(r(x_1), r(x_2), \ldots, r(x_k))$ is a cycle in q. Hence the action of r on p preserves the cycles of p, and therefore p and q are of the same type.

Conversely, suppose two permutations p and q are of the same type $(a_1, a_2, \ldots, a_n)$. Then for each cycle $(x_1, x_2, \ldots, x_k)$ in p there is a corresponding cycle $(y_1, y_2, \ldots, y_k)$ in q of the same length. Define a permutation r such that $r(x_i) = y_i$ for all $1 \leq i \leq k$, where addition is performed modulo k. Then $r(p(r^{-1}(y_i))) = r(p(x_i)) = r(x_{i+1}) = y_{i+1} = q(y_i)$. If this is done for each cycle of p, then it follows that $r \circ p \circ r^{-1} = q$. ■

The size of a conjugacy class is determined in the following proposition.

Proposition A.1.3 *If two n-permutations p and q are both of type $(a_1, a_2, \ldots, a_n)$, then the number of permutations r for which $r \circ p \circ r^{-1} = q$ is $\prod_{i=1}^{n} a_i! i^{a_i}$.*

Proof: Since the action of r on p above preserves the cycle structure of p, each of the a_i cycles of length i in p are mapped to one of the a_i cycles of length i in q. This may be done in any order, *i.e.* in $a_i!$ distinct ways. Consider mapping the cycle $(x_1, x_2, \ldots, x_i)$ in p to the cycle $(y_1, y_2, \ldots, y_i)$ in q. The permutation r may be chosen such that $r(x_1) = y_j$ for any $1 \leq j \leq i$ in i distinct ways. Then, since $q(y_j) = y_{j+1}$ (where addition is performed modulo i), $r(p(r^{-1}(y_j))) = r(p(x_1)) = r(x_2) = y_{j+1}$. Continuing in this fashion it may be shown that $r(x_3) = y_{j+2}$, $r(x_4) = y_{j+3}$, and so on, mapping the entire cycle of p to the cycle of q. Hence each of the a_i cycles of length i in p may be mapped to one of the a_i cycles of length i in q in i^{a_i} distinct ways. Taking the product over all cycles in p delivers the desired result. ■

A.2 Groups

Abstract algebra is to a large extent concerned with the notion of combining two elements of a set by some rule or process in order to obtain a unique new element of the set as a result [69, p. 1]. This rule of combination is most commonly referred to as *composition* [89, p. 1], denoted by the symbol '$\circ$', and is defined to be a *binary operator* in view of the fact that it combines *two* elements [19, p. 271]. The notation $a \circ b = c$ is used to denote the composition of two elements a and b, where c, often called the *product* of a and b [89, p. 2], is the result after composition. This notion leads to the important notion of a *group*.

A.2.1 Basic definitions

Given a set of elements S and a binary operator $\circ$, if $a, b, a \circ b \in S$, then S is *closed* with respect to $\circ$ [75, p. 27]. The binary operator $\circ$ is said to be *associative* if $(a \circ b) \circ c = a \circ (b \circ c)$ for any three elements $a, b, c \in S$, and if there is an element $e \in S$ such that $e \circ a = a \circ e = a$ for all $a \in S$, the element e is known as an *identity element* of S. If e is an identity element of S and $a \in S$, then an element $a^{-1} \in S$ for which $a \circ a^{-1} = a^{-1} \circ a = e$ is known as an *inverse element* of a in S.

The notions defined above are often referred to as *laws* and may be found in most textbooks on group theory (see, for instance, Allenby [4, §5.3] and Herstein [75, §2.1]). These laws may be used to define various combinatorial structures, the following of which represents the basis of group theory and which may be found in most books (or chapters) on group theory (see, for instance, Allenby [4, Definition 5.3.1] and Biggs [19, §13.1]).

Definition A.2.1 (Group) *A set G consisting of n distinct elements that are closed with respect to a binary operator $\circ$ forms a* group *of order n, denoted by $(G, \circ)$, if*

(1) $\circ$ is associative,

(2) there exists an identity element in G, and

(3) for each element of G there exists an inverse element. □

An example of a group is the set of the integers $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ together with the binary operation of addition modulo $n \in \mathbb{N}$, denoted by $(\mathbb{Z}_n, +)$. Since the remainder after division by n is one of the integers $0, 1, \ldots, n-1$, the set $\mathbb{Z}_n$ is closed with respect to addition modulo n. To show that this set forms a group, it may be shown that the required laws are satisfied. Since ordinary addition is associative, addition modulo n is also associative, and the element 0 has the property that $a + 0 = a \,(\mathrm{mod}\ n)$ and is therefore an identity element. Furthermore, for each element $a \in \mathbb{Z}_n$ there exists a unique element b such that $a + b = 0 \,(\mathrm{mod}\, n)$, given by $b = n - a$ in ordinary integer arithmetic. It is also easy to see that the group $(\mathbb{Z}_n, +)$ exists for any $n \in \mathbb{N}$.

A simple representation of any group may be found via its so-called Cayley table.

Definition A.2.2 (Cayley Table) *Given a group $(G, \circ)$ of order n, the* Cayley table *(such named due to investigations of such tables by Arthur Cayley [36]) of $(G, \circ)$ is an $n \times n$ table in which the rows and columns are indexed by the elements of G and for which the intersection of the row indexed by a and the column indexed by b contains the product $a \circ b$.* □

The Cayley table of the group $(\mathbb{Z}_4, +)$ is given in Table A.2. It is customary to write the binary operator of the group in the top-left corner of the table (see Allenby [4, p. 64] and Grimaldi [67, p. 778]). The row and column indicating the indexing symbol of each row and column in the table are often referred to as the *borders* of the Cayley table [41, p. 15].

The following two definitions underpin the connection between Latin squares and group theory. These definitions may be found in Hall [69, p. 7] and Dénes and Keedwell [41, p. 16].

Definition A.2.3 (Quasigroup) *A set Q closed with respect to a binary operator $\circ$ is a* quasigroup *of order n, denoted by $(G, \circ)$, if $a \circ b = c$ has a unique solution in Q when any two of a, b or c are specified in Q.* □

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

TABLE A.2: *The Cayley table of the group* $(\mathbb{Z}_4, +)$.

Definition A.2.4 (Loop) *A* loop *of order n is a quasigroup $(Q, \circ)$ of order n containing an identity element.* □

An example of a quasigroup (that does not form a group) is $(\mathbb{Z}_n, \ominus)$, where $\ominus$ is a well-defined binary operator such that $a \ominus b = a - b \pmod n$ for any $a, b \in \mathbb{Z}_n$. To prove that $(\mathbb{Z}_n, \ominus)$ forms a quasigroup, let $a \ominus x = b$ and $a \ominus y = b$ for $a, b, x, y \in \mathbb{Z}_n$. Hence $a - x = b \pmod n$ and $a - y = b \pmod n$. Subtracting the second relation from the first delivers $y - x = 0 \pmod n$, and, since x and y were elements of $\mathbb{Z}_n$ to begin with, $x = y$. The Cayley table of the quasigroup $(\mathbb{Z}_4, \ominus)$ is given in Figure A.3.

$\ominus$	0	1	2	3
0	0	3	2	1
1	1	0	3	2
2	2	1	0	3
3	3	2	1	0

TABLE A.3: *The Cayley table of the quasigroup* $(\mathbb{Z}_4, \ominus)$.

Consider the set P_n of all permutations of order n together with the binary operation of composition of permutations. It is clear, by definition, that the set P_n is closed with respect to the composition of permutations. The following theorem shows that $(P_n, \circ)$ is, in fact, a group commonly known as the *symmetric group* of order n, denoted by S_n (see Bóna [20, p. 73] and Dixon and Mortimer [48, p. 2] for proofs of this theorem).

Theorem A.2.1 ([89], Theorem 1) *The set P_n of all permutations of order n forms a group with respect to the composition of permutations.*

Throughout this dissertation it is assumed that all elements of the group S_n are permutations of the set $\mathbb{Z}_n$, except where otherwise stated. In the case where the elements of S_n are permutations of some other set S, this group is referred to as the *symmetric group on S*.

Consider the set $\{0, 2\}$, which is a subset of $\mathbb{Z}_4$, together with the binary operation of addition modulo 4. It is easily verified that $\{0, 2\}$ is closed with respect to addition modulo 4, that associativity holds, that 0 is an identity element and that 2 has an inverse, *i.e.* itself. Hence $\{0, 2\}$ forms a smaller group within the group $(\mathbb{Z}_4, +)$. A formal definition of such a smaller group follows in general and may be found in, for instance, Armstrong [11, §5] and Budden [30, §14].

Definition A.2.5 (Subgroup) *Given a group $(G, \circ)$, a subset H of G forms a* subgroup $(H, \circ)$ *of $(G, \circ)$ if $(H, \circ)$ forms a group.* □

Consider the subset $\{2\}$ of $\mathbb{Z}_4$ together with the binary operation of addition modulo 4. Clearly this is not a group since $\{2\}$ is not closed with respect to addition modulo 4. By performing addition modulo 4 the element 0 is obtained, and the group $(\{0, 2\}, +)$ is generated by this action. A formal definition of such an occurrence follows and a similar definition may be found in [4, Definition 5.6.11].

Definition A.2.6 (Generating set) *Given a group $(G, \circ)$, a subset H of G is a* generating set *of another subset of G, denoted by $\langle H\rangle$, if any element of $\langle H\rangle$ may be written as a sequence (possibly with repetitions) of compositions of elements of H. If $(\langle H\rangle, \circ)$ forms a group, then H* generates *the subgroup $(\langle H\rangle, \circ)$ of $(G, \circ)$.* □

It is known for a group $(G, \circ)$ that any subset of G generates a subgroup of $(G, \circ)$ (see, for instance, Allenby [4, Theorem 5.6.12]). This gives rise to the following corollary which provides a means of finding a generating set for a group.

Corollary A.2.1 *If a and b are elements of a group $(G, \circ)$ which do not appear together in any subgroup of $(G, \circ)$ except for $(G, \circ)$ itself, then $\{a, b\}$ generates $(G, \circ)$.*

A.2.2 Group actions

A group of particular interest when dealing with Latin squares is the symmetric group of order 6, namely S_3. Consider the six symmetries of the equilateral triangle shown in Figure A.2. If T_1 is regarded as the initial triangle, then T_2 and T_3 are the two distinct rotations of it, and T_4, T_5 and T_6 are reflections of it through the three axes shown. Equivalently the six symmetries of the equilateral triangle represent the six different ways of labelling the corners by using three distinct symbols.

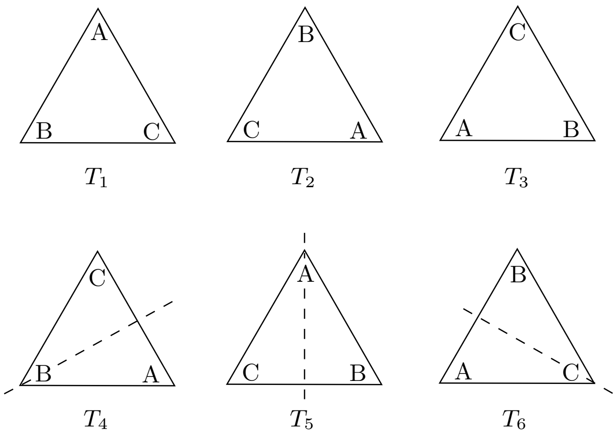

FIGURE A.2: *The six symmetries of the equilateral triangle.*

Let θ be a mapping defined by $\theta(T_i) = T_j$ if T_j is a clockwise rotation of T_i. Hence θ may be seen as a rotation operator and $\theta(T_1) = T_2$, for example. Note also that $\theta^2(T_1) = T_3$, for example, and that $\theta^3(T_i) = T_i$ for any $1 \leq i \leq 6$. Hence θ^3 is an identity mapping, henceforth denoted by ϵ. Define also the mapping ϕ by $\phi(T_i) = T_j$ if T_j is a reflection of T_i through the vertical axis. For example, $\phi(T_1) = T_5$. Therefore ϕ may be seen as a reflection operator. Note that, for example, $\phi(T_3) = T_4$ and $\phi^2(T_i) = T_i$ for any $1 \leq i \leq 6$, so that $\phi^2 = \epsilon$.

Furthermore, it may be noted that $\epsilon(T_1) = T_1$, $\theta(T_1) = T_2$, $\theta^2(T_1) = T_3$, $\theta(\phi(T_1)) = T_4$, $\phi(T_1) = T_5$ and $\theta^2(\phi(T_1)) = T_6$. Each operation in the set $\{\epsilon, \theta, \theta^2, \theta\phi, \phi, \theta^2\phi\}$ therefore corresponds to a different permutation of the symmetric group S_3, and since the composition of two mappings is equivalent to the composition of the corresponding permutations, this set forms a group with respect to composition of mappings, known as the *dihedral group* D_3[1].

The act of the dihedral group D_3 transforming (*i.e.* rotating and/or reflecting) the equilateral triangle is an example of a *group action*, of which a formal definition follows and may be found in Holt [76, §2.2] and Martin [95, §37].

Definition A.2.7 (Group action) *Given a group $(G, \bullet)$ and a set S, a* group action *of $(G, \bullet)$ on S is a mapping α from G to the symmetric group on S such that $\alpha(a) \circ \alpha(b) = \alpha(a \bullet b)$, where $\circ$ represents the composition of permutations.* □

Hence each element of G is associated with a permutation of S. The image of an element $s \in S$ under the permutation $\alpha(g)$ is commonly denoted by s^g, and $s^g \in S$ may be seen as the result of g *acting* upon s. Since $\alpha(g)$ is a permutation, $s^g = t^g$ implies that $s = t$ for $g \in G$ and $s, t \in S$. Note, however, that $s^g = s^h$ for $s \in S$ and $g, h \in G$ does not necessarily imply that $g = h$.

Since $a \bullet b = c$ for any $a, b, c \in G$ implies that $\alpha(a) \circ \alpha(b) = \alpha(c)$ (where $\circ$ denotes the composition of permutations), it follows that $(s^a)^b = s^c = s^{a \bullet b}$ for any $s \in S$. If e is the identity element of G, then $a \bullet e = e \bullet a = a$ implies that $\alpha(a) \circ \alpha(e) = \alpha(e) \circ \alpha(a) = \alpha(a)$ and $\alpha(e)$ is the identity permutation of S. Therefore, $s^e = s$ for any $s \in S$. Also, if g^{-1} is the inverse element of g, then $g^{-1} \bullet g = e$ implies $\alpha(g^{-1}) \circ \alpha(g) = \alpha(e)$ and therefore $\alpha(g^{-1}) = \alpha(g)^{-1}$. Hence, if $s^g = t$, then $s = t^{g^{-1}}$ for any $s, t \in S$.

Consider, for example the six triangles shown in Figure A.2. The dihedral group D_3 acts on the set $\{T_1, T_2, T_3, T_4, T_5, T_6\}$ by means of the rotation operator θ, the reflection operator ϕ and the identity operator ϵ. For instance, the element $\epsilon \in D_3$ is associated with the permutation

$$\begin{pmatrix} T_1 & T_2 & T_3 & T_4 & T_5 & T_6 \\ T_1 & T_2 & T_3 & T_4 & T_5 & T_6 \end{pmatrix},$$

while the element θ is associated with the permutation

$$\begin{pmatrix} T_1 & T_2 & T_3 & T_4 & T_5 & T_6 \\ T_2 & T_3 & T_1 & T_6 & T_4 & T_5 \end{pmatrix}.$$

It may be verified that each element of D_3 is associated with a permutation of this set.

For a group $(G, \circ)$ acting on a set S, define a relation $\sim$ on S such that $s \sim t$ for all $s, t \in S$ if and only if there exists an element $g \in G$ such that $s^g = t$. It is easy to see that the classes formed by the relation $\sim$ form equivalence classes, a formal definition of which may be found in Holt [76, Definition 2.14] and Biggs [19, p. 304].

Definition A.2.8 (Orbits) *For a group $(G, \circ)$ acting on a set S, the equivalence classes formed by the relation $\sim$ on S for which $s \sim t$ if and only if there exists an element $g \in G$ such that $s^g = t$ for all $s, t \in S$ are called* orbits *of the group action.* □

Two elements are therefore in the same equivalence class or orbit if and only if one may be transformed via a group action into the other. In particular, the orbit of a specific element

[1]See Budden [30, §13] for a complete discussion of dihedral groups, including the group D_3.

$s \in S$ is given by the set $s^G = \{s^g \mid g \in G\}$, and it may be noted that $s^G = t^G$ if and only if $s \sim t$. As noted before, $s^g = s^h$ for $s \in S$ and $g, h \in G$ does not necessarily imply that $g = h$. If $g \neq h$, then $s^{g \circ h} = s$, and the element $g \circ h \in G$ *fixes* the element s (note that g is also not necessarily equal to h^{-1}). This gives rise to the following definition which may also be found in Holt [76, Definition 2.15] and Biggs [19, p. 305].

Definition A.2.9 (Stabiliser) *In a group $(G, \circ)$ acting on a set S, the set $G_s = \{g \in G \mid s^g = s\}$ is called the* stabiliser *of $s \in S$.* □

Given an element $g \in G$, the set $S_g = \{s \in S \mid s^g = s\}$ may also be defined and has been called the *fix* of g by Martin [95, p. 91] and the *fixed point set* of g by Holt [76, p. 19]. Furthermore, it may be noted that $\sum_{g \in G} S_g = \sum_{s \in S} G_s$.

The following two lemmas are extremely useful in the enumeration of various combinatorial designs, as noted by Holt [76, §10.5]. The proofs of these lemmas are neither long nor intricate, but are not given here since they rely on concepts not within the scope of this dissertation. See, for instance, Holt [76, pp. 19–20], Martin [95, pp. 90–92] and Biggs [19, pp. 307–310] for the proofs of these lemmas.

Lemma A.2.1 (Orbit-stabiliser theorem) *If a group $(G, \circ)$ acts on a set S, then $|G| = |s^G||G_s|$ for any $s \in S$. Hence the order of the group is equal to the cardinality of any orbit multiplied by the order of the stabiliser of any element in that orbit.*

A result that follows directly from the proof of the above lemma is that $|G_s| = |G_t|$ if $s^G = t^G$. In other words, the sizes of the stabilisers of elements in the same orbit are equal.

The following lemma, according to Rotman [124, p. 52], should be credited to Cauchy and Frobenius, since Frobenius first proved it by utilising some ideas put forth by Cauchy[2].

Lemma A.2.2 (Cauchy-Frobenius Lemma) *If a group $(G, \circ)$ acts on a set S, then the number of orbits on S is $\frac{1}{|G|}\sum_{g \in G} S_g = \frac{1}{|G|}\sum_{s \in S} G_s$. Hence the number of orbits equals the average number of elements fixed by each element of the group.*

As an example of the usefulness of these lemmas (as well as the concepts of group actions, orbits and stabilisers) in the enumeration of combinatorial designs, the isomorphism classes of a special type of triple system is considered here. A *transitive triple* $||a, b, c||$ on a set S is a 3-set of ordered pairs of the form $\{(a, b), (a, c), (b, c)\}$ for $a, b, c \in S$. A *directed triple system (DTS)* on a set S is a set of transitive triples such that any ordered pair on S appears in exactly one triple, and $|S|$ is said to be the *order* of the triple system. The set of triples $\{||0, 1, 2||, ||1, 0, 3||, ||3, 2, 0||, ||2, 3, 1||\}$ is an example of a DTS on $\mathbb{Z}_4$. An *isomorphism* α of a DTS D of order n on the set S is a permutation of S which replaces each triple $||a, b, c||$ by $||\alpha(a), \alpha(b), \alpha(c)||$. It is easy to verify that an isomorphism applied to a DTS again produces

[2] In spite of this there still seems to be some confusion as to the name of Lemma A.2.2. It has been called Burnside's Lemma by Martin [95, p. 92], the Frobenius-Burnside Lemma by McKay *et al.* [99] and the Cauchy-Frobenius Lemma by Holt [76, p. 20] and Rotman [124, p. 52]. Neumann [111], however, seems to be the most outspoken about the true identities of the persons who should receive credit for this lemma, namely Cauchy and Frobenius, and he summarises his reasons for the mistake of calling it Burnside's Lemma in his paper entitled *A lemma that is not Burnside's* [111]. Neumann's paper, as well as the remark by Rotman, may stand as motivation for calling this lemma (in this dissertation, at least) the Cauchy-Frobenius Lemma.

another (not necessarily distinct) DTS. An isomorphism of a DTS of order n is therefore a group action of the group S_n on the set of all DTS of order n. The orbits of this group action are called *isomorphism classes*. Hence if a DTS D may be transformed into a DTS D' by an isomorphism, then they are in the same isomorphism class. The stabilisers of this group action are called *automorphism groups*, and the automorphism group of a DTS D, denoted by $A(D)$, are those isomorphisms which map D onto itself.

There are three isomorphism classes (orbits) of DTS of order 4 (see Colbourn and Rosa [39, p. 433]), and three representatives of these classes (one from each class) are given in Table A.4.

D_1	D_2	D_3
$\|\|0,1,2\|\|$	$\|\|0,1,2\|\|$	$\|\|0,1,2\|\|$
$\|\|1,0,3\|\|$	$\|\|1,0,3\|\|$	$\|\|1,3,0\|\|$
$\|\|3,2,0\|\|$	$\|\|2,3,0\|\|$	$\|\|2,0,3\|\|$
$\|\|2,3,1\|\|$	$\|\|3,2,1\|\|$	$\|\|3,2,1\|\|$

TABLE A.4: *Three non-isomorphic directed triple systems of order 4*

It is easily verified (by applying all possible permutations to each DTS) via MATHEMATICA, for instance, that these three DTS are, in fact, non-isomorphic. Since it is of such a small order, the computing time is insignificant. The stabilisers of D_1, D_2 and D_3 (*i.e.* their automorphism groups), namely $A(D_1)$, $A(D_2)$ and $A(D_3)$, may also easily be computed by considering all possible permutations. Lemma A.2.1 may now be employed in order to enumerate the total number of distinct DTS of order 4. It is found that $|A(D_1)| = |A(D_2)| = |A(D_3)| = 4$ and therefore that each of the three orbits has size $|S_4|/|A(D_1)| = 24/4 = 6$. There are therefore no more than 18 distinct DTS of order 4. This result may also easily be verified computationally via MATHEMATICA. Finally, since the sizes of the stabilisers of the elements in a single orbit are equal, all DTSs of order 4 have automorphism groups of order 4. Therefore, the number of orbits may be determined by Lemma A.2.2 as $\frac{1}{|S_n|}\sum_{D\in\mathcal{D}} A(D) = \frac{1}{24}\cdot 18\cdot 4 = 3$, where $\mathcal{D}$ is the set of all DTS of order 4.

APPENDIX B

A repository of SOLS, SOLSSOMs and MOLS

Contents

The following three sections contain lists of representatives from classes of SOLS, SOLSSOMs and MOLS. Below each SOLS, SOLSSOM or MOLS the size of the corresponding autotransformation group is given, and this value may be used together with the expressions in §5.2.2 and §5.3.3 in order to determine the size of various other equivalence classes (as discussed in Chapter 5) of which the corresponding SOLS, SOLSSOM or MOLS is a member.

B.1 RC-paratopism class representatives of SOLS

$n = 4$	$n = 5$	$n = 7$				$n = 8$			
0231	02143	0214365	0214365	0214563	0234561	02145673	02145673	02345671	02345671
3102	31402	3160542	3160524	3105624	6105243	31670245	31702456	31460752	41607352
1320	43210	4526013	4526031	4621035	1420635	43257016	46257301	65207413	53270146
2013	24031	5643201	5643102	6053241	2653014	20736154	57630124	74136205	67431025
24	10324	6351420	6352410	2536410	3516402	65314702	75364210	27654130	76154203
	20	1032654	2401653	1460352	4362150	76402531	13076542	13072546	14726530
		2405136	1035246	5342106	5041326	17523460	20413765	50721364	20513764
		42	**6**	**6**	**42**	54061327	64521037	46513027	35062417
						1	**8**	**7**	**56**

$n = 9$

021436587	021436587	021436587	021436587	021436587	021436587	021436587	021436587	021436587	021436587	021436587
318507264	318064725	316078245	316578420	317502864	315874260	310257846	318764250	315784062	310274856	316278405
472061835	472508361	452801763	482167305	482067135	432058716	452803761	472851306	472013856	472068135	452617830
207358146	280357416	260387154	570321864	576328041	578361024	576382014	560382741	587360421	586317240	580362741
180642753	107643852	105742836	605842731	658140723	607142835	763148205	706143825	760148235	758640321	768143052
746185320	764185203	738165402	748605213	764285310	786205143	148675320	187605432	238605714	207185463	204785316
853724601	835721640	874523610	837014652	835714602	843527601	805714632	854027613	854271603	835702614	837051624
635810472	653812074	683254071	154283076	140853276	150683472	284560173	635218074	146852370	164853072	645820173
564273018	546270138	547610328	263750148	203671458	264710358	637021458	243570168	603527148	643521708	173504268
4	**8**	**8**	**2**	**4**	**2**	**1**	**1**	**1**	**1**	**1**

021436587	021436587	021436587	021436587	021436587	021436587	021436587	021436587	021436785	021436785	021436785
318027456	316807425	318607254	318760425	318720465	316820754	316507842	314508762	318654207	310857246	315872046
432810765	582173064	572184036	562178034	562871034	582071463	542873016	562783014	452718036	472068351	432761850
564378012	170384256	180362745	180324756	180364752	178364205	204358761	206357841	285367140	548371062	564380127
750641823	765248310	763548120	705841362	705148326	705148326	785642130	783641250	507142863	687240513	607548231
287165340	208615743	207815463	273685140	237615840	237615840	160785324	140875326	763085412	136725804	178205364
875204631	834751602	845273601	834257601	874253601	840753612	837124605	857214603	874503621	854103627	843057612
603582174	453062871	436051872	456012873	456082173	463582071	658210473	638120475	136820574	263584170	280614573
146753208	647520138	654720318	647503218	643507218	654207138	473061258	475062138	640271358	705612438	756123408
1	**4**	**8**	**4**	**4**	**4**	**4**	**4**	**1**	**1**	**1**
021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785
314867520	317052846	314058267	318264057	315784206	315782406	315784206	315784026	317508462	314687052	317628504
402758361	462587103	402671853	432687510	432051867	432057861	432057861	432057861	462810357	482703516	462187350
560382147	578314062	578324106	574301862	587362041	587361042	587361042	587361240	586372041	540378261	548370162
678041253	603748251	683740521	685740231	608147352	608143257	608142357	608142357	758143206	756140823	785043216
243175806	284605317	237865410	703825146	870625134	846275130	876205134	876205134	134765820	168025437	134865027
837504612	845271630	850217634	857013624	143578620	173508624	143578620	143578602	870254613	837512640	870512643
185623074	136820574	146583072	260158473	264810573	264810573	264810573	264810573	203681574	205861374	653204871
756210438	750163428	765102348	146572308	756203418	750624318	750623418	750623418	645027138	673254108	206751438
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785
316870524	318670254	314602857	316728450	315628407	317254806	316728054	315870246	318267504	316527804	316807542
472058163	532061847	562087314	502863147	572104863	502781364	572804316	572608134	532671840	532870416	542713860
567384201	174308526	157328046	164387502	148367250	185367240	154360827	157364802	160384257	104358267	264380157
758241036	685742310	685741203	675041823	786540321	763148052	785143260	708542361	756148032	785643021	657048321
283605417	867215403	806175432	837105264	237085146	278605413	207685143	263085417	407825316	467085132	708125436
835127640	240857631	478513620	458270631	804753612	854012637	840517632	840157623	845710623	853712640	835271604
140563872	406583172	243860571	283514076	653812074	640823571	638052471	684213570	683052471	648201573	180654273
604712358	753124068	730254168	740652318	460271538	436570128	463271508	436721058	274503168	270164358	473562018
1	**1**	**2**	**1**	**2**	**1**	**1**	**1**	**1**	**1**	**1**
021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785
316758042	316580427	315867024	318604257	315874206	318507264	318627540	314750862	316587024	310824567	314708526
572810463	542678130	542703861	542781036	572168034	502768341	562871304	582017436	532078461	582673140	582167340
247361850	207354861	270384156	286357401	206357841	246310857	605384217	647328510	687354102	765380214	760382451
608143527	670843512	608541237	765048312	783041562	875042136	786142053	876142053	875643210	673541802	638541207
834075216	863715204	867125403	470125863	834605127	184675023	147205836	738605124	740215836	138705426	203875164
183527604	158027643	453078612	807513624	457283610	457283610	834750621	150283647	153802647	847012653	875014632
450682371	485102376	184652370	134862570	168520473	630851472	453068172	205864371	468120573	406258371	146250873
765204138	734261058	736210548	653270148	640712358	763124508	270513468	463571208	204761358	254167038	457623018
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785
315072864	314807526	315627840	316078452	316758402	317864250	310527846	317528046	318674520	314678520	314687520
562784130	562180437	532860417	502814367	572184063	582071463	542813067	562873401	562087314	502163847	502163847
746358201	740351862	740381256	740351826	758310246	764352801	865370124	846310257	857302146	847352016	847350216
653841027	657248013	867143502	857643201	807642531	875240316	673048512	653047812	685143207	758240361	758042361
478205316	836725140	186705324	178265034	463875120	436185027	187265403	178205364	473815062	176085234	186275034
804127653	283074651	258074631	235187640	184023657	208517634	438702651	480751623	204758631	483517602	473518602
180563472	108562374	604258173	684520173	230561874	143608572	254681370	235684170	146520873	265804173	265804173
237610548	475613208	473512068	463702518	645207318	650723148	706154238	704162538	730261458	630721458	630721458
8	**1**	**2**	**1**	**1**	**1**	**6**	**1**	**1**	**2**	**2**
021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785
314768502	310678524	310687524	314257806	316780452	317052864	514680327	518674230	513678240	513872460	513824067
502614837	532761840	532761840	502768341	532067841	562807431	652078413	642158307	642153807	642153807	672153804
857320416	846352017	846350217	876314052	865372014	846320157	786324501	785362014	785312064	765318042	764318520
738542061	758240361	758042361	738641520	708543126	735648012	805743162	837240561	837240516	837240516	837540216
176805243	174085236	184275036	283105467	240815367	480175326	247165830	360715842	370865421	380765124	380765142
483157620	483517602	473518602	450872613	457128603	253781640	173802654	104587623	204781653	204587631	245087631
265083174	265804173	265804173	165083274	183654270	108264573	438251076	253801476	168504372	158604273	158602473
640271358	607123458	607123458	647520138	674201538	674513208	360517248	476023158	456027138	476021358	406271358
2	**4**	**4**	**2**	**1**	**1**	**6**	**1**	**4**	**4**	**4**

021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021436785	021453786
516827034	518674230	518674230	518627430	517823460	518623047	513867420	513687420	513867420	514863027	318064527
642178503	642158307	602158347	672158304	682170534	652170834	642570831	642570831	642570813	682751403	432786105
764381250	785361024	785361024	784361052	764358012	784362510	768314052	786314052	768314052	768324510	285371064
835240167	837240561	837240561	837540261	835641207	835741206	875241306	875241306	875243106	857640132	156247830
380715426	360715842	364715802	360215847	376205841	376805421	386105247	368105247	386105247	370185246	670835241
278053641	204587613	240587613	205784613	208714653	247018653	204758613	204758613	204758631	243078651	847520613
153604872	153802476	153802476	143802576	140582376	160584372	130682574	130862574	130682574	136502874	564108372
407562318	476023158	476023158	456073128	453067128	403257168	457023168	457023168	457021368	405217368	703612458
2	**4**	**2**	**4**	**2**	**2**	**2**	**4**	**4**	**4**	**2**

021453786	021453786	021453786	021453786	021453786	021453786	021453786	021453786	021453786	021453786	021453786
317560842	317268054	315208467	316582407	315820467	318527064	317806425	316507842	314876052	318267054	310286457
452786310	462837501	472681530	472830561	482567103	472168305	452731860	682730451	652784103	672830415	672518304
208374165	576314820	584376021	604378125	640372851	605384127	608314257	168374025	268307415	265371840	268371540
680241537	608742135	650847312	768241350	708246315	750246831	835647012	270148563	130542867	157048362	705642831
873605421	740685312	867135204	187065234	874615032	864735210	780265341	834615207	847165230	846725103	483705162
145827603	853021647	238710645	853704612	153708624	247801653	174528603	507281634	573018624	583104627	857024613
536018274	184506273	106524873	540126873	236184570	583610472	263180574	453826170	486230571	430682571	134860275
764132058	235170468	743062158	235617048	567031248	136072548	546072138	745062318	705621348	704516238	546137028
1	**2**	**1**	**4**	**2**	**1**	**1**	**1**	**1**	**1**	**1**

021453786	021453786	021453786	021453786	021453786	021453786	021453786	021456783	021456783	021456783	021456783
316278540	316287450	314876250	314560827	314562807	310562847	318726540	317268450	316572840	314672850	318627450
602781435	602718534	672180543	682137450	682137450	682137450	652870413	462837105	432168507	482167305	452168307
258367014	258376041	507362814	740386215	740386215	704386215	867304251	576310824	578314062	547308162	547301862
730846152	837642105	153248067	875641032	875641032	875641032	170548362	608742531	687240135	765843021	705843126
847625301	740865312	486715302	168275304	168075324	168075324	786215034	240185367	804735216	803715246	863075241
485130627	584130627	840527631	503728641	503728641	543728601	543182607	835071642	153807624	258034617	280734615
164502873	165024873	268034175	256804173	256804173	256804173	204631875	184503276	265083471	136280574	136280574
573014268	473501268	735601428	437012568	437210568	437210568	435067128	753624018	740621358	670521438	674512038
2	**2**	**2**	**1**	**1**	**2**	**2**	**8**	**1**	**2**	**2**

021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783
318627450	318627450	318627450	318627450	318627450	318627450	317628450	315678420	314708256	314572860	318527460
452168307	452163807	452163807	452863017	452861307	452863107	452863017	432587061	482617305	482167305	452168307
540371862	547308162	540378162	540371862	547308162	540371862	540371862	608324517	608372514	647308152	647301852
705843126	705841326	705841326	705148326	705143826	705148326	805147326	160743852	267540831	765843021	705843126
863705241	860735241	867035241	867035241	863075241	867035241	768035241	874015236	136085427	803715246	863075241
287034615	283074615	283704615	283714605	280734615	283704615	283714605	587231604	875123640	258034617	280734615
136280574	136280574	136280574	136280574	136280574	136280574	136280574	243860175	543861072	136280574	136280574
674512038	674512038	674512038	674502138	674512038	674512038	674502138	756102348	750234168	570621438	574612038
8	**4**	**2**	**1**	**8**	**4**	**2**	**1**	**6**	**4**	**4**

021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783
318527460	318527460	318527460	318527460	318527460	315064827	315678240	317528460	316508427	317860542	318724065
452163807	452163807	452863017	452863107	452863107	482710536	402783561	452863017	472180536	452687130	432687510
647308152	640378152	640371852	647301852	640371852	648327150	658307124	640371852	785321064	704312856	765308124
705841326	705841326	705148326	705148326	705148326	756842301	763842015	805147326	650847312	673548201	807142356
860735241	867035241	867035241	860735241	867035241	873105462	847165302	768035241	264735801	840125367	180265437
283074615	283704615	283714605	283074615	283704615	230578614	284031657	283714605	837214650	238704615	254873601
136280574	136280574	136280574	136280574	136280574	164283075	130524876	136280574	148063275	586231074	643510872
574612038	574612038	574602138	574612038	574612038	507631248	576210438	574602138	503672148	165073428	576031248
4	**4**	**1**	**4**	**4**	**2**	**8**	**2**	**2**	**2**	**2**

021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	021456783	023156784	023156784
317608245	314680257	314687250	316208547	316287450	316208457	316287450	317280546	315867240	317620845	318574206
562830417	572038461	502738461	682731450	602738541	682731540	602873541	642873150	682170534	142768503	432761850
205387164	658307124	658370124	258370124	258370164	258370164	257318064	576301824	867312405	485317026	506328417
756243801	867142305	867142305	867142305	867142305	867142305	863742105	205148367	208543167	670843251	781642035
438175026	743865012	743865012	743865012	743865012	743865012	748065312	468725031	734685012	734085162	870415362
873014652	285713640	285013647	475083621	584013627	574083621	584130627	834517602	543708621	851402637	145087623
684521370	130524876	130524876	130524876	130524876	130524876	130524876	180634275	150234876	268531470	264803571
140762538	406271538	476201538	504617238	475601238	405617238	475601238	753062418	476021358	506274318	657230148
8	**2**	**4**	**2**	**8**	**4**	**16**	**6**	**6**	**8**	**4**

023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784
315687420	315467820	415263807	415263807	415863027	415863027	415863207	415863207	418267305	415863027	415287360
432870156	472683501	582617430	582617430	582617430	582617430	582617430	582617430	542671830	582417306	562718403
607328541	781324065	674308251	604378251	604372851	604372851	604372851	604372851	674308251	647302815	684301257
861743205	157840236	750842316	750842316	730248516	750248316	730248516	750248316	756843012	750648231	750843126
748265013	806735142	806735142	876035142	876035142	876035142	876035142	876035142	830725146	876035142	837465012
580412637	234508617	138074625	138704625	158724603	138724605	158704623	138704625	185034627	231784650	208574631
156034872	568012473	261480573	261480573	261480375	261480573	261480375	261480573	261480573	168520473	146032875
274501368	640271358	347521068	347521068	347501268	347501268	347521068	347521068	307512468	304271568	371620548
16	**8**	**4**	**4**	**2**	**4**	**2**	**4**	**2**	**4**	**8**

023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784	023156784	023416785
415287360	417580263	415863027	415863027	415863207	417683502	416280537	410783562	415263807	415863207	315627840
562718403	532604817	572618430	572618430	572618430	682517430	672018453	652478130	682517430	682517430	562078413
684302517	648372105	604372851	604372851	604372851	508362147	587302146	581307246	574308261	504372861	701384526
750843126	871243056	830247516	850247316	830247516	236740815	760841325	736841025	750842316	750248316	876541032
837065241	786015432	786035142	786035142	786035142	841075263	234765801	874265301	806735142	876035142	480235167
208471635	154837620	158724603	138724605	158704623	375408621	805473612	148032657	138074625	138704625	138752604
146530872	205468371	261480375	261480573	261480375	150824376	158634270	205614873	261480573	261480573	654803271
371624058	360721548	347501268	347501268	347521068	764231058	341527068	367520418	347621058	347621058	247160358
16	**8**	**4**	**12**	**4**	**8**	**4**	**8**	**16**	**8**	**12**

023416785	023416785	023416785	023416785	023416785	023416785	023416785	023456781	023456781	023456781
314760852	417082536	415783026	514683027	514832067	514638027	517823460	315780462	315687402	415863207
572184360	182507463	182604537	652178403	832570416	862753401	832671504	632874105	732061845	582617430
805327146	576321840	504378162	786324510	761328540	781324560	764358012	784312056	681374520	601372854
637548201	651840327	678140253	835740162	675143802	657840312	685140237	206541837	207148356	750248316
481635027	864735201	847265301	247065831	386705124	370185246	340785126	870165324	148235067	876035142
150872634	208173654	251837640	371802654	248057631	248071653	208537641	158237640	854702613	138704625
268051473	340658172	360521874	408251376	150684273	136502874	156204873	541608273	560813274	264180573
746203518	735264018	736052418	160537248	407261358	405267138	471062358	467023518	476520138	347521068
8	**4**	**4**	**72**	**4**	**12**	**144**	**12**	**4**	**144**

B.2 RC-paratopism class representatives of SOLSSOMs

$\boldsymbol{n = 4}$

0231	0123
3102	1032
1320	2301
2013	3210
24	

$\boldsymbol{n = 5}$

02143	04312
31402	41023
43210	30241
24031	12430
10324	23104
20	

$\boldsymbol{n = 7}$

0456123	0231564	0612345	0345612
3160542	2146035	2146530	3164025
1024365	3425601	3025164	4621503
2503614	1653240	4503621	5413260
6215430	5062413	5260413	6052431
4632051	6304152	6431052	1206354
5341206	4510326	1354206	2530146
42		**42**	

$\boldsymbol{n = 8}$

07462315	01234567	07462315	01234567	07462315	01234567	07462315	01234567	07462315	01234567	07462315	01234567
51643270	10472653	51643270	10473652	51643270	14502673	51643270	15402673	51643270	14503672	51643270	15403672
10256734	24051376	10256734	24051376	10256734	25741306	10256734	24761305	10256734	25741306	10256734	24761305
42037651	37506241	42037651	37506241	42037651	30476251	42037651	30675241	42037651	30476251	42037651	30675241
75304126	42160735	75304126	43160725	75304126	42165730	75304126	42156730	75304126	43165720	75304126	43156720
26170543	56327014	26170543	56327014	26170543	56327014	26170543	56327014	26170543	56327014	26170543	56327014
34715062	65743102	34715062	65742103	34715062	67053142	34715062	67043152	34715062	67052143	34715062	67042153
63521407	73615420	63521407	72615430	63521407	73610425	63521407	73510426	63521407	72610435	63521407	72510436
8		**8**		**8**		**4**		**8**		**4**	

07462315	01234567	07462315	01234567	07462315	01234567	07462315	01234567	07462315	01234567	07462315	01234567
51643270	15472603	51643270	15473602	51643270	15402673	51643270	15403672	51643270	15472603	51643270	15473602
10256734	24160375	10256734	24160375	10256734	24751306	10256734	24751306	10256734	24061375	10256734	24061375
42037651	37615240	42037651	37615240	42037651	30576241	42037651	30576241	42037651	37605241	42037651	37605241
75304126	42056731	75304126	43056721	75304126	42165730	75304126	43165720	75304126	42156730	75304126	43156720
26170543	56327014	26170543	56327014	26170543	56327014	26170543	56327014	26170543	56327014	26170543	56327014
34715062	60743152	34715062	60742153	34715062	67043152	34715062	67042153	34715062	60743152	34715062	60742153
63521407	73501426	63521407	72501436	63521407	73610425	63521407	72610435	63521407	73510426	63521407	72510436
8		**8**		**4**		**4**		**4**		**4**	

07462315 01234567	07462315 01234567	06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567
51643270 15472603	51643270 15473602	51463270 10362754	51463270 10372654	51463270 10472653	51463270 10472653
10256734 24051376	10256734 24051376	60257431 23051476	60257431 23051476	60257431 24051376	60257431 24061375
42037651 37506241	42037651 37506241	72036154 36507142	72036154 37506142	72036154 37506142	72036154 37605142
75304126 42165730	75304126 43165720	15304726 42170635	15304726 42160735	15304726 42160735	15304726 42150736
26170543 56327014	26170543 56327014	27640513 57416023	27640513 56417023	27640513 56317024	27640513 56317024
34715062 60743152	34715062 60742153	34175062 65743201	34175062 65743201	34175062 65743201	34175062 65743201
63521407 73610425	63521407 72610435	43521607 74625310	43521607 74625310	43521607 73625410	43521607 73526410
8	**8**	**8**	**8**	**8**	**8**

06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567
51463270 10472653	51463270 10462753	51463270 10472653	51463270 10472653	51463270 10462753	51463270 10472653
60257431 24051376	60257431 24051376	60257431 24051376	60257431 24061375	60257431 24051376	60257431 24051376
72036154 37506241	72036154 36547102	72036154 37546102	72036154 37645102	72036154 36547201	72036154 37546201
15304726 42160735	15304726 42170635	15304726 42160735	15304726 42150736	15304726 42170635	15304726 42160735
27640513 56327014	27640513 57316420	27640513 56317420	27640513 56317420	27640513 57326410	27640513 56327410
34175062 65743102	34175062 65703241	34175062 65703241	34175062 65703241	34175062 65703142	34175062 65703142
43521607 73615420	43521607 73625014	43521607 73625014	43521607 73526014	43521607 73615024	43521607 73615024
56	**8**	**8**	**8**	**8**	**8**

06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567	06712345 01234567
51463270 10472653	51463270 10463752	51463270 10473652	51463270 10473652	51463270 10472653	51463270 10472653
60257431 24061375	60257431 24051376	60257431 24051376	60257431 24061375	60257431 24057316	60257431 24067315
72036154 37645201	72036154 36547201	72036154 37546201	72036154 37645201	72036154 37546201	72036154 37645201
15304726 42150736	15304726 43170625	15304726 43160725	15304726 43150726	15304726 42760135	15304726 42750136
27640513 56327410	27640513 57326410	27640513 56327410	27640513 56327410	27640513 56321470	27640513 56321470
34175062 65703142	34175062 65702143	34175062 65702143	34175062 65702143	34175062 65103742	34175062 65103742
43521607 73516024	43521607 72615034	43521607 72615034	43521607 72516034	43521607 73615024	43521607 73516024
8	**8**	**8**	**8**	**8**	**8**

06712345 01234567	06712345 01234567
51463270 10473652	51463270 10473652
60257431 24057316	60257431 24067315
72036154 37546201	72036154 37645201
15304726 43760125	15304726 43750126
27640513 56321470	27640513 56321470
34175062 65102743	34175062 65102743
43521607 72615034	43521607 72516034
8	**8**

$\boldsymbol{n = 9}$

021436785 086723541	021436785 063287154	021436785 034127856	021436785 064827153	021453786 068574312
315628407 814567230	310678524 614523087	514680327 318076542	513867420 615034287	318064527 617430285
572104863 642078315	532761840 342018765	652078413 482503761	642570813 452108736	432786105 872651430
148367250 750386124	846352017 250371846	786324501 105362487	768314052 801376524	285371064 546312807
786540321 267841053	758240361 821746530	805743162 270648315	875243106 230741865	156247830 735148026
237085146 378615402	174085236 738165402	247165830 763285104	386105247 748615302	670835241 401285763
804753612 523104687	483517602 107854623	173802654 857431620	204758631 127583640	847520613 324807651
653812074 431250876	265804173 586430271	438251076 546810273	130682574 583260471	564108372 183026574
460271538 105432768	607123458 475602318	360517248 621754038	457021368 376452018	703612458 250763148
2	**4**	**6**	**4**	**2**

021453786 046718235	021453786 065824137	021453786 074268135	021456783 076581324	021456783 067128435
316582407 413207856	316287450 614752083	314876250 710432586	317608245 715836402	314687250 618072543
472830561 632154087	602718534 542687301	672180543 402853761	562830417 652704831	502738461 782601354
604378125 721386504	258376041 876301254	507362814 248316057	205387164 587310246	658370124 106354287
768241350 105842763	837642105 258043716	153248067 635147802	756243801 830142567	867142305 270543816
187065234 874625310	740865312 427135860	486715302 823675410	438175026 164025783	743865012 821435760
853704612 280573641	584130627 103278645	840527631 157084623	873014652 348257610	285013647 453287601
540126873 358061472	165024873 380516472	268034175 386501274	684521370 203468175	130524876 345816072
235617048 567430128	473501268 731460528	735601428 561720348	140762538 421673058	476201538 534760128
4	**2**	**2**	**8**	**4**

021456783 064728135	021456783 064728135	021456783 047168235	021456783 063278145	023156784 067438125
316287450 615872043	316287450 615872043	317280546 410853762	315867240 610752834	315687420 618573042
602738541 452601387	602873541 452601387	642873150 702431586	682170534 302567481	432870156 782654301
258370164 786354201	257318064 786354201	576301824 184326057	867312405 275384016	607328541 456301287
867142305 270543816	863742105 270543816	205148367 653247801	208543167 756841203	861743205 375042816
743865012 821435760	748065312 821435760	468725031 831675420	734685012 827415360	748265013 834125760
584013627 103287654	584130627 103287654	834517602 275084613	543708621 184023657	580412637 103287654
130524876 348016572	130524876 348016572	180634275 368502174	150234876 438106572	156034872 240816573
475601238 537160428	475601238 537160428	753062418 526710348	476021358 541630728	274501368 521760438
8	**16**	**6**	**6**	**16**

023156784 058461327	023156784 056874231	023156784 065724831	023416785 064821357	023416785 034127856
415287360 517630482	415863027 518432706	415263807 610437285	315627840 618754032	514683027 318076542
562718403 872154036	572618430 682751043	682517430 502861743	562078413 482503761	652178403 482503761
684302517 461378205	604372851 847316520	574308261 748316502	701384526 875360214	786324510 105362487
750843126 635742810	850247316 735140862	750842316 236148057	876541032 250647183	835740162 270648315
837065241 104825763	786035142 421605387	806735142 471685320	480235167 143075826	247065831 763285104
208471635 340287651	138724605 270583614	138074625 827503614	138752604 307218645	371802654 857431620
146530872 283016574	261480573 304268175	261480573 384052176	654803271 536182470	408251376 546810273
371624058 726503148	347501268 163027458	347621058 153270468	247160358 721436508	160537248 621754038
16	**12**	**16**	**12**	**72**

023416785 034127856	023416785 061278453	023416785 034127856	023456781 078563412	023456781 061237854
514638027 315082764	517823460 610437825	517823460 316078245	315780462 714628305	415863207 610482735
862753401 452601387	832671504 102584736	832671504 462503187	632874105 842716530	582617430 102574386
781324560 106378245	764358012 245306187	764358012 105382764	784312056 567380124	601372854 245308167
657840312 280746531	685140237 738042561	685140237 270846513	206541837 621847053	750248316 387046521
370185246 721865403	340785126 874625310	340785126 783265401	870165324 386075241	876035142 724865013
248071653 873254610	208537641 487153602	208537641 821754630	158237640 435102687	138704625 873150642
136502874 568430172	156204873 523861074	156204873 548610372	541608273 103254876	264180573 538621470
405267138 647513028	471062358 356710248	471062358 657431028	467023518 250431768	347521068 456713208
12	**4**	**144**	**12**	**4**

023456781 056781234
415863207 517430826
582617430 672854013
601372854 748316502
750248316 835142760
876035142 104625387
138704625 280573641
264180573 321068475
347521068 463207158
144

B.3 Main class representatives of k-MOLS

$(n,k)=(3,2)$	$(n,k)=(4,2)$	$(n,k)=(4,3)$	$(n,k)=(5,2)$	$(n,k)=(5,3)$	$(n,k)=(5,4)$
012 012	0123 0123	0123 0123 0123	01234 01234	01234 01234 01234	01234 01234 01234 01234
201 120	1032 2301	1032 2301 3210	20413 13042	20413 13042 42301	20413 13042 42301 34120
120 201	2301 3210	2301 3210 1032	13042 20413	13042 20413 34120	13042 20413 34120 42301
432	3210 1032	3210 1032 2301	42301 34120	42301 34120 13042	42301 34120 13042 20413
	1 152	**5 760**	34120 42301	34120 42301 20413	34120 42301 20413 13042
			800	**2 000**	**12 000**

$(n,k)=(7,2)$

0123456 0123456	0123456 0123456	0123456 0123456	0123456 0123456	0123456 0123456	0123456 0123456	0123456 0123456
1065243 4201365	1056243 4201635	2015634 5601342	6014523 1305642	2041635 1305264	1062543 5204361	4031625 5604213
4201365 1065243	5401632 6015324	1206543 3042615	5601342 2054163	1305264 2041635	3501624 4062513	5604213 6410532
3610524 6534012	4610325 5436012	4560312 6415023	4360215 3546021	4260513 3516042	6340215 3615042	6410532 1352064
6534012 3610524	6532014 2340561	3654021 1530264	3245061 4610235	3516042 4260513	4615032 2436105	1352064 2546301
5342601 2456130	2364501 3652140	6341205 4256130	2536104 5462310	6452301 5634120	2456301 6541230	2546301 3265140
2456130 5342601	3245160 1564203	5432160 2364501	1452630 6231504	5634120 6452301	5234160 1350624	3265140 4031625
6	**6**	**126**	**48**	**2 352**	**24**	**3 528**

$(n,k)=(7,3)$	$(n,k)=(7,4)$	$(n,k)=(7,5)$
0123456 0123456 0123456	0123456 0123456 0123456 0123456	0123456 0123456 0123456 0123456 0123456
2041563 1306245 4250631	2041563 1306245 4250631 3615024	2041563 1306245 4250631 3615024 6534102
1306245 2041563 3615024	1306245 2041563 3615024 4250631	1306245 2041563 3615024 4250631 5462310
4250631 3615024 6534102	4250631 3615024 6534102 5462310	4250631 3615024 6534102 5462310 2041563
3615024 4250631 5462310	3615024 4250631 5462310 6534102	3615024 4250631 5462310 6534102 1306245
6534102 5462310 2041563	6534102 5462310 2041563 1306245	6534102 5462310 2041563 1306245 4250631
5462310 6534102 1306245	5462310 6534102 1306245 2041563	5462310 6534102 1306245 2041563 3615024
1 764	**3 528**	**12 348**

$(n, k) = (7, 6)$

0123456 0123456 0123456 0123456 0123456 0123456
2041563 1306245 4250631 3615024 6534102 5462310
1306245 2041563 3615024 4250631 5462310 6534102
4250631 3615024 6534102 5462310 2041563 1306245
3615024 4250631 5462310 6534102 1306245 2041563
6534102 5462310 2041563 1306245 4250631 3615024
5462310 6534102 1306245 2041563 3615024 4250631
98 784

Since there are 2 165 main classes of 2-MOLS of order 8, representatives of these main classes are not listed here.

$(n, k) = (8, 3)$

01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567
10462735 64015372 46107253 10462735 64015372 42507613 10625473 65071234 42307156 10642375 76053214 34507126
23015476 10326745 57462031 23015476 10326745 67451032 23016745 10325476 54761032 65021734 40512376 13746052
54706123 72650431 65023714 54706123 72650431 26013754 32407651 74160325 17652403 34507126 52370641 25461730
32570614 46107253 23751406 32570614 46107253 53726401 47150326 32407651 23516740 43710652 34601725 67325401
76341052 27563104 12675340 76341052 27563104 15672340 74563012 56742103 60425371 72356041 27165403 40613275
45627301 53471620 30546172 45627301 53471620 30145276 65372104 23516740 76043215 27165403 65427130 56072314
67153240 35742016 74310625 67153240 35742016 74360125 56741230 47653012 35170624 56473210 13746052 72150643
16 **24** **32** **96**

01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567
10327654 23015476 32106745 10327654 23015476 32106745 10327654 23015476 32106745 10426753 63072145 47605312
25041376 40527613 57462031 26071345 50426713 75642031 25041376 40527613 57462031 25043176 10567234 52176043
32106745 56470231 74653102 32105476 47560231 56473102 52406731 36170245 64753120 67301425 72140356 16453270
56470231 32106745 65741320 65740231 32107654 47561320 36170245 52406731 75641302 36570241 25706413 74312605
47562013 74653102 10327654 74652013 65743102 10325476 47562013 74653102 10327654 72615034 46351702 23067451
74653102 65741320 23015476 47563102 74651320 23017654 74653102 65741320 23015476 54167302 37415620 65720134
63715420 17362054 46570213 53416720 16372045 64750213 63715420 17362054 46570213 43752610 54623071 30541726
32 **16** **64** **96**

01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567
30741625 23015476 54602713 70351624 23015476 54602713 60723154 74015326 36402715 10543276 73012654 64105723
56072431 70146352 45320176 56072431 70146352 45320176 43065271 10743652 27510436 76052134 30641275 57326041
14603752 46570213 37061425 15607342 46570213 37061425 74106325 32560741 13025674 34601725 46750132 12573406
43510276 57462031 62157304 43510276 57462031 62157304 27510436 56472013 60347152 42170653 24507316 75462130
27465013 15723604 73516240 27465013 15723604 73516240 56472013 65327104 74651320 25367041 57126403 30741652
75126304 62357140 10743652 34126705 62357140 10743652 15347602 47651230 52176043 63715402 15463720 26057314
62357140 34601725 26475031 62743150 34601725 26475031 32651740 23106475 45763201 57426310 62375041 43610275
128 **64** **192** **32**

01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567
10472653 24051376 37506241 30127645 23015476 12306754 30126754 23015476 12307645 30126754 23015476 12307645
24051376 37506241 42160735 25041376 50427631 47562013 27061345 40526731 75642013 27061345 40526731 75642013
37506241 42160735 56327014 42506713 16370254 75641302 62705413 17360245 56471302 62705413 17360245 56471302
42160735 56327014 65743102 16370254 42506713 64753120 15340276 52407613 47563120 15340276 52407613 47563120
56327014 65743102 73615420 57462031 74653102 30127645 74652031 65743102 30125476 46572031 74653102 23015476
65743102 73615420 10472653 74653102 65741320 23015476 46573102 74651320 23016754 74653102 65741320 30126754
73615420 10472653 24051376 63715420 37162045 56470231 53417620 36172054 64750231 53417620 36172054 64750231
5376 **64** **32** **128**

01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567 01234567
40526713 24051376 12307645 40625173 25071634 12307456 30742156 56023741 64501273 10327654 23015476 32106745
23015476 10326745 57462031 23016745 10325476 54761032 25071634 10746325 43617052 47015236 10472653 74560321
52407631 36170254 74651320 62407351 34160725 47652103 14506372 27350614 35472106 32106745 47560231 65743102
17360254 62705413 35146702 37150426 62407351 73516240 43610725 34501276 72165430 23560471 56327014 47651230
36172045 43517602 60723154 74563012 56742103 60425371 72365041 65172403 20746315 56472013 65743102 10327654
64751302 75643120 23015476 15372604 73516240 26043715 56127403 72465130 17053624 65743102 74651320 23015476
75643120 57462031 46570213 56741230 47653012 35170624 67453210 43617052 56320741 74651320 32106745 56472013
64 **64** **32** **192**

01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567
10327654	74015326	47106235	10327654	23015476	32106745	10327654	23015476	74106325	10327654	47015236	74106325
74015326	10327654	32560741	47015236	10472653	74560321	47015236	10472653	23560471	47015236	10327654	23560471
47106235	32560741	65743102	74106325	32560741	56743012	74106325	32560741	56472013	74106325	23560471	56472013
32560741	56472013	23651470	23560471	56327014	47651230	23560471	56327014	32651740	23560471	56472013	32651740
56472013	65743102	10327654	56472013	65743102	10327654	56472013	65743102	10327654	56472013	65743102	10327654
65743102	23651470	74015326	65743102	74651320	23015476	65743102	74651320	47015236	65743102	32651740	47015236
23651470	47106235	56472013	32651740	47106235	65472103	32651740	47106235	65743102	32651740	74106325	65743102
	256			**128**			**32**			**256**	

01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567
10327654	32015746	23106475	10327654	32015746	47106235	10743652	32015746	47106235	10743652	74015326	23106475
74015326	10472653	47560231	74015326	10472653	32560741	23015476	10472653	32560741	23015476	10327654	47560231
23106475	74560321	56472013	23106475	74560321	56743012	32106745	74560321	56743012	32106745	47560231	56472013
32560741	56327014	74651320	32560741	56327014	23651470	47560231	56327014	23651470	47560231	56472013	74651320
56472013	65743102	10327654	56472013	65743102	10327654	56472013	65743102	10327654	56472013	65743102	10327654
65743102	47651230	32015746	65743102	47651230	74015326	65327104	47651230	74015326	65327104	23651470	32015746
47651230	23106475	65743102	47651230	23106475	65472103	74651320	23106475	65472103	74651320	32106745	65743102
	64			**24**			**64**			**192**	

01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567
10743652	23015476	74106325	10543276	25067134	34601725	10543276	75062314	34601725	10643725	26075413	34701652
32015746	10472653	23560471	26057314	30641275	43710652	26057314	10643725	43710652	26075413	34701652	62157304
47106235	32560741	56472013	34701652	42570316	75362041	34701652	43510276	75362041	34701652	43510276	75326140
74560321	56327014	32651740	43610725	16753042	62475130	43610725	26357041	62475130	43510276	57462031	26075413
56472013	65743102	10327654	62375041	57126403	10543276	62375041	57126403	10543276	57462031	62157304	10643725
65327104	74651320	47015236	75162403	63415720	57026314	75162403	62475130	57026314	62157304	75326140	57462031
23651470	47106235	65743102	57426130	74302651	26157403	57426130	34701652	26157403	75326140	10643725	43510276
	64			**64**			**128**			**3840**	

01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567
40527613	25041376	32106745	50623471	16047235	72401653	30625471	76041235	12407653	40625371	26041735	62407153
23015476	10327654	57462031	63012745	70321654	36745012	23016745	10327654	56743012	23016745	10327654	56743012
12306754	46570213	74653102	12407653	45170326	67352104	12407653	45170326	67352104	62407153	35170426	17352604
56470231	32106745	65741320	47150326	32605471	23516740	47150326	32605471	23516740	37150426	42605371	73516240
37162045	73615402	10327654	34765012	27456103	50123476	54763012	67452103	30125476	54763012	67452103	30125476
75641302	64753120	23015476	25376104	63512740	14067235	65372104	23516740	74061235	15372604	73516240	24061735
64753120	57462031	46570213	76541230	54763012	45670321	76541230	54763012	45670321	76541230	54763012	45670321
	32			**32**			**32**			**64**	

01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567	01234567
20746351	16053724	34501276	10543276	75062314	62301745	10457236	75062314	62301745
65073124	40726351	53617042	26057314	10643725	57462031	26075413	10643725	57462031
34501276	57310642	65472103	34701652	43510276	26075413	34701652	43510276	26075413
46320715	35402176	72165430	43610725	26357041	75143602	57610324	26357041	75143602
73165042	62571403	20746315	62375041	57126403	34657120	62543071	57126403	34657120
52617403	74165230	17053624	75162403	62475130	10726354	43162705	62475130	10726354
17452630	23647015	46320751	57426130	34701652	43510276	75326140	34701652	43510276
	32			**128**			**96**	

$(n, k) = (8, 4)$

01234567	01234567	01234567	01234567
10472653	24051376	37506241	42160735
24051376	37506241	42160735	56327014
37506241	42160735	56327014	65743102
42160735	56327014	65743102	73615420
56327014	65743102	73615420	10472653
65743102	73615420	10472653	24051376
73615420	10472653	24051376	37506241
	8 064		

$(n, k) = (8, 5)$

01234567	01234567	01234567	01234567	01234567
10472653	24051376	37506241	42160735	56327014
24051376	37506241	42160735	56327014	65743102
37506241	42160735	56327014	65743102	73615420
42160735	56327014	65743102	73615420	10472653
56327014	65743102	73615420	10472653	24051376
65743102	73615420	10472653	24051376	37506241
73615420	10472653	24051376	37506241	42160735
		18 816		

$(n,k) = (8,6)$

01234567	01234567	01234567	01234567	01234567	01234567
10472653	24051376	37506241	42160735	56327014	65743102
24051376	37506241	42160735	56327014	65743102	73615420
37506241	42160735	56327014	65743102	73615420	10472653
42160735	56327014	65743102	73615420	10472653	24051376
56327014	65743102	73615420	10472653	24051376	37506241
65743102	73615420	10472653	24051376	37506241	42160735
73615420	10472653	24051376	37506241	42160735	56327014

75 264

$(n,k) = (8,7)$

01234567	01234567	01234567	01234567	01234567	01234567	01234567
10472653	24051376	37506241	42160735	56327014	65743102	73615420
24051376	37506241	42160735	56327014	65743102	73615420	10472653
37506241	42160735	56327014	65743102	73615420	10472653	24051376
42160735	56327014	65743102	73615420	10472653	24051376	37506241
56327014	65743102	73615420	10472653	24051376	37506241	42160735
65743102	73615420	10472653	24051376	37506241	42160735	56327014
73615420	10472653	24051376	37506241	42160735	56327014	65743102

677 376

APPENDIX C

Contents of the accompanying compact disc

In this appendix a brief description of the contents of the compact disc included with this dissertation is given. The compact disc contains computer code of all enumeration algorithms presented in this dissertation, and this code enables the user to reproduce the main results of the dissertation. All code was written using the programming language C, and details on the compilation and usage of the computer code are provided on the compact disc. The compact disc contains the following five directories:

Enumeration of RC-paratopism classes. This directory contains four subdirectories, named "SOLS", "SOLSSOMs (generated from SOLS)", "SOLSSOMs (generate from symmetric Latin squares)" and "Symmetric Latin squares of odd order", which in turn contain computer code for generating RC-paratopism class representatives of SOLS, SOLSSOMs (using two different approaches) and symmetric Latin squares of odd order, respectively.

Enumeration of main classes of MOLS. This directory contains computer code for generating main class representatives of k-MOLS of order n.

Enumeration of other classes. This directory contains two subdirectories, named "SOLS", "SOLSSOMs" and "MOLS", which contain computer code for determining the numbers of various other classes of SOLS and SOLSSOMs, respectively, using the methods presented in §4.5.

SOLSSOMs of order 10. This directory contains computer code of a procedure which tests whether or not SOLS of order 10 satisfy two necessary conditions for admitting common orthogonal mates with their transposes. The procedure establishes the non-existence of SOLSSOMs and 3-MOLS containing SOLS and their transposes.

nauty24r1. This directory contains all the necessary code for version 2.4 of the computer program `nauty`, the latest version available from [96].

Repository. In this directory text files are provided which contain RC-paratopism class representatives of SOLS, SOLSSOMs and symmetric Latin squares.