

MONASH UNIVERSITY

PH.D. THESIS

On the number of Latin rectangles

拉丁方

Douglas S. Stones

Supervised by: Ian Wanless, Graham Farr and Darryn Bryant

A thesis submitted for the degree of Doctor of Philosophy, November 2009.

Abstract	iv
Declaration	v
Acknowledgements	vii
1 Introduction	1
1.1 The problem	1
1.2 Tools of the trade	5
1.2.1 Isotopisms and parastrophy	6
1.2.2 Equivalence	11
1.2.3 Subrectangles and transversals	16
1.2.4 Permanents and bounds	18
1.2.5 The sign of a Latin square	19
1.2.6 Algorithms	23
1.2.7 Software	25
1.3 History of the enumeration of Latin rectangles	26
1.3.1 Formulae for L_n and $L_{k,n}$	26
1.4 Outline	32
2 Divisors of the number of Latin rectangles	35
2.1 Proof template	36
2.2 Factorial divisors	36
2.3 Recurrence congruences	40
2.4 Modulo n	43
2.5 Application to subsets of Latin hypercuboids	46
2.5.1 Introduction	46
2.5.2 Divisors of the number of Latin hypercuboids	53
2.5.3 Latin hypercubes of order four	55
2.6 Application to graph decompositions	57
2.6.1 Introduction	57
2.6.2 One-factorisations	58

2.6.3	Cycle decompositions	60
2.7	On the Alon-Tarsi Conjecture	62
2.7.1	Introduction	62
2.7.2	A modified proof template	62
2.7.3	Congruences for Latin squares	63
3	Orthomorphisms and partial orthomorphisms	67
3.1	Introduction	68
3.1.1	Equivalences	72
3.2	Latin rectangles and partial orthomorphisms	73
3.2.1	A congruence for the number of Latin rectangles	73
3.2.2	Enumeration of partial orthomorphisms	75
3.2.3	A graph theoretic approach	79
3.3	Compound orthomorphisms	85
3.3.1	Evaluating $z_n \pmod{n}$	88
3.3.2	Evaluating $z_n \pmod{3}$	88
3.3.3	Polynomial and compatible orthomorphisms	90
3.3.4	Partial orthomorphism completion	95
3.3.5	Orthogonal compound orthomorphisms	97
4	Autotopisms	99
4.1	How large can an autotopism group be?	100
4.1.1	Divisors of R_n	100
4.2	The maximum number of subsquares of a Latin square	101
4.3	Which isotopisms are autotopisms?	105
4.3.1	The equivalence	105
4.3.2	Autotopisms of Latin squares	106
4.3.3	Simple permutations and contours	109
4.3.4	Automorphisms of Latin squares	112
4.3.5	Autotopisms of small Latin squares	118
5	Future research	119
	Notation	124
	References	125
A	Appendix	143
A.1	Finding the autotopism and autoparatopism groups	143
A.2	The number of even and odd Latin squares	146
A.3	The number of four-line and five-line Latin rectangles	148
A.4	Autotopisms of Latin squares of orders 12, 13 and 14.	151
A.5	Data tables for Section 3.2.3	153
	Index	155

This thesis primarily investigates the number $R_{k,n}$ of reduced $k \times n$ Latin rectangles. Specifically, we find many congruences that involve $R_{k,n}$ with the aim of improving our understanding of $R_{k,n}$.

In general, the problem of finding $R_{k,n}$ is difficult and furthermore, the literature contains many published errors. Modern enumeration algorithms, such as that of McKay and Wanless, require lengthy computations and storage of a large amount of data. Consequently, even into the future, the possibility of obtaining an erroneous result remains, for example, through a hardware or bookkeeping error. In this thesis we find many congruences satisfied by $R_{k,n}$ so that future researchers will be able to check that their purported value of $R_{k,n}$ satisfies these congruences.

We extend the methodology developed in this thesis to encompass the number of certain graph factorisations, the number of orthomorphisms and partial orthomorphisms and the size of certain subsets of Latin hypercuboids. Consequently we find new congruences satisfied by all these numbers. Additionally, we give new sufficient conditions for when a partial orthomorphism admits a completion to an orthomorphism. In a 1997 paper, Drisko suggested some ideas for future research in the study of the Alon-Tarsi Conjecture, which we show to be futile.

We find a new bound on the maximum size of an autotopism group of a Latin square which enables us to find new divisors of $R_{n,n}$ for large n . A similar method gives a bound on the maximum number of $k \times k$ subsquares in a Latin square, for general k . Finally, we find new strong necessary conditions for when an isotopism can be an autotopism of some Latin square.

Keywords: Latin squares, Latin rectangles, Latin cubes, Latin hypercubes, Latin hypercuboids, even Latin squares, odd Latin squares, Alon-Tarsi Conjecture, graph decompositions, orthomorphisms, partial orthomorphisms, compound orthomorphisms, compatible orthomorphisms, polynomial orthomorphisms, isotopisms, isomorphisms, autotopisms, automorphisms, subsquares.

AMS2000 Subject Classification: 05B15, 05A05, 20D60, 20D45

Declaration

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university or other affirms. To the best of my knowledge, this thesis contains no material previously published or written by another person, except where due reference is made in the text. This work was done wholly while in candidature for a research degree at Monash University.

I certify that I have made all reasonable efforts to secure copyright permissions for third-party content included in this thesis and have not knowingly added copyright content to my work without the owner’s permission.

Douglas S. Stones

Under the Copyright Act 1968, this thesis must be used only under the normal conditions of scholarly fair dealing. In particular, no results or conclusions should be extracted from it, nor should it be copied or closely paraphrased in whole or in part without the written consent of the author. Proper written acknowledgement should be made for any assistance obtained from this thesis.

This thesis is largely based upon the following works.

1. D. S. STONES AND I. M. WANLESS, *Divisors of the number of Latin rectangles*, J. Combin. Theory Ser. A, 117 (2010), pp. 204–215.
2. D. S. STONES AND I. M. WANLESS, *A congruence connecting Latin rectangles and partial orthomorphisms*. Submitted.
3. D. S. STONES AND I. M. WANLESS, *Compound orthomorphisms of the cyclic group*. Submitted.
4. D. S. STONES, *The many formulae for the number of Latin rectangles*. In preparation.
5. D. S. STONES AND I. M. WANLESS, *How not to prove the Alon-Tarsi Conjecture*. In preparation.
6. D. S. STONES AND I. M. WANLESS, *Latin squares with many subsquares and large autotopism groups*. In preparation.
7. D. S. STONES, I. M. WANLESS, AND P. VOJTĚCHOVSKÝ, *Autotopisms and automorphisms of Latin squares*. In preparation.

Paper 1 forms the basis of Chapter 2. Paper 5 forms Section 2.7. Papers 2 and 3 form Chapter 3. Chapter 4 is formed from Paper 6 and part of Paper 7. Paper 4 is primarily a survey paper which is relevant to the whole thesis. Papers 4 and 5 are intended to be submitted for the Faculty of Science Postgraduate Publication Award, shortly after submission of this thesis. Also, some components of this thesis are currently not intended to be published outside of this thesis, specifically, Sections 2.5 and 2.6.

Two additional papers, separate from the thesis topic, were also prepared during candidature.

8. S. LIN, G. WANG, D. S. STONES, X. LIU, AND J. LIU, *T-Code: 3-erasure longest lowest-density MDS codes*. IEEE J. Sel. Areas Commun., 28 (2010), pp. 289–296.
9. D. S. STONES, *On prime chains*, Submitted. (2009).

Thanks

I would like to thank many people for their assistance during my Ph.D. candidature. Firstly, great thanks are due to Ian Wanless whose excellent supervision has resulted in a strong passion for combinatorics. I wish Wanless many descendants on the mathematics genealogy tree and encourage futures Ph.D. candidates to seriously consider Wanless as a supervisor.

Additional thanks are due to Graham Farr, who organised our regular research meetings that enabled me to broaden my understanding of combinatorics. I would also like to thank the regular participants of our meetings: Joshua Browning, Daniel Delbourgo, Judith Egan, Graham Farr, Arun Mani, Marsha Minchenko, Kerri Morgan, Kyle Pula, Rebecca Robinson, Ian Wanless, and the many other sporadic participants.

I would also like to thank the following people who have, at some stage during this thesis candidature, provided valuable feedback on my research: Darryn Bryant, Nicholas Cavenagh, Diana Combe, Daniel Delbourgo, Arthur Drisko, Anthony Evans, Graham Farr, Raúl Manuel Falcón Ganfornina, Hans Lausch, Brendan McKay, Chris Mears, Kerri Morgan, Petr Vojtěchovský.

Thanks also go to Darryn Bryant, Graham Farr and Ian Wanless for carefully proofreading this thesis.

Other thanks go to: Helene Barcelo, Richard Brualdi, Rod Canfield, William Chen, Sheng Lin, Jing Liu, Xiaoguang Liu, Gang Wang, Nicholas Wormald, Arthur Yang.

Personal thanks

I would finally like to thank my family and friends, particular my wife Jenny and daughter Gemma, for their support and motivation during my candidature.

1.1 The problem

It is reported [186] that on March 8, 1779, Leonhard Euler [97, 99] introduced a “new kind of magic square” to the St. Petersburg Academy which he called a *quarré latin* or a *Latin square*, that is, a square matrix such that every row and every column contains every symbol exactly once. Although, this cannot be the birthplace of such a simple concept as a Latin square¹, Euler’s work certainly helped spur mathematical interest in Latin squares. Euler’s title suggests he believed that the scientific study of Latin squares was new and in his papers Euler does not make any references to any prior work in the subject.

“It may be surprising that the study of these squares provides an environment rich in important results, in unsolved problems, as well as practical applications. Moreover the results touch on and even influence a variety of mathematical areas both within and outside the general rubric of combinatorics. Such fields include algebra, finite geometries, coding theory, combinatorial design theory, and statistics.”

— LAYWINE AND MULLEN [203]

The name “Latin square” originated from Euler using the Latin alphabet, a, b, c, \dots , to denote symbols in his new kind of magic square. Since Euler, several different symbol sets have been used for Latin squares. In this thesis we will usually use either \mathbb{Z}_n or $[n] = \{1, 2, \dots, n\}$ for the symbol set and we will index the rows and columns of Latin squares by the same set. We also define $\mathbb{N} = \{1, 2, \dots\}$. An $n \times n$ Latin square is called a Latin square of *order* n . Instead of “order” some authors prefer the term “side,” notably [61, 251].

We will study the number L_n of $n \times n$ Latin squares with some fixed symbol set of cardinality n . For instance, if $n = 2$ and the symbol set is \mathbb{Z}_2 , then $L_n = 2$ counting the two Latin

¹For example, Kendall [182] claimed that Dudeney [87] referenced work of Claude Gaspar Bachet, circa 1624, discussing a problem on Latin squares.

squares of order 2

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Most past evaluations of L_n involved, or were related to, Latin rectangles. A *Latin rectangle* is a $k \times n$ array containing exactly n distinct symbols such that each row and each column contains only distinct symbols. A Latin square is therefore a $k \times n$ Latin rectangle with $k = n$. Importantly, the number of symbols in a Latin rectangle is also the number of columns. Therefore if we take a Latin square and “chop off” some rows, we get a Latin rectangle. One of the most important theorems in the study of Latin squares comes from M. Hall Jr [148] (see also [149]), using a result by P. Hall [151].

Theorem 1.1.1. *Any $k \times n$ Latin rectangle can be extended to a Latin square of order n .*

Theorem 1.1.1 implies that every $k \times n$ Latin rectangle can be obtained from some Latin square by “chopping off” the last $n - k$ rows.

For now we will take the symbol set of a Latin rectangle to be \mathbb{Z}_n , while the rows will be indexed by $\{0, 1, \dots, k - 1\} \subseteq \mathbb{Z}_n$. A $k \times n$ Latin rectangle is called *normalised* if the first row is $(0, 1, \dots, n - 1)$, and *reduced* if the first row is $(0, 1, \dots, n - 1)$ and the first column is $(0, 1, \dots, k - 1)^T$. If the symbol set is not \mathbb{Z}_n , but does have a total order on it, then “reduced” and “normalised” can be defined analogously.

The use of the term “reduced” goes back at least to MacMahon [209], and was adopted, for example, by Fisher and Yates [119], Denés and Keedwell [71, 74] and Laywine and Mullen [203]. Euler [97] instead used the term *quarrés réguliers* or “regular square.” Some authors use “normalised” [223], “standardized” [96], “standard” or “in standard form” [251] in place of what we call “reduced.” Similarly, our definition of “normalised” also has some alternative names; for example “standardised” [79], “in the standard form” [27], “semi-normalised” [340] and “reduced” [46, 64, 269], which can be confusing. Some authors avoid this problem by not assigning names to reduced or normalised Latin squares, for example [54, 137, 273, 315].

The number of $k \times n$ normalised Latin rectangles $L = (l_{ij})$ satisfying $l_{00} < l_{10} < \dots < l_{(k-1)0}$ is the number of $k \times n$ Latin rectangles with the first row and column in order. For $k < n$ this is not, in general, the number of reduced $k \times n$ Latin rectangles. In [314] this type of Latin rectangle was called “reduced.” A notion of “very reduced” was considered by Moser [236], which was later generalised to “ $i - j$ reduced” by Mullen [239] and Hamilton and Mullen [152].

A Latin square $L = (l_{ij})$ is called *unipotent* if l_{ii} is independent of $i \in \mathbb{Z}_n$ and *idempotent* if $l_{ii} = i$ for all $i \in \mathbb{Z}_n$. In particular, a reduced unipotent Latin square satisfies $l_{ii} = 0$ for all $i \in \mathbb{Z}_n$.

Let

- $L_{k,n}$ denote the number of $k \times n$ Latin rectangles,
- $K_{k,n}$ denote the number of $k \times n$ normalised Latin rectangles and
- $R_{k,n}$ denote the number of reduced $k \times n$ Latin rectangles.

In the case of Latin squares, the numbers $L_{n,n}$, $K_{n,n}$ and $R_{n,n}$ will be replaced by L_n , K_n and R_n , respectively.

Some values of R_n and $R_{k,n}$ are listed in Figures 1.1 and 1.2, which have been found over many years by numerous authors. We will see that it is easy to find $L_{k,n}$ and $K_{k,n}$ given knowledge of $R_{k,n}$ using (1.1). The enumeration of Latin squares and rectangles is discussed in more detail in Section 1.3. We observe the following commentary.

“One of the major unsolved problems in the theory of Latin squares is the determination of the number L_n of distinct Latin squares of order n .
— BRUALDI AND RYSER [36]

“The determination of R_n (and thus of L_n)... appears to be extremely difficult.
— ALTER [7]

“Not much is known about $L_{k,n}$... for large k, n .
— ATHREYA, PRANESACHAR AND SINGHI [12]

“Suppose that someone wished to write down all Latin squares of order 15. Then... that person would have to inscribe millions of Latin squares on each and every atom in the universe!
— LAYWINE AND MULLEN [203]

This raises the question: what can we say about R_n and $R_{k,n}$? Actually, surprisingly little is known about divisors of R_n and $R_{k,n}$. After inspecting the value of R_n for $n \leq 9$ (see Figure 1.1), Alter [7] was inspired to ask the following three interesting questions concerning the divisibility of R_n .

Question 1.1.2. *Do increasing powers of 2 divide R_n ?*

Question 1.1.3. *What is the highest power of 2 that will divide R_n ?*

Question 1.1.4. *Does 3 divide R_n for all $n \geq 6$?*

These questions remained unanswered for thirty years until McKay and Wanless [225] proved the following theorem.

Theorem 1.1.5. *R_n is divisible by $\lfloor n/2 \rfloor!$ for all $n \geq 1$. If n is odd and $\lfloor n/2 \rfloor + 1$ is composite then $(\lfloor n/2 \rfloor + 1)!$ divides R_n .*

Theorem 1.1.5 answers the first and third of Alter’s questions. In fact, it shows that for all $d \geq 2$ the greatest a such that d^a divides R_n increases at least linearly with n . Alter’s second question remains open. Figure 2.1 on page 39 lists the prime factorisation of $R_{k,n}$ for $2 \leq k < n \leq 11$, which also displays surprisingly many small divisors. While Alter’s questions motivate us to find divisors of R_n (and $R_{k,n}$), it would also be of interest to prove that $R_{k,n}$ is indivisible by a certain number. This leads us to our major goal in this thesis.



Major goal: Find new congruences satisfied by $R_{k,n}$.

Aside from Theorem 1.1.5, we begin our study of congruences for $R_{k,n}$ with an almost clean slate. The only other published congruences for $R_{k,n}$, that the author is aware of, are the recurrence congruences for $R_{3,n}$, given by Riordan [269] and Carlitz [46]. By the end of the thesis, these results will be just the tip of the iceberg.

For general k and n , currently there is no “easy” way of finding $R_{k,n}$. There are plenty of interesting, but impractical, formulae for $R_{k,n}$, as listed in Section 1.3.1. Although, according to Wilf’s [330] classification, finding $R_{k,n}$ is p -solved when k is fixed, that is, there exists an algorithm that returns the value of $R_{k,n}$ in $O(n^{\text{constant}})$ time, for example (1.16). Estimates for R_n were given by McKay and Rogoyski [223], Zhang and Ma [344] and Kuznetsov [200] (see Figure 1.3).

We will now identify an application for the congruences of R_n and $R_{k,n}$ derived in this thesis. McKay, Meynert and Myrvold [222] surveyed the “sorry history” of the enumeration of R_n and related numbers, where they noted numerous published errors (for example [122, 168, 211]). Norton [251] gave an incomplete enumeration of the Latin squares of order 7, having found 16927968 reduced Latin squares of order 7 (the total number is 16942080 [275]). In Figure 3.4 on page 76, amongst other congruences for R_n , we will prove that 5 divides R_7 , but since 5 does not divide 16927968, we can deduce that $R_7 \neq 16927968$ without finding the Latin squares that Norton missed.

“It is the purpose of this paper to present an extensive – possibly an exhaustive – study of 7×7 Latin and higher squares.”

— NORTON [251]

Here, higher squares refers not to Latin squares of order greater than 7, but to Graeco-Latin squares [71, Ch. 5], so Norton indeed acknowledged the possibility that his enumeration was incomplete.

The results of this thesis will similarly provide the future researcher with a congruence² for R_n that can be used to check their results. For instance, the value of R_{12} is currently unknown. In Chapter 3 we find that $R_{12} \equiv 50400 \pmod{55440}$. When a future mathematician claims $R_{12} = x$, for some number x , we can at least check that $x \equiv 50400 \pmod{55440}$. It is unlikely (although not impossible) that an erroneous computation would satisfy this congruence.

²If we have more than one congruence for $R_{k,n}$, they can be combined into a single congruence using the Chinese Remainder Theorem.

“With the increasing use of computers in mathematics, the correctness of such “proofs” is very difficult to determine.”
 — KOLESOVA, LAM AND THIEL [191]

McKay and Wanless [225], who found R_{11} , also listed all of the values of $R_{k,11}$, which were discovered by a similar algorithm. Congruences for $R_{k,n}$ would therefore also be of assistance in checking the validity of an enumeration of R_n .

We will find that $R_{k,n}$ is related to the numbers of several other interesting combinatorial objects. This enables us to find analogous results which will also be included in this thesis. In particular, we will find that the methodology developed in the study of $R_{k,n}$ will be applicable to other enumeration problems in combinatorics.



Goal: Find divisors of the numbers of related combinatorial objects.

Before we dive in, the reader should be aware of the following texts devoted to the study of Latin squares. The first book devoted to Latin squares was by Denés and Keedwell [71] which has a sequel [74]. A book by Laywine and Mullen [203] contains many applications of Latin squares. Much data on Latin squares can be found in the CRC handbook [61]. Bosák [26] also published a book on Latin squares in Slovak.

1.2 Tools of the trade

The three numbers $L_{k,n}$, $K_{k,n}$ and $R_{k,n}$ are related by the following theorem.

Theorem 1.2.1.

$$L_{k,n} = n!K_{k,n} = \frac{n!(n-1)!}{(n-k)!}R_{k,n} \quad (1.1)$$

and in particular

$$L_n = n!K_n = n!(n-1)!R_n. \quad (1.2)$$

Proof. From every $k \times n$ Latin rectangle L , by permuting the columns of L , we can construct $n!$ distinct $k \times n$ Latin rectangles of which exactly one is normalised. Consequently $L_{k,n} = n!K_{k,n}$. Now we wish to show that $K_{k,n} = (n-1)!R_{k,n}/(n-k)!$. Let C be the set of $k \times n$ normalised Latin rectangles and let \mathcal{D} be the set of reduced $k \times n$ Latin rectangles. We want to show that $|\mathcal{D}|(n-1)! = |C|(n-k)!$.

Let G be the group of permutations of \mathbb{Z}_n that fix 0. First, observe that for any $L \in \mathcal{D}$ and any permutation $\alpha \in G$, we can construct a $k \times n$ normalised Latin rectangle by (a) permuting the symbols of L according to α and then (b) permuting the columns of L according to α . For this proof, we will let L_α denote the $k \times n$ normalised Latin rectangle obtained in this way. We formally introduce this concept in Section 1.2.1.

We cannot rule out the possibility that $L_\alpha = L_\beta$ while $\alpha \neq \beta$, so to find a relation between $|C|$ and $|\mathcal{D}|$ we construct a bipartite multigraph H with vertex bipartition

$$\{(M, 1) : M \in C\} \cup \{(L, 2) : L \in \mathcal{D}\}$$

in the following way. For every $L \in \mathcal{D}$ and $\alpha \in G$ we add an edge between $(L_\alpha, 1)$ and $(L, 2)$. Thus there are precisely $|\mathcal{D}|(n-1)!$ edges in H , counting multiedges with their multiplicity.

Now consider the degree of a vertex $(M, 1)$ where $M = (m_{ij}) \in C$. There is an edge between $(M, 1)$ and some $(L, 2)$ for each $\alpha \in G$ such that $\alpha(m_{i0}) = i$ for all $0 \leq i \leq k-1$. Therefore every $(M, 1)$ has degree $(n-k)!$ and so the total number of edges is $|C|(n-k)! = |\mathcal{D}|(n-1)!$. \square

Attention in this thesis will be primarily upon $R_{k,n}$ (and R_n) since any divisibility property of $R_{k,n}$ transfers to the numbers $L_{k,n}$ and $K_{k,n}$ by (1.1). Figure 1.1 lists the known values of R_n along with a list of relevant references. McKay and Wanless [225] listed the values of $R_{k,n}$ for $2 \leq k < n \leq 11$, which we reproduce in Figure 1.2; note that $R_n = R_{n-1,n}$ and $R_{1,n} = 1$ so these values are omitted. It is clear that much research has been put into the enumeration of R_n for many years and some surveys of its history were provided by Denés and Keedwell [71, Sec. 4.3], McKay and Wanless [225] and McKay, Meynert and Myrvold [222]. It is possible that Clausen found R_6 as early as 1842 (see [187] for a discussion). The value of R_{12} is currently unknown, but the estimate $R_{12} \approx 1.62 \cdot 10^{44}$ was given by McKay and Rogoyski [223]. Zhang and Ma [344] and Kuznetsov [200] later gave estimates for R_n , which agree with the estimates in [223]. These estimates are tabulated in Figure 1.3.

n	R_n	Year	References
1	1		
2	1		
3	1		
4	4		
5	56	1782	[54, 97, 211]
6	9408	1890	[119, 122, 168, 278, 280, 310]
7	16942080	1948	[122, 132, 251, 274, 275, 279, 336]
8	535281401856	1967	[11, 191, 240, 326]
9	377597570964258816	1975	[16, 240]
10	7580721483160132811489280	1995	[223]
11	5363937773277371298119673540771840	2005	[225]

FIGURE 1.1: The value of R_n for $1 \leq n \leq 11$.

1.2.1 Isotopisms and parastrophy

Let $\mathcal{I}_n = S_n \times S_n \times S_n$ where S_n is the symmetric group acting on \mathbb{Z}_n . Then \mathcal{I}_n acts on the set of Latin squares $L = (l_{ij})$ in the following way. For each $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ we define $\theta(L)$ to be the Latin square formed by permuting the rows of L according to α , permuting the columns of L according to β and permuting the symbols of L according to γ . In other words, $\theta(L) = (l'_{ij})$ is the Latin square defined by

$$l'_{ij} = \gamma(l_{\alpha^{-1}(i)\beta^{-1}(j)}) \quad (1.3)$$

for all $i, j \in \mathbb{Z}_n$. If L is a $k \times n$ Latin rectangle and α fixes $\{0, 1, \dots, k-1\}$ setwise then $\theta(L)$ is a well-defined $k \times n$ Latin rectangle. The mapping θ is called an *isotopism*. The group of all isotopisms \mathcal{I}_n is called the *isotopism group*. The identity permutation will be denoted ε . Any isotopism other than $(\varepsilon, \varepsilon, \varepsilon)$ is *non-trivial*.

n, k	$R_{k,n}$
3, 2	1
4, 2	3
3	4
5, 2	11
3	46
4	56
6, 2	53
3	1064
4	6552
5	9408
7, 2	309
3	35792
4	1293216
5	11270400
6	16942080
8, 2	2119
3	1673792
4	420909504
5	27206658048
6	335390189568
7	535281401856

n, k	$R_{k,n}$
9, 2	16687
3	103443808
4	207624560256
5	112681643083776
6	12952605404381184
7	224382967916691456
8	377597570964258816
10, 2	148329
3	8154999232
4	147174521059584
5	746988383076286464
6	870735405591003709440
7	177144296983054185922560
8	4292039421591854273003520
9	7580721483160132811489280
11, 2	1468457
3	798030483328
4	143968880078466048
5	7533492323047902093312
6	96299552373292505158778880
7	240123216475173515502173552640
8	86108204357787266780858343751680
9	2905990310033882693113989027594240
10	5363937773277371298119673540771840

FIGURE 1.2: The value of $R_{k,n}$ for $2 \leq k < n \leq 11$ [223, 225].

n	McKay, Rogoyski $R_n \approx$	Zhang, Ma $R_n \approx$	$R_n \approx$	Kuznetsov confidence interval	%err.
12	$1.62 \cdot 10^{44}$	$1.622 \cdot 10^{44}$	$1.612 \cdot 10^{44}$	$(1.596 \cdot 10^{44}, 1.629 \cdot 10^{44})$	1
13	$2.51 \cdot 10^{56}$	$2.514 \cdot 10^{56}$	$2.489 \cdot 10^{56}$	$(2.465 \cdot 10^{56}, 2.515 \cdot 10^{56})$	1
14	$2.33 \cdot 10^{70}$	$2.332 \cdot 10^{70}$	$2.323 \cdot 10^{70}$	$(2.300 \cdot 10^{70}, 2.347 \cdot 10^{70})$	1
15	$1.5 \cdot 10^{86}$	$1.516 \cdot 10^{86}$	$1.516 \cdot 10^{86}$	$(1.499 \cdot 10^{86}, 1.531 \cdot 10^{86})$	1
16		$7.898 \cdot 10^{103}$	$8.081 \cdot 10^{103}$	$(7.920 \cdot 10^{103}, 8.242 \cdot 10^{103})$	2
17		$3.768 \cdot 10^{123}$	$3.717 \cdot 10^{123}$	$(3.642 \cdot 10^{123}, 3.791 \cdot 10^{123})$	2
18		$1.869 \cdot 10^{145}$	$1.828 \cdot 10^{145}$	$(1.773 \cdot 10^{145}, 1.883 \cdot 10^{145})$	3
19		$1.073 \cdot 10^{169}$	$1.103 \cdot 10^{169}$	$(1.059 \cdot 10^{169}, 1.147 \cdot 10^{169})$	4
20		$7.991 \cdot 10^{194}$	$7.647 \cdot 10^{194}$	$(7.264 \cdot 10^{194}, 8.028 \cdot 10^{194})$	5
50		$3.06 \cdot 10^{2123}$			
100		$1.78 \cdot 10^{11396}$			

FIGURE 1.3: Estimates for R_n .

Let L and L' be Latin rectangles. If there exists an isotopism θ such that $\theta(L) = L'$ then L and L' are said to be *isotopic*. The set of all Latin rectangles isotopic to L is called the *isotopy class* of L . If $\theta(L) = L$, then θ is said to be an *autotopism* of L . Hence (1.3) implies that, if $L = (l_{ij})$ and $\theta = (\alpha, \beta, \gamma)$ is an autotopism of L , then

$$\gamma(l_{ij}) = l_{\alpha(i)\beta(j)} \quad (1.4)$$

for all $i, j \in \mathbb{Z}_n$.

If $\theta = (\alpha, \beta, \gamma)$ is an isotopism such that $\alpha = \beta = \gamma$, then θ is said to be an *isomorphism*. The group of all isomorphisms is called the *isomorphism group*. The set of all Latin squares isomorphic to L is called the *isomorphism class* of L . Not all isomorphism classes of Latin squares contain a reduced Latin square, for example, Figure 1.7 gives a representative from each of the 5 isomorphism classes of Latin squares of order 3, while there is only one reduced Latin square of order 3. If θ is an isomorphism and an autotopism of L then θ is said to be an *automorphism* of L . Motivation for studying automorphisms of Latin squares stems from the algebraic theory of quasigroups – that is, the algebraic structure defined when a Latin square is viewed as a multiplication table. We introduce quasigroups in Section 1.2.2.

Given a Latin square $L = (l_{ij})$ of order n we can construct a set of n^2 ordered triplets

$$O = \{(i, j, l_{ij}) : i, j \in \mathbb{Z}_n\}$$

called the *orthogonal array* of L . Conversely, any set O of n^2 triplets $(i, j, l_{ij}) \in \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$, such that distinct triplets differ in at least two coordinates, gives rise to a Latin square $L = (l_{ij})$. Any element of the orthogonal array O of L is called an *entry* of L . There are six, not necessarily distinct, Latin squares that can be constructed from L by uniformly permuting the coordinates of each entry in O and each is called a *parastrophe* of L . We use $\lambda \in \{\varepsilon, (rc), (rs), (cs), (rcs), (rsc)\}$ to permute the coordinates of each entry in O , where r, c and s correspond to the first, second and third coordinates, respectively. We use L^λ to denote the parastrophe of L induced by λ . For example, $L^{(rc)}$ is the matrix transpose of L . We use L^λ to denote the λ -parastrophe of L and call $\{\varepsilon, (rc), (rs), (cs), (rcs), (rsc)\}$ under composition

the *parastrophy group*. For $k \times n$ Latin rectangles L with $k < n$, we can similarly construct a set of kn entries O from L . However, it is only sensible to consider the (cs) -parastrophe of L .

Typically, “conjugate” is used in place of “parastrophe” [71]. In this thesis we are unable to use the term “conjugate,” due to likely confusion with the well-established notion of conjugation in group theory. In Section 4.3 we will see that group-theoretic conjugation plays an important role in the study of autotopisms. Norton [251], for example, used the term “adjugate,” but this terminology is rarely adopted in modern times. The term “adjugate” also has a use in linear algebra.

The *main class* of L is the set of all Latin squares that are isotopic to some parastrophe of L . If L and L' are within the same main class, then they are said to be *paratopic*. A map that combines both isotopism and parastrophy is called a *paratopism*. The group of all paratopisms is called the *paratopism group*. If τ is a paratopism such that $\tau(L) = L$ then τ is said to be an *autoparatopism* of L .

In this thesis we define a *symmetric* Latin square L as one that satisfies $L = L^{(rc)}$, that is, L is its own matrix transpose. A *totally symmetric* Latin square L satisfies $L = L^{(rc)} = L^{(rs)} = L^{(cs)} = L^{(rcs)} = L^{(rsc)}$. Some authors define a “symmetry” to be any non-trivial autoparatopism, for example [225].

Several other subgroups of the paratopism group are of importance. For instance, McKay, Meynert and Myrvold [222] considered the *type* of L , which is the set of all Latin squares that are either isotopic to L or isotopic to $L^{(rc)}$. We will call the group combining isotopism with (rc) -parastrophy the *type group*. Another example are isotopisms of the form $\theta = (\alpha, \beta, \varepsilon)$, which are called *principal isotopisms*. Principal isotopisms have been studied, for example, by Ganfornina [126].

Let L be a Latin square. We make the following definitions.

- The group of all automorphisms of L is called the *automorphism group* of L , denoted $\text{Aut}(L)$.
- The group of all autotopisms of L is called the *autotopism group* of L , denoted $\text{Atop}(L)$.
- The group of all autoparatopisms of L is called the *autoparatopism group* of L , denoted $\text{Apar}(L)$.

We depict some of the subgroup structure of the paratopism group in Figure 1.4, with arrows denoting subgroups. The first row of groups vary only with n , the second row of groups vary with the Latin square L (which is of order n) and the third row of groups are independent of both L and n .

McKay, Meynert and Myrvold [222] gave a construction from L of three graphs, G_1 , G_2 and G_3 , with automorphism groups that are isomorphic to $\text{Apar}(L)$, $\text{Atop}(L)$ and $\text{Aut}(L)$, respectively. We write GAP [127] code that constructs G_1 and G_2 for use with GRAPE [295] and nauty [220] in Appendix A.1. The LOOPS [242, 243] package for GAP implements a completely different algorithm for finding the automorphism group of a Latin square. Actually, LOOPS is a package designed for the study of quasigroups (see Section 1.2.2).

For orders $1 \leq n \leq 10$, the number of (a) main classes, (b) types, (c) isotopy classes, (d) isomorphism classes and (e) isomorphism classes containing a reduced Latin square was given by McKay, Meynert and Myrvold [222], who acknowledged several earlier enumerations. Hulpke, Kaski and Östergård [164] reported these numbers for order 11. These values

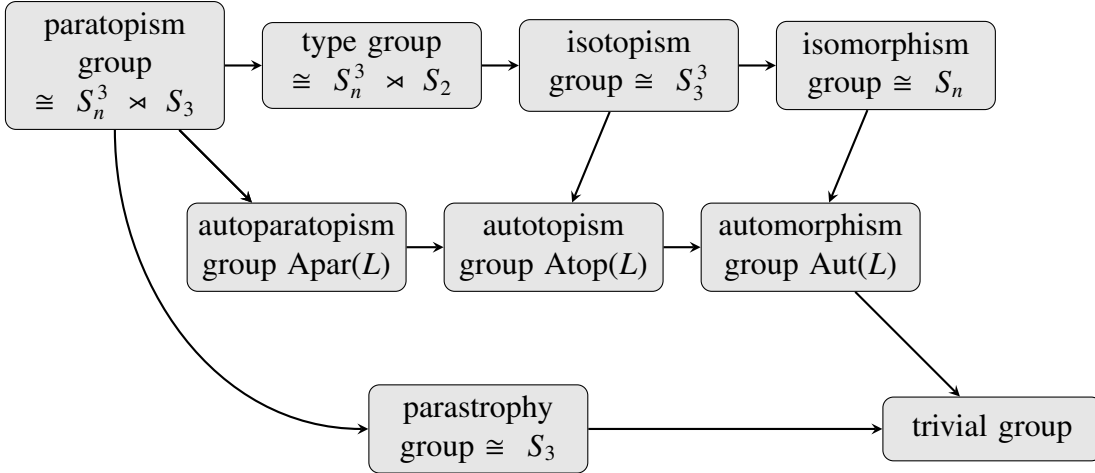


FIGURE 1.4: Some important subgroups of the paratopism group, where L is a Latin square of order n .

are listed in Figures 1.5 and 1.6, along with lists of relevant references. None of these numbers alone provide sufficient information to find L_n .

n	Main classes	Types	Isotopy classes
1	1	1	1
2	1	1	1
3	1	1	1
4	2	2	2
5	2	2	2
6	12	17	22
7	147	324	564
8	283657	842227	1676267
9	19270853541	57810418543	115618721533
10	34817397894749939	104452188344901572	208904371354363006
11	2036029552582883134196099	6108088657705958932053657	12216177315369229261482540
References: [11, 33, 34, 119, 164, 191, 222, 251, 265, 274, 278, 280, 326]			

FIGURE 1.5: The number of main classes, types and isotopy classes of Latin squares of order n .

The following theorem, by McKay and Wanless [225], implies that asymptotically almost all Latin squares of order n have a trivial autoparatopism group. Additionally, Theorem 1.2.2 implies that the number of isomorphism classes, isotopy classes and main classes of Latin squares of order n are asymptotic to $L_n/n!$, $L_n/n!^3$ and $L_n/(6n!^3)$, respectively.

Theorem 1.2.2. *The proportion of Latin squares of order n which have a non-trivial autoparatopism group is no more than*

$$n^{-3n^2/8+o(n^2)}.$$

Wanless and Ihrig [325] and Ihrig and Ihrig [165] studied when a Latin square is isotopic to a symmetric Latin square.

1.2.2 Equivalence

Quasigroups

A *quasigroup* (Q, \oplus) of order n is a set Q of cardinality n together with a binary operation \oplus , such that for all $g, h \in Q$, the equations $x \oplus g = h$ and $g \oplus y = h$ have unique solutions with $x, y \in Q$. If (Q, \oplus) possesses an identity element e , that is e satisfies $e \oplus g = g = g \oplus e$ for all $g \in Q$, then Q is called a *loop*.

If (Q, \oplus) is a quasigroup and \triangleleft is a total order on Q , then we call $(Q, \oplus, \triangleleft)$ an *ordered quasigroup*. The *Cayley table* of an ordered quasigroup $(Q, \oplus, \triangleleft)$ is the matrix $L = (l_{ij})$ such that $l_{ij} = i \oplus j$, where the rows and columns of L are indexed by Q in the order defined by \triangleleft . In fact, L must be a Latin square and moreover, Latin squares are precisely the Cayley tables of ordered quasigroups on a set Q with a total order \triangleleft . Hence L_n is the number of ordered quasigroups on a set Q of cardinality n with total order \triangleleft . If $(Q, \oplus, \triangleleft)$ is an ordered loop such that the identity e is the minimum under \triangleleft , then its Cayley table is a reduced Latin square. Hence R_n is the number of ordered loops on a set Q of cardinality n with identity $e \in Q$ and total order \triangleleft with minimum e .

If we do not assume that Q possesses a predefined ordering, we call (Q, \oplus) an *unordered quasigroup*, for emphasis. We define a Cayley table of an unordered quasigroup (Q, \oplus) to be the Cayley table of $(Q, \oplus, \triangleleft)$ for any total order \triangleleft on Q . Therefore, while an ordered quasigroup possesses a unique Cayley table, an unordered quasigroup may possess many.

For any permutation α of Q , we may define a quasigroup (Q, \star) by $\alpha(i) \star \alpha(j) = \alpha(i \oplus j)$ for all $i, j \in Q$. We say that (Q, \star) is *isomorphic* to (Q, \oplus) and call the set of quasigroups isomorphic to (Q, \oplus) the *isomorphism class* of (Q, \oplus) . Let \triangleleft be any total order on Q . Let L and L' be the unique Cayley tables of the ordered quasigroups $(Q, \oplus, \triangleleft)$ and $(Q, \star, \triangleleft)$, respectively. Then $\theta(L) = L'$ where $\theta = (\alpha, \alpha, \alpha)$ by (1.3), that is, L is isomorphic to L' . It follows that an isomorphism class of Latin squares is precisely the set of Cayley tables of an unordered quasigroup. In fact, the definition of isomorphism amongst Latin squares stems from isomorphism amongst quasigroups.

The number of isomorphism classes of quasigroups is the number of isomorphism classes of Latin squares of order n . Theorem 1.2.2 implies that the number of isomorphism classes of quasigroups is asymptotic to $L_n/n! = K_n$. In each isomorphism class of quasigroups there (a) might not be a loop, (b) might be one loop or (c) might be more than one loop. The number of isomorphism classes of Latin squares that contain a reduced Latin square is the number of isomorphism classes of quasigroups that contain a loop (the number of isomorphism classes of loops). These numbers are listed for $n \leq 11$ in Figure 1.6 sourced from [164, 222], along with a list of relevant references.

In Figure 1.7 we reproduce the list, given by Bailey and Cameron [15], of isomorphism class representatives of Latin squares of order 3. These Latin squares are not isomorphic, but they are isotopic. In fact, there is only one isotopy class of Latin squares of order 3.

Some particularly active research areas in the theory of quasigroups involve so-called Moufang loops [238] and Bol loops [25].

Graphs

In this section we identify some graph-theoretic objects that are equivalent to Latin squares (see also [71, Sec. 9.1] and [203, Ch. 7]).

n	Loops	Quasigroups
1	1	1
2	1	1
3	1	5
4	2	35
5	6	1411
6	109	1130531
7	23746	12198455835
8	106228849	2697818331680661
9	9365022303540	15224734061438247321497
10	20890436195945769617	2750892211809150446995735533513
11	1478157455158044452849321016	19464657391668924966791023043937578299025
References: [2, 29, 39, 71, 164, 222, 276, 280], Bower, Guérin and “QSCGZ” [222]		

FIGURE 1.6: The number of isomorphism classes of loops of order n and the number of isomorphism classes of quasigroups of order n , for $1 \leq n \leq 11$.

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

FIGURE 1.7: A Latin square from each isomorphism class of order 3.

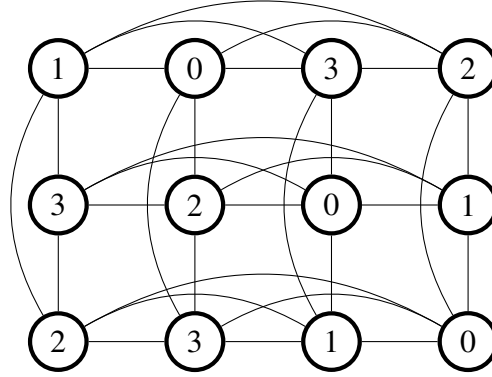
Rook's graph Let $G = G_{k,n}$ be the graph with vertex set $\{(i, j) : 0 \leq i \leq k-1 \text{ and } 0 \leq j \leq n-1\}$ and edges between distinct (i, j) and (i', j') whenever $i = i'$ or $j = j'$. We will call G a *rook's graph* since edges represent legal moves by a rook on a $k \times n$ chess board. There are other names for G , for example G is (a) the line graph of the complete bipartite graph and (b) the graph Cartesian product of the complete graphs on k and n vertices. As usual we assume $k \leq n$.

A $k \times n$ Latin rectangle $L = (l_{ij})$ corresponds to a proper vertex-colouring of G with colour set \mathbb{Z}_n , with vertex (i, j) receiving colour l_{ij} . This observation was made by Athreya, Pranesachar and Singhi [12]. Figure 1.8 is $G_{3,4}$ with an example of a proper vertex-colouring from the colour set \mathbb{Z}_4 . Hence $L_{k,n}$ is the number of proper vertex-colourings of G with colour set \mathbb{Z}_n . Equivalently, $L_{k,n}$ is the chromatic polynomial $P(G, x)$ evaluated at $x = n$, the chromatic number of G . In Figure 1.9 we list $P(G, x)$ for some small values of k and n that were computed by Kerri Morgan (private communication).

The number of $k \times n$ matrices with at most x distinct symbols in total and without repeated symbols in each row and column, is enumerated by $P(G, x)$. The enumeration of this type of generalised Latin rectangle was also considered by Light Jr [207] and Nechvatal [245]. We discuss generalisations of Latin squares in Section 2.5.

Latin square graphs Let $L = (l_{ij})$ be a Latin square of order n . Let $H = H(L)$ be the graph with vertex set $\{(i, j) : i, j \in \mathbb{Z}_n\}$ and an edge between distinct (i, j) and (i', j') whenever $i = i'$ or $j = j'$ or $l_{ij} = l_{i'j'}$. The graph H is called a *Latin square graph* of order n .

We say a graph G is (v, a, b, c) -strongly regular if (a) G has v vertices, (b) every vertex has

FIGURE 1.8: The graph $G_{3,4}$ with a proper vertex-colouring from the colour set \mathbb{Z}_4 .

k	n	$P(G_{k,n}, x)$
2	2	$x(x-1)(x^2-3x+3)$
2	3	$x(x-1)(x-2)(x^3-6x^2+14x-13)$
2	4	$x(x-1)(x-2)(x-3)(x^4-10x^3+41x^2-84x+73)$
2	5	$x(x-1)(x-2)(x-3)(x-4)(x^5-15x^4+95x^3-325x^2+609x-501)$
3	3	$x(x-1)(x-2)(x^6-15x^5+100x^4-381x^3+877x^2-1152x+688)$
3	4	$x(x-1)(x-2)(x-3)(x^8-24x^7+264x^6-1746x^5+7620x^4-22512x^3+43939x^2-51630x+27808)$
3	5	$x(x-1)(x-2)(x-3)(x-4)(x^{10}-35x^9+570x^8-5710x^7+39098x^6-191728x^5+683055x^4-1746375x^3+3063456x^2-3321652x+1684912)$
4	4	$x(x-1)(x-2)(x-3)(x^{12}-42x^{11}+833x^{10}-10338x^9+89589x^8-572046x^7+2762671x^6-10172046x^5+28328427x^4-58124022x^3+83236871x^2-74505978x+31430160)$

FIGURE 1.9: $P(G_{k,n}, x)$ for some small values of k and n .

a neighbours, (c) every pair of adjacent vertices has b common neighbours and (d) every pair of non-adjacent vertices has c common neighbours. A Latin square graph is $(n^2, 3(n-1), n, 6)$ -strongly regular. The following theorem was attributed to Bruck [38] (see also [37]) by Bailey and Cameron [15, Pro. 3].

Theorem 1.2.3. *If $n \geq 24$ then any $(n^2, 3(n-1), n, 6)$ -strongly regular graph is a Latin square graph. Furthermore, if (a) L is a Latin square of order $n \geq 5$, (b) H is the Latin square graph of L and (c) H' is a graph isomorphic to H , then H' is the Latin square graph of a Latin square L' paratopic to L .*

It follows that, for $n \geq 24$, the number of isomorphism classes of $(n^2, 3(n-1), n, 6)$ -strongly regular graphs is the number of main classes of Latin squares of order n . The automorphisms of Latin square graphs were studied by Phelps [259, 260].

Proper edge-colourings of the complete bipartite graph Let G be the complete bipartite graph with vertex bipartition $\{u_0, u_1, \dots, u_{n-1}\} \cup \{w_0, w_1, \dots, w_{n-1}\}$. Let C be a proper edge-colouring of G with edge colour set \mathbb{Z}_n . The edges of colour s define a permutation of \mathbb{Z}_n by $i \mapsto j$ whenever u_i is adjacent to w_j by an edge of colour s . So we can construct a Latin

square $L = L(C) = (l_{ij})$ from C with $l_{ij} = s$ whenever u_i is adjacent to w_j by an edge of colour s . Hence L_n is the number of proper edge-colourings of G with edge colour set \mathbb{Z}_n .

The group $\text{Aut}(G) \times S_n$ acts on the set of proper edge-colourings of G ; with $(\tau, \gamma) \in \text{Aut}(G) \times S_n$ permuting the vertices of G according to τ and the edge colours according to γ . In fact, $\text{Aut}(G) \times S_n$ is isomorphic to the type group (see Section 1.2.1). Let C be an arbitrary edge-colouring of G . The orbit of C under $\text{Aut}(G) \times S_n$ corresponds to the type of $L(C)$. Therefore the number of non-isomorphic edge-colourings of G is the number of types of Latin squares of order n .

A *one-factor* of a graph (in this case G) is a 1-regular spanning subgraph. A *decomposition* of G is a set of subgraphs of G whose edge sets partition the edge set of G . In particular, a *one-factorisation* of G is a decomposition of G into a set of one-factors. Given a one-factorisation of G , we can construct $n!$ proper edge-colourings by assigning a distinct colour of \mathbb{Z}_n to each one-factor and then colouring each edge in G according to the colour of one-factor to which it belongs. Consequently, K_n is the number of one-factorisations of G . The number of non-isomorphic one-factorisations of G is the number of types of Latin squares of order n .

Figure 1.10 depicts a one-factorisation of the complete bipartite graph on 10 vertices. The first column of vertices is u_0, u_1, \dots, u_{n-1} and the second is w_0, w_1, \dots, w_{n-1} , with both in descending order. To illustrate the correspondence with Latin squares, the vertices u_i are marked j whenever u_i is adjacent to w_j . Note that Figure 1.10 identifies the Latin square defined by $l_{is} = j$, that is, $L(C)^{(cs)}$.

Denés and Keedwell [72, 73] and Laywine and Mullen [203] discussed one-factorisations of the complete bipartite graph (see also [71] and [74]). Wanless and Ihrig [325] studied the Latin squares formed from a certain construction of one-factorisations of G .

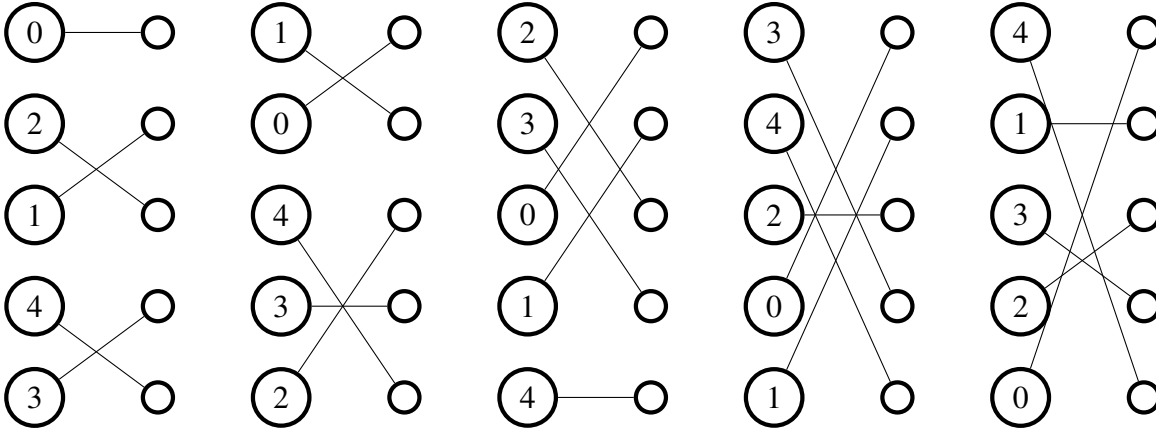


FIGURE 1.10: A one-factorisation of the complete bipartite graph on 10 vertices.

One-factorisations of the complete directed graph A set S of permutations of \mathbb{Z}_n is called *sharply transitive* if for all $i, s \in \mathbb{Z}_n$ there is a unique $\sigma \in S$ such that $\sigma(i) = s$. It follows that $|S| = n$. We define $\sigma_j \in S$ to be the permutation that maps 0 to j . We can construct a normalised Latin square $L = (l_{ij})$ of order n from S by assigning $l_{ij} = \sigma_j(i)$. Moreover, if $\varepsilon \in S$ then L is a reduced Latin square. Hence K_n is the number of sharply transitive sets of \mathbb{Z}_n and R_n is the number of sharply transitive sets S of \mathbb{Z}_n with $\varepsilon \in S$.

A *one-factorisation* of a directed graph G is a decomposition of G into subgraphs in which every vertex has in-degree and out-degree 1.

Let G be the loop-free complete directed graph on the vertex set \mathbb{Z}_n . Assume that $\varepsilon \in S$. Each non-trivial $\sigma \in S$ is equivalent to the subgraph of G with an edge from each $i \in \mathbb{Z}_n$ to $\sigma(i)$. Together, the non-trivial $\sigma \in S$ yield a one-factorisation of G . Conversely, given a one-factorisation of G we may reverse this process to construct a sharply transitive set of permutations $S = \{\sigma_j\}_{j \in \mathbb{Z}_n}$ with $\sigma_0 = \varepsilon$. Hence R_n is the number of one-factorisations of G . This equivalence was noticed in [203, pp. 112–113].

Let G' be the complete directed graph on n vertices, with a single loop on each vertex. A one-factorisation of G' corresponds to a sharply transitive set $S = \{\sigma_j\}_{j \in \mathbb{Z}_n}$, but this time we do not necessarily have $\sigma_0 = \varepsilon$. Consequently, K_n is the number of one-factorisations of G' . This equivalence was also noticed in [203, pp. 111–112].

Triangle decompositions of the complete tripartite graph Let G be the complete tripartite graph with vertex partition $R \cup C \cup S$ with $|R| = |C| = |S| = n$. We will consider a triangle of G to be any triplet in $R \times C \times S$. The orthogonal array of L therefore defines a decomposition of G into triangles. Hence L_n is the number of decompositions of G into triangles. Figure 1.11 gives an example of a triangulation of the complete tripartite graph on 6 vertices; identically labelled vertices are identified.

Colbourn [60] used the problem of decomposing a tripartite graph into triangles to show that the problem of partial Latin square completion is NP-complete.

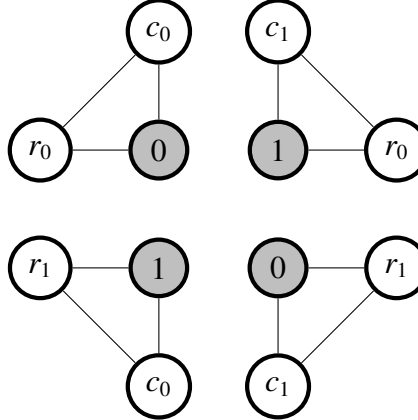


FIGURE 1.11: A triangulation of the complete tripartite graph on 6 vertices.

Miscellany

3-nets and transversal designs A *3-net* [15, 71, 157, 175] is an incidence structure with n^2 points and $3n$ lines such that (a) each line contains n points and each point lies on 3 lines, (b) each pair of points lie on at most one line and (c) the lines can be partitioned into 3 families of n lines, each of which is a partition of the set of points, with each pair of lines from distinct families intersecting at a unique point. A Latin square L forms a 3-net with its orthogonal array as the set of points and lines corresponding to the rows, columns and symbols of L . Condition (c) implies that L can be recovered from the 3-net [15].

A *transversal design* is the dual of a 3-net. It has $3n$ points and n^2 lines such that (a) each line contains 3 points and each point lies on n lines, (b) each pair of points lie on at most one line and (c) the points can be partitioned into 3 families of n points, with each pair of points from different families lying on a unique line and each line containing one point from each family.

Isomorphism amongst 3-nets and transversal designs corresponds to paratopism of Latin squares. Therefore, the number of non-isomorphic 3-nets is the number of non-isomorphic transversal designs, and is also the number of main classes of Latin squares.

Error-detecting codes We can write the orthogonal array of a Latin square $L = (l_{ij})$ as an $n^2 \times 3$ array with each row equal to (i, j, l_{ij}) for some $i, j \in \mathbb{Z}_n$. It has the property that any pair of distinct rows differs by at least two entries. Such an array is called a *1-error-detecting code* [71, p. 354]. The rows are referred to as *codewords*, the symbol set is called the *alphabet* and the *word length* is 3, the number of columns. It is straightforward to construct an orthogonal array of a Latin square from a 1-error-detecting code with these parameters. Hence L_n is the number of 1-error-detecting codes with n^2 codewords of word length 3 and alphabet of size n .

Permutation cubes Let L be a Latin square. Then L corresponds to the $n \times n \times n$ $(0, 1)$ -array $M = (m_{ijk})$ with $m_{ijk} = 1$ whenever $l_{ij} = k$. Equivalently M indicates the position of n^2 mutually non-attacking rooks on an $n \times n \times n$ chess board. Hence L_n is the number of such arrays M and the number of arrangements of n^2 mutually non-attacking rooks on an $n \times n \times n$ chess board.

1.2.3 Subrectangles and transversals

We will now discuss two useful objects that occur within some Latin squares – subsquares and transversals. We will generally deal with both objects from a functional perspective, that is, as a catalyst in the study of enumeration problems relating to Latin squares and rectangles. However, in Section 4.2 we will find new bounds on the maximum number of subsquares in a Latin square and some results in Chapter 3 will be applicable to transversals of the Cayley table of \mathbb{Z}_n . There remain some interesting open problems in the study of both subsquares and transversals and the interested reader should consult [74, Ch. 4] and [324], respectively.

Let L be an arbitrary Latin rectangle. If a submatrix M of L is also a Latin rectangle then M is called a *subrectangle* of L , and if M is a Latin square then M is called a *subsquare* of L . So a subrectangle is a Latin rectangle contained within a Latin rectangle and is different to an arbitrary rectangular submatrix, which might not be a Latin rectangle. We stress that subrectangles and subsquares do not need to consist of contiguous rows and columns. We will not consider M to be a subrectangle if it consists of more rows than columns.

Every Latin square of order n contains (a) a subsquare of order 0, (b) n^2 subsquares of order 1 and (c) one subsquare of order n . A subsquare of order 2 is called an *intercalate* and is the smallest non-trivial subsquare. The term “intercalate” is usually traced back to Norton [251]. Most Latin squares have many intercalates [224].

Subsquares M of $k \times n$ Latin rectangles have the handy property that they can be replaced by another subsquare of the same order and with the same symbol set to give another $k \times n$

Latin rectangle. This switch yields a distinct $k \times n$ Latin rectangle when the order of M is at least 2. Subsquares are a simple example of a class of switches, called Latin trades, that are possible within Latin squares [48].

We now list some more properties of subsquares. Lemmata 1.2.4 and 1.2.5 are well-known and straightforward to prove. Lemma 1.2.7 arose in the proof of [222, Thm 1] and Lemma 1.2.8 is a straightforward consequence of Lemma 1.2.7.

Lemma 1.2.4. *Let M be a subsquare of order m of a $k \times n$ Latin rectangle L . Then $m \leq \lfloor n/2 \rfloor$ or M is L itself.*

Proof. Let M' denote the $m \times (n - m)$ subrectangle of L formed by the rows of L in M and columns of L outside of M . For M' to exist we require $n - m \geq m$ or $n - m = 0$. \square

If M is a subsquare in a Latin square L of order n , then M is called a *proper* subsquare if the order of M is not 0, 1 or n . By Lemma 1.2.4 this requires the order of M to be between 2 and $\lfloor n/2 \rfloor$ inclusive. Latin squares without proper subsquares exist for many orders [214].

Lemma 1.2.5. *Suppose M and M' are both subsquares of a Latin square L . Then the intersection of M and M' is also a subsquare of L .*

Proof. Let M^* denote the submatrix formed by the intersection of M and M' . Assume that M^* is non-empty and $M^* \neq L$, otherwise the lemma is trivial.

Let x be an arbitrary symbol in M^* . Then x occurs in each row of both subsquares M and M' . However, x occurs exactly once in every row of L . Therefore every row in M^* contains x . Since x is arbitrary, every symbol in M^* occurs in every row of M^* . That x is in every column of M^* follows similarly. \square

Lemma 1.2.6. *Let E be a set of entries of a Latin square L . There exists a unique smallest subsquare M_E of L such that every entry in E is in M_E .*

Proof. Follows from Lemma 1.2.5. \square

Lemma 1.2.7. *Let $L = (l_{ij})$ be a $k \times n$ Latin rectangle and let $\theta = (\alpha, \beta, \gamma)$ be an autotopism of L . Let i index a row of L and let j index a column of L . Any two of following statements implies the other:*

1. *row i is fixed by α ,*
2. *column j is fixed by β ,*
3. *symbol l_{ij} is fixed by γ .*

Proof. Suppose row i is fixed by α and column j is fixed by β . Since θ is an autotopism, $\gamma(l_{ij}) = l_{\alpha(i)\beta(j)} = l_{ij}$ by (1.4). The remaining cases are handled similarly. \square

Our next lemma illustrates how subsquares arise naturally in the study of autotopisms and is often used in Chapter 2.

Lemma 1.2.8. *Let L be a Latin rectangle and $\theta = (\alpha, \beta, \gamma)$ be an autotopism of L . Let M denote the submatrix formed by the intersection of the rows whose indices are fixed by α and the columns whose indices are fixed by β . Then M is a subrectangle of L . In particular, if L is a Latin square, then M is a (possibly empty) subsquare of L .*

Proof. Lemma 1.2.7 implies that (a) every symbol in M is fixed by γ and (b) every symbol occurring outside of M , but in a row shared with M , is not fixed by γ . Therefore, M is a subrectangle of L .

When L is a Latin square, a similar argument shows that $M^{(rc)}$ is a subrectangle of $L^{(rc)}$. Hence M must be a subsquare. \square

Lemma 1.2.8 was a precursor to a theorem of McKay, Meynert and Myrvold [222] (Theorem 4.3.6). Lemma 1.2.8 will be generalised by Lemma 2.5.4 on page 53, when L is a Latin square.

We will now briefly introduce transversals of Latin squares, which are another important object within many Latin squares. If $L = (l_{ij})$ is a Latin square of order n , then a *diagonal* of L (or any square matrix) is a set of n entries of L such that if (i, j, l_{ij}) and $(i', j', l_{i'j'})$ are two distinct entries in the diagonal then $i \neq i'$ and $j \neq j'$. A diagonal that consists of n distinct symbols is called a *transversal*. A survey on the theory of transversals of Latin squares was given by Wanless [324].

We consider a notion of transversals for Latin hypercuboids in Section 2.5. In Chapter 3, we will see that transversals of the Cayley table of \mathbb{Z}_n are equivalent to orthomorphisms of \mathbb{Z}_n .

1.2.4 Permanents and bounds

In this section we discuss the known bounds for R_n . We will see that the best known bounds for R_n are still quite poor. We can easily find a super-exponential lower bound on R_n . In fact, for any $k \geq 2$, $R_{k,n}$ increases super-exponentially as $n \rightarrow \infty$. To show this, observe that $R_{k,n} \geq R_{k',n}$ whenever $k' \leq k \leq n$, by Theorem 1.1.1 and (1.1). A *derangement* is a permutation without fixed points. When $n \geq k$ we have $R_{k,n} \geq R_{2,n} = D_n/(n-1)$, where D_n is the number of derangements on a set of cardinality n . It is well-known that $D_n \sim \exp(-1) \cdot n!$. Hence $R_{k,n}$ increases super-exponentially with n and $R_n \geq R_{k,n}$ when $n \geq k$.

To study the bounds on $R_{k,n}$, we will need to introduce the permanent function for square matrices. The *permanent* of a square matrix, $M = (m_{ij})_{n \times n}$ is defined as

$$\text{PER}(M) = \sum_{\sigma \in S_n} \prod_{i \in \mathbb{Z}_n} m_{i\sigma(i)}$$

where S_n is the symmetric group on \mathbb{Z}_n . The primary source of information for permanents is Minc [233, 234, 235]; see also his biography by Marcus [216].

Given a $k \times n$ Latin rectangle L we can construct an $n \times n$ $(0, 1)$ -matrix $T = (t_{ij})$ such that $t_{ij} = 1$ if and only if symbol j does not occur in column i in L . The matrix T is called the *template* of L . We will index the rows and columns of T by \mathbb{Z}_n . For any $\sigma \in S_n$, if $t_{i\sigma(i)} = 1$ for all $i \in \mathbb{Z}_n$ then L can be extended to a $(k+1) \times n$ Latin rectangle with the new row containing symbol $\sigma(i)$ in column i for each $i \in \mathbb{Z}_n$. Therefore, the number of ways L can be extended to a $(k+1) \times n$ Latin rectangle is $\text{PER}(T)$.

Let Λ_n^s denote the set of $(0, 1)$ -matrices with exactly s non-zero entries in each row and column. It follows that

$$\prod_{s=0}^{k-1} \min_{M \in \Lambda_n^{n-s}} \text{PER}(M) \leq L_{k,n} \leq \prod_{s=0}^{k-1} \max_{M \in \Lambda_n^{n-s}} \text{PER}(M). \quad (1.5)$$

Let $M = (m_{ij})$ be a $(0, 1)$ -matrix and define the row sum $r_i = \sum_{j \in \mathbb{Z}_n} m_{ij}$ for all rows i . Hall Jr [149] showed that if $\text{PER}(M) > 0$ then $\text{PER}(M) \geq \min_{i \in \mathbb{Z}_n} r_i!$. Jurkat and Ryser [176, (12.33)] showed that $\text{PER}(M) \geq \prod_{i=1}^n \max(0, r_i - i + 1)$. Minc [232] showed that a result of Sinkhorn [287] implies that if $M \in \Lambda_n^s$ then $\text{PER}(M) \geq n(s-3)/3$ and improved this lower bound to $\text{PER}(M) \geq n(s-2) + 2$.

Minc [230] showed that $\text{PER}(M) \leq \prod_{i \in \mathbb{Z}_n} (r_i + 1)/2$ with equality if and only if $M \in \Lambda_n^1$ which was subsequently improved [231] to $\text{PER}(M) \leq \prod_{i \in \mathbb{Z}_n} (r_i + \sqrt{2})/(1 + \sqrt{2})$. Brègman [31] (see also [281]) proved a conjecture of Minc [230] that $\text{PER}(M) \leq \prod_{i \in \mathbb{Z}_n} r_i!^{1/r_i}$. Liang and Bai [205] gave $\text{PER}(M) \leq \prod_{i=0}^{n-1} \sqrt{a_i(r_i - a_i + 1)}$ where $a_i = \min(\lceil (r_i + 1)/2 \rceil, \lceil i/2 \rceil)$. A lower bound for the maximum permanent in Λ_n^s was given by Wanless [321].

We can combine (1.5) with the above bounds on the permanent of matrices in Λ_n^s to find bounds for $L_{k,n}$ and consequently $R_{k,n}$ by (1.1). We will now discuss some other bounds on R_n . Hall Jr [149] gave the lower bound $R_{k,n} \geq \prod_{i=n-k+1}^{n-2} i!$, which was also proved by Ryser [273, pp. 52–53]. Alter [7] gave the “crude upper bound” $R_n \leq (n-1)! \prod_{i=1}^{n-2} i^{n-i-1} \cdot i!$. An upper bound was also given by Duan [86], but it is no better than that of Alter for $n \geq 13$, although it appears Duan did not have access to Alter’s paper. Smetaniuk [291] showed that $L_{n+1} \geq (n+1)!L_n$ and therefore $R_{n+1} \geq (n-1)!R_n$ by (1.1). Van Lint and Wilson [315, Thm 17.2] showed that the van der Waerden Conjecture [313] (proved by [90, 115]) implies that $L_n \geq n!^{2n} n^{-n^2}$.

A comparison of the discussed bounds for R_n is given in Figure 1.12. We also include the known values of R_n and the approximations by [200, 223, 344] (see also Figure 1.3). It is clear there remains a large difference between the best upper and lower bounds on R_n . Judging from Figure 1.12, it appears that the best known upper and lower bounds on R_n both have at least an exponential difference from R_n .

n	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Lower bound by:																
Hall Jr	2	3	5	8	12	16	22	28	36	45	54	65	77	91	105	121
Smetaniuk								42	51	61	72	84	97	112	127	145
van Lint and Wilson	1	2	4	8	13	20	28	37	48	61	76	93	112	132	155	180
R_n	2	4	8	12	18	25	34									
Approximation	2	4	8	12	18	25	34	45	57	71	87	104	124	146	170	195
Upper bound by:																
Brègman, Minc	3	5	9	14	21	29	38	49	63	77	94	113	134	156	181	208
Liang and Bai	2	5	9	14	20	29	38	50	63	79	96	116	137	161	187	215
Alter	4	7	12	19	27	37	50	64	80	99	119	142	168	196	226	259
Duan	2	5	10	16	25	35	48	63	81	101	123	149	177	208	242	278

FIGURE 1.12: The number of decimal digits of some bounds on R_n , approximations of R_n and the value of R_n itself.

1.2.5 The sign of a Latin square

Let α be a permutation of \mathbb{Z}_n . If α can be decomposed into the composition of an even number of transpositions, then α is called an *even* permutation, otherwise α is called an *odd*

permutation. Define the *sign* of α , denoted $\epsilon(\alpha)$, as $+1$ if α is an even permutation and -1 if α is an odd permutation. Since “ α is an even (or odd) permutation” and “ $\epsilon(\alpha) = +1$ (or -1)” are equivalent statements, the adjective that describes α , even or odd, is also referred to as the *sign* of α .

Given a Latin square $L = (l_{ij})$ of order n , we can identify the following $3n$ permutations of \mathbb{Z}_n .

- For all $i \in \mathbb{Z}_n$ define $\sigma_i^{\text{row}} = \sigma_i^{\text{row}}(j)$ such that $\sigma_i^{\text{row}}(j) = l_{ij}$.
- For all $j \in \mathbb{Z}_n$ define $\sigma_j^{\text{col}} = \sigma_j^{\text{col}}(i)$ such that $\sigma_j^{\text{col}}(i) = l_{ij}$.
- For all $\ell \in \mathbb{Z}_n$ define $\sigma_\ell^{\text{sym}} = \sigma_\ell^{\text{sym}}(i)$ such that $\sigma_\ell^{\text{sym}}(i)$ is equal to j for which $l_{ij} = \ell$.

We call $\epsilon_{\text{row}}(L) := \prod_i \epsilon(\sigma_i^{\text{row}})$, $\epsilon_{\text{col}}(L) := \prod_j \epsilon(\sigma_j^{\text{col}})$ and $\epsilon_{\text{sym}}(L) := \prod_\ell \epsilon(\sigma_\ell^{\text{sym}})$ the *row-sign*, *column-sign* and *symbol-sign* of L , respectively. The product $\epsilon(L) := \epsilon_{\text{row}}(L)\epsilon_{\text{col}}(L)$ is called the *sign* of L .

A Latin square is called *even* or *odd* if $\epsilon(L) = +1$ or $\epsilon(L) = -1$, respectively. A Latin square is called *row-even* or *row-odd* if $\epsilon_{\text{row}}(L) = +1$ or $\epsilon_{\text{row}}(L) = -1$, respectively. A Latin square is called *column-even* or *column-odd* if $\epsilon_{\text{col}}(L) = +1$ or $\epsilon_{\text{col}}(L) = -1$, respectively. A Latin square is called *symbol-even* or *symbol-odd* if $\epsilon_{\text{sym}}(L) = +1$ or $\epsilon_{\text{sym}}(L) = -1$, respectively. We define the properties

- EVEN = “is an even Latin square,”
- ODD = “is an odd Latin square,”
- RE = “is a row-even Latin square,”
- RO = “is a row-odd Latin square,”
- CE = “is a column-even Latin square,”
- CO = “is a column-odd Latin square,”
- SE = “is a symbol-even Latin square,”
- SO = “is a symbol-odd Latin square.”

Let P be a property of Latin squares of order n .

- Let L_n^P be the number of Latin squares of order n that satisfy P .
- Let R_n^P be the number of reduced Latin squares of order n that satisfy P .
- Let U_n^P be the number of normalised unipotent Latin squares of order n that satisfy P .
- Let T_n^P be the number of unipotent Latin squares of order n with the first column $(0, 1, \dots, n-1)^T$ that satisfy P .

Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be an isotopism. By considering the action of θ on each individual row and column we find that

$$\epsilon(\theta(L)) = \epsilon(L)\epsilon^n(\alpha)\epsilon^n(\beta)\epsilon^{2n}(\gamma) = \epsilon(L)\epsilon^n(\alpha)\epsilon^n(\beta). \quad (1.6)$$

For example, (1.6) implies that θ preserves the sign of a Latin square (a) if n is even or (b) if θ is a isomorphism. So, when n is even and $P \in \{\text{EVEN}, \text{ODD}\}$,

$$L_n^P = n!(n-1)!R_n^P = n!(n-1)!U_n^P. \quad (1.7)$$

Let L be an arbitrary Latin square of order n for odd $n \geq 3$, if we choose $\theta = (\alpha, \varepsilon, \varepsilon)$ where α consists of a single 2-cycle (i.e. a transposition) and fixed points, then $\epsilon(L) = -\epsilon(\theta(L))$, by (1.6). Since $\theta(L) \neq L$, we find that, when n is odd and $n \geq 3$,

$$L_n^{\text{EVEN}} = L_n^{\text{ODD}} = \frac{1}{2}L_n = \frac{1}{2}n!(n-1)!R_n = \frac{1}{2}n!(n-1)!U_n. \quad (1.8)$$

For odd n , despite $L_n^{\text{EVEN}} = L_n^{\text{ODD}}$, it is conjectured that both $R_n^{\text{EVEN}} \neq R_n^{\text{ODD}}$ and $U_n^{\text{EVEN}} \neq U_n^{\text{ODD}}$, as we will discuss in the next section. On the other hand, for even n , (1.7) implies that

$$R_n^{\text{EVEN}} = R_n^{\text{ODD}} \iff U_n^{\text{EVEN}} = U_n^{\text{ODD}} \iff L_n^{\text{EVEN}} = L_n^{\text{ODD}}.$$

Conjectures

We now introduce the following conjecture by Alon and Tarsi [5] and a theorem of Drisko [83], which motivate the results in Section 2.7.

Conjecture 1.2.9 (Alon-Tarsi Conjecture). $L_n^{\text{EVEN}} \neq L_n^{\text{ODD}}$ when n is even.

Theorem 1.2.10. *If p is a prime and $p \geq 3$ then $L_{p+1}^{\text{EVEN}} - L_{p+1}^{\text{ODD}} \equiv (-1)^{(p+1)/2} p^2 \pmod{p^3}$.*

Theorem 1.2.10 proves a special case of the Alon-Tarsi Conjecture. After proving Theorem 1.2.10, Drisko asked if his method could be extended to include other cases, giving three examples which he thought looked promising. In Corollary 2.7.7 we will prove that $L_{n+1}^{\text{EVEN}} \equiv L_{n+1}^{\text{ODD}} \pmod{t^3}$ for all $1 \leq t \leq n$ except when $t = n$ and n is prime, which includes all of the cases suggested by Drisko.

Alon and Tarsi showed that their conjecture implies the even n case of a conjecture (Theorem 1.2.11) that has been attributed to Dinitz [94]. Theorem 1.2.11 was proved by Galvin [125] and Slivnik [289] (see also [57, 147, 170, 341]).

Theorem 1.2.11 (Dinitz Conjecture). *Given any n^2 sets S_{ij} of cardinality n with $0 \leq i, j \leq n-1$, there always exists an $n \times n$ matrix (l_{ij}) with each $l_{ij} \in S_{ij}$ without repeated symbols in any row or column.*

Huang and Rota [163] showed that the Alon-Tarsi Conjecture is equivalent to the following conjecture.

Conjecture 1.2.12. $R_n^{\text{RE}} \neq R_n^{\text{RO}}$ when n is even.

Actually, in [163] it was conjectured that $L_n^{\text{RE}} \neq L_n^{\text{RO}}$ for even n , but this is equivalent to Conjecture 1.2.12. Some values of R_n^{RE} and R_n^{RO} were given in [145] for $n \leq 7$ (which is incorrect for $n = 4$ and the sign of $R_n^{\text{RE}} - R_n^{\text{RO}}$ is missing when $n = 7$). Also see [171, 217, 218, 343] for further results on the row-sign of Latin squares and Latin rectangles.

Huang and Rota [163] showed that the Alon-Tarsi Conjecture implies a conjecture of Rota entitled ‘‘Rota’s Colorful Conjecture’’ [256] or ‘‘Rota’s Basis Conjecture’’ [134].

Dougherty and Szczepanski [80] conjectured a generalisation of the Alon-Tarsi Conjecture, which is discussed in Section 2.5.1. We prove a special case of Dougherty and Szczepanski’s generalised version of the Alon-Tarsi Conjecture in Theorem 2.5.11.

We also list the following related conjectures. The first conjecture was made by Zappa [340] and the second was not found in the literature.

Conjecture 1.2.13. $U_n^{\text{EVEN}} \neq U_n^{\text{ODD}}$ for all $n \geq 1$.

Conjecture 1.2.14. $R_n^{\text{EVEN}} \neq R_n^{\text{ODD}}$ for all $n \geq 1$.

For even n , (1.7) implies that

$$R_n^{\text{EVEN}} - R_n^{\text{ODD}} = \frac{1}{n!(n-1)!} (L_n^{\text{EVEN}} - L_n^{\text{ODD}}) = U_n^{\text{EVEN}} - U_n^{\text{ODD}}. \quad (1.9)$$

However, Conjectures 1.2.13 and 1.2.14 are not equivalent for all odd n , for example, Figures 1.13 and 1.14 show that $R_7^{\text{EVEN}} - R_7^{\text{ODD}} = 276480 \neq 368640 = U_7^{\text{EVEN}} - U_7^{\text{ODD}}$. Figure 1.13 implies that $|R_n^{\text{RE}} - R_n^{\text{RO}}| = |U_n^{\text{EVEN}} - U_n^{\text{ODD}}|$, so Conjecture 1.2.13 implies Conjecture 1.2.12 is true for all $n \geq 1$.

Drisko [84] showed that $U_p^{\text{EVEN}} - U_p^{\text{ODD}} \equiv (-1)^{(p-1)/2} \pmod{p}$ for odd primes p . Glynn [134] showed that $L_{p-1}^{\text{EVEN}} - L_{p-1}^{\text{ODD}} \equiv (-1)^{(p-1)/2} \pmod{p}$ for odd primes p . Glynn also showed that a result of Zappa [340] is unreliable, which has consequences for [84]. Marini and Pirillo [217] (see also [340]) gave the value of $U_n^{\text{EVEN}} - U_n^{\text{ODD}}$ for $n \leq 8$.

To review, we know the Alon-Tarsi Conjecture and Conjectures 1.2.12, 1.2.13 and 1.2.14 are true when $n = p \pm 1$ for some odd prime p and when $n \leq 8$ (see Figure 1.14 or Appendix A.2). Additionally, Conjecture 1.2.13 holds when n is a prime.

Data

A theorem of Wanless [322] (see also [339]) states that

$$\epsilon_{\text{row}}(L)\epsilon_{\text{col}}(L)\epsilon_{\text{sym}}(L) = \begin{cases} +1 & \text{if } n \equiv 0 \text{ or } 1 \pmod{4} \\ -1 & \text{if } n \equiv 2 \text{ or } 3 \pmod{4} \end{cases} \quad (1.10)$$

In particular, we can use (1.10) to find $\epsilon_{\text{sym}}(L)$ from $\epsilon_{\text{row}}(L)$, $\epsilon_{\text{col}}(L)$ and the value of $n \pmod{4}$. We define the *parity* of a Latin square L to be the triplet

$$\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}} \in \left\{ \overbrace{000, 011, 101, 110}^{n \equiv 0 \text{ or } 1 \pmod{4}}, \overbrace{001, 010, 100, 111}^{n \equiv 2 \text{ or } 3 \pmod{4}} \right\}$$

such that $\pi_x = 0$ when $\epsilon_x(L) = +1$ and $\pi_x = 1$ when $\epsilon_x(L) = -1$ for $x \in \{\text{row}, \text{col}, \text{sym}\}$. Consequently, we can deduce the equations given in Figure 1.13, where $R_n^{\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}}$ is the number of reduced Latin squares of order n with given parity $\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}$.

Figure 1.14 lists the number $R_n^{\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}}$ of reduced Latin squares with parity $\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}$ for some small n , sourced from [217, 339] and Ian Wanless (private communication). In Appendix A.2 we give tables of values of R_n^{EVEN} , R_n^{ODD} , R_n^{RE} , R_n^{RO} , U_n^{EVEN} and U_n^{ODD} . By considering the effect of transposition on the sign of a Latin square, it can easily be seen that $U_n^{\text{EVEN}} = T_n^{\text{EVEN}}$ and $U_n^{\text{ODD}} = T_n^{\text{ODD}}$ for all n and so $R_n^{010} = R_n^{100}$ and $R_n^{011} = R_n^{101}$ for all n . Moreover, combining Figure 1.13 and (1.9), we find that $R_n^{110} = R_n^{101} = R_n^{011}$ when $n \equiv 0 \pmod{4}$ and $R_n^{100} = R_n^{010} = R_n^{001}$ when $n \equiv 2 \pmod{4}$. The Alon-Tarsi Conjecture is therefore equivalent to the conjecture that $R_n^{000} \neq R_n^{110}$ when $n \equiv 0 \pmod{4}$ and $R_n^{001} \neq R_n^{111}$ when $n \equiv 2 \pmod{4}$ [217].

If $n \equiv 0$ or $1 \pmod{4}$	If $n \equiv 2$ or $3 \pmod{4}$
$R_n^{\text{EVEN}} = R_n^{\text{SE}} = R_n^{110} + R_n^{000}$	$R_n^{\text{EVEN}} = R_n^{\text{SO}} = R_n^{111} + R_n^{001}$
$R_n^{\text{ODD}} = R_n^{\text{SO}} = R_n^{101} + R_n^{011}$	$R_n^{\text{ODD}} = R_n^{\text{SE}} = R_n^{100} + R_n^{010}$
$U_n^{\text{EVEN}} = R_n^{\text{CE}} = R_n^{101} + R_n^{000}$	$U_n^{\text{EVEN}} = R_n^{\text{CO}} = R_n^{111} + R_n^{010}$
$U_n^{\text{ODD}} = R_n^{\text{CO}} = R_n^{110} + R_n^{011}$	$U_n^{\text{ODD}} = R_n^{\text{CE}} = R_n^{100} + R_n^{001}$
$T_n^{\text{EVEN}} = R_n^{\text{RE}} = R_n^{011} + R_n^{000}$	$T_n^{\text{EVEN}} = R_n^{\text{RO}} = R_n^{111} + R_n^{100}$
$T_n^{\text{ODD}} = R_n^{\text{RO}} = R_n^{110} + R_n^{101}$	$T_n^{\text{ODD}} = R_n^{\text{RE}} = R_n^{010} + R_n^{001}$

FIGURE 1.13: Table of equations.

	Even Latin squares				Odd Latin squares	
	$n \equiv 0, 1 \pmod{4}$		$n \equiv 2, 3 \pmod{4}$		$n \equiv 0, 1 \pmod{4}$	$n \equiv 2, 3 \pmod{4}$
	R_n^{000}	R_n^{110}	R_n^{001}	R_n^{111}	$R_n^{011} = R_n^{101}$	$R_n^{010} = R_n^{100}$
$n = 2$				1		
3			1			
4	4					
5	8	32			8	
6			1776	4080		1776
7			4120320	4488960		4166400
8	138478485504	132267638784			132267638784	

FIGURE 1.14: The number $R_n^{\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}}$ of reduced Latin squares of order n with given parity $\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}$.

1.2.6 Algorithms

Enumeration algorithms

Modern enumeration algorithms for Latin rectangles, for example those of McKay and Ro-goyski [223] and McKay and Wanless [225], stem from a result of Sade [274], related to Theorem 1.2.15.

Recall the definition of the template of a Latin rectangle from Section 1.2.4. We call two $k \times n$ Latin rectangles L and L' *template equivalent* if the template of L' or its transpose can be formed from the template of L by some row and column permutations.

Theorem 1.2.15. *Suppose L and L' are $k \times n$ Latin rectangles such that L and L' are template equivalent. Then L can be extended to a $k^* \times n$ Latin rectangle, for any k^* in the range $k \leq k^* \leq n$, in the same number of ways as L' .*

There is some discrepancy in the literature as to which equivalence relation Sade actually used in [274]. According to Wells [326] (and [71, pp. 142–143]), Sade found isotopy class representatives for the 2×7 , the 3×7 and the 4×7 Latin rectangles, keeping track of the number of ways each rectangle could have been formed. Afterwards, Sade simply computed the number of completions of each 4×7 Latin rectangle representative to complete the enumeration of the Latin squares of order 7. However, both Yamamoto [336] and Bammel and

Rothstein [16] imply that the equivalence relation that Sade used is what we call template equivalent, but without transposition.

Sade's idea was first adapted to the computer by Wells [326, 327], who gave the correct value for R_8 , which he computed on the MANIAC II computer at the Los Alamos Scientific Laboratory. Bammel and Rothstein [16] verified the values for R_7 and R_8 and discovered R_9 , with the use of the PDP-10 (Programmed Data Processor model 10) computer. The algorithms of [223] and [225] were graph theoretic adaptations of Theorem 1.2.15 that made use of *nauty* [220].

We will now describe the formulae that McKay and Wanless [225] used to find $R_{k,11}$. Given a $k \times n$ Latin rectangle L , we can construct a bipartite graph $B = B(L)$ with vertex bipartition $C \cup S$ where C is the set of columns of L , and S is the set of symbols of L . Vertices $c \in C$ and $s \in S$ are adjacent if and only if symbol s occurs in column c in L . So B is regular of degree k .

Let \mathcal{T} be the group of paratopisms that combines isotopisms of the form $(\varepsilon, \beta, \gamma)$ and (cs) -conjugation, where ε is the identity permutation. Then \mathcal{T} acts on the set of k -regular bipartite graphs on C and S , by permuting the vertices of C and S individually and possibly by swapping the sets C and S . Let $\mathcal{B}(k, n)$ be a set containing one representative from each orbit of k -regular bipartite graphs on the vertices $C \cup S$ under the action of \mathcal{T} . For any $B \in \mathcal{B}(k, n)$ let $\text{Aut}_{\mathcal{T}}(B)$ denote the group of all $\tau \in \mathcal{T}$ such that $\tau(B) = B$.

Let B' be the bipartite complement of B , that is, B' is a bipartite graph with vertex bipartition $C \cup S$ such that $c \in C$ is adjacent to $s \in S$ if and only if symbol s does not occur in column c in L . Recall that, for any graph, a one-factor is a 1-regular spanning subgraph and a one-factorisation is a decomposition into one-factors. Let $m(H)$ denote the number of one-factorisations of a graph H . Whenever $0 \leq k \leq n$,

$$R_n = 2nk!(n-k)! \sum_{B \in \mathcal{B}(k,n)} \frac{m(B)m(B')}{|\text{Aut}_{\mathcal{T}}(B)|}$$

and

$$R_{k,n} = 2nk!(n-k)! \sum_{B \in \mathcal{B}(k,n)} \frac{m(B)}{|\text{Aut}_{\mathcal{T}}(B)|}.$$

It is possible to compute $m(B)$ with the recurrence relation

$$m(B) = \sum_{F \in \mathcal{F}_e} m(B - F)$$

for any edge e of B , where \mathcal{F}_e is the set of all one-factors F of B that contain e . We use $B - F$ to denote the graph formed by deleting the edges from B that are also in F . Describing their computation of $R_{k,11}$, McKay and Wanless made the following comment.

“The main practical difficulty was the efficient management of the fairly large amount of data... It is unlikely that R_{12} will be computable by the same method for some time.”

— MCKAY AND WANLESS [225]

Random Latin squares and Latin rectangles

In this section we will briefly review the algorithms used in generating random Latin squares and rectangles. There are several reasons why one would want to generate random Latin squares, for example, they can assist in identifying which properties of Latin squares are typical or not. There are also practical applications, for example, in experimental design [14, 15]. The problem of uniform random Latin square generation is outside of the scope of this thesis, however the following quote motivates at least a brief mention.

“Why is this a challenge? Counting Latin squares is hard, and the problems of counting and random generation are, in general, closely related. The difficulties are illustrated by a couple of unsuitable generation algorithms:

We could generate random permutations of the symbols to fill a square a row at a time. Each permutation would be restricted to choices that would not cause column conflicts with the already-filled rows... However, we have no general way of weighting these choices appropriately in order to achieve the uniform distribution on Latin squares.

We could generate uniformly distributed random permutations to fill a square a row at a time, restarting from scratch if we produce a column conflict. This algorithm terminates with probability 1, and it produces uniformly distributed random Latin squares. However, the expected number of “starts” we make before successfully completing an order- n LS is $n!^{n-1}/L_n = e^{n^2(1+o(1))}$, which is unacceptable; the price we pay for uniformity is computational complexity.

— JACOBSON AND MATTHEWS [169]

O’Carroll [253] described a basic algorithm for generating random Latin squares which was implemented on the Elliott 803 computer. However, O’Carroll’s algorithm does not generate Latin squares uniformly at random. McKay and Wormald [227] provide an algorithm that generates a $k \times n$ Latin rectangle uniformly at random in expected time $O(nk^3)$ provided $k = o(n^{1/3})$. Jacobson and Matthews [169] provided a Markov chain Monte-Carlo algorithm for generating Latin squares of order n approximately uniformly at random. This algorithm has been implemented in the LOOPS [242] package for GAP [127] and SAGE [277], for example.

1.2.7 Software

Nagy and Vojtěchovský [243] produced a package LOOPS [242] for GAP [127] for the study of loops and quasigroups. Some functions that are likely to be useful to the reader are:

- `RandomQuasigroup(n)`; returns a random quasigroup of order n .
- `RandomLoop(n)`; returns a random loop of order n .

- `CayleyTable(Q)`; returns a Cayley table of the quasigroup Q .
- `AutomorphismGroup(L)`; returns the automorphism group of the loop L .
- `IsotopismLoops(L,M)`; returns an isotopism θ such that $\theta(L) = M$ if θ exists and returns `fail` otherwise.

The `RandomQuasigroup(n)` and `RandomLoop(n)` functions make use of the algorithm by Jacobson and Matthews [169].

Two features that are absent from LOOPS (version 2.1.0) are (a) a function that returns the autotopism group of a quasigroup and (b) a function that returns the autoparatopism group of a quasigroup. In Appendix A.1 we have included some GAP code that will enable us to compute the autotopism and autoparatopism groups of a Latin square. It requires the GRAPE [295] package for GAP, which in turn requires McKay’s nauty [220] package.

1.3 History of the enumeration of Latin rectangles

The enumeration of Latin rectangles, particularly Latin squares, has a long history stretching back to Euler [97, 99], including names like Cayley [54] and MacMahon [209, 210, 211]. McKay, Meynert and Myrvold [222] surveyed the “sorry history” of the enumeration of Latin squares, pointing out numerous published errors. We survey the formulae for the number of Latin rectangles in Section 1.3.1. Denés and Keedwell [71, Sec. 4.4] also gave a brief survey of the enumeration of Latin rectangles. Several other Ph.D. theses were concerned with problems related to the enumeration of Latin squares and rectangles; for example, Brown [33], Nechvatal [244], Smetaniuk [292], Green [139] and Drisko [82].

1.3.1 Formulae for L_n and $L_{k,n}$

In this section we will survey the general formulae for L_n (Sloane’s [290] A002860) and $L_{k,n}$. The first part of this section focuses on the formulae for $R_{k,n}$ for small fixed k , which comes from the literature review in [308]. The remainder of this section follows the survey paper [301].

The number D_n of derangements (permutations without fixed points) of n elements is related to the number of $2 \times n$ Latin rectangles by

$$D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!} = K_{2,n} = (n-1)R_{2,n}. \quad (1.11)$$

The enumeration of $L_{3,n}$, the number of three-line Latin rectangles, has a long history. Recurrence formulae for $L_{3,n}$ were shown by Jacob [168] (which is invalid for $n \geq 8$), Kerewala [183] and Riordan [269]. Riordan [267, 268] established the link between three-line Latin rectangles and the famous *problème de ménages* (see also [237]). Dulmage [88] provided an explicit formula for $L_{3,n}$, which was later refined by Dulmage and McMaster [89]. Bogart and Longyear [24] provided a practical formula for $K_{3,n}$, which they used for $n \leq 11$ exactly (with typographical errors in the values of $K_{3,7}$ and $K_{3,8}$) and approximately for $n \leq 20$, accurate to

12 significant figures. Riordan [269] gave the credit to Yamamoto [333] for the equation

$$R_{3,n} = \sum_{i+j+k=n} n(n-3)!(-1)^j \frac{2^k i!}{k!} \binom{3i+j+2}{j}, \quad (1.12)$$

where i, j, k are non-negative integers. Equation (1.12) also appears in [264]. Gessel [130] provided a formula for $K_{3,n}$ based on the cycle decomposition of the permutations defined by the second and third rows of a normalised three-line Latin rectangle. Kerawala [184] and Yamamoto [334, 337] studied the asymptotic value of $L_{3,n}$. Goulden and Jackson [137] showed that $R_{3,n}$ is the coefficient of $x^n/(n(n-3)!)$ in the expansion of

$$\exp(2x) \sum_{i \geq 0} \frac{i! x^i}{(1+x)^{3i+3}}.$$

Riordan [269] gave the congruence $R_{3,n+p} \equiv 2R_{3,n} \pmod{p}$ for all odd primes p , which was generalised by Carlitz [46] to $R_{3,n+t} \equiv 2^t R_{3,n} \pmod{t}$ for all $t \geq 1$. We will later generalise these congruences by Corollary 2.3.6.

Light Jr [206], Athreya, Pranesachar and Singhi [12, 263] and Doyle [81] gave formulae for $L_{4,n}$, the number of four-line Latin rectangles (Sloane's A000573). Light Jr gave a table of values of $K_{4,n}$ that is correct for $4 \leq n \leq 7$, but incorrect when $n = 8$.

We now begin our survey of explicit formulae for $L_{k,n}$ for general k . First, we identify $L_{k,n}$ as a coefficient in a polynomial in kn variables. Let $X = (x_{ij})$ be a $k \times n$ matrix whose symbols are the kn variables x_{ij} . We index the rows of X by $[k] := \{1, 2, \dots, k\}$ and the columns of X by $[n] := \{1, 2, \dots, n\}$, so $[k] \subseteq [n]$. Let $S_{k,n}$ be the set of injections $\sigma : [k] \rightarrow [n]$. We define the *permanent* of the rectangular matrix X to be

$$\text{PER}(X) = \sum_{\sigma \in S_{k,n}} \prod_{i=1}^k x_{i\sigma(i)}.$$

When $k = n$ this matches our definition of permanent for square matrices introduced in Section 1.2.4, except with different indices on X . It follows that $L_{k,n}$ is the coefficient of $\prod_{i=1}^k \prod_{j=1}^n x_{ij}$ in $\text{PER}(X)^n$. This property was noticed over a century ago by MacMahon [209] in the theory of symmetric functions encoded with $x_{ij} = \alpha_i^{2^{j-1}}$. He gives a different, but related formula in [211, Vol. 2, pp. 323–326] (also see his collected works [212]). We can obtain the value of $L_{k,n}$ from $\text{PER}(X)^n$ by differentiation, for example

$$L_{k,n} = \frac{\partial}{\partial x_{11}} \Big|_{x_{11}=0} \cdots \frac{\partial}{\partial x_{kn}} \Big|_{x_{kn}=0} \text{PER}(X)^n \quad (1.13)$$

which, when $k = n$, was one of Fu's [124] equations. MacMahon also used differentiation to “obliterate” the unwanted terms from $\text{PER}(X)^n$ but in a different, more complicated, way to (1.13). The merit of MacMahon's formulae has inspired much discussion.

“The calculation will, no doubt, be laborious but that is here not to the point, as an enumeration problem may be considered to be solved when definite algebraical processes are set forth which lead to the solution.”

— MACMAHON [209]

“The problem of enumerating n by k Latin rectangles was solved formally by MacMahon using his operational methods.”
— ERDŐS AND KAPLANSKY [93]

“A complete algebraic solution has been given by MacMahon in two forms, both of which involve the action of differential operators on an extended operand. If MacMahon’s algebraic apparatus be actually put into operation, it will be found that different terms are written down, corresponding to all the different ways in which each row of the square could conceivably be filled up, that those arrangements which conflict with the conditions of the Latin square are ultimately obliterated, and those which conform to these conditions survive the final operation and each contribute unity to the result. The manipulation of the algebraic expressions, therefore, is considerably more laborious than the direct enumeration of the possible squares by a systematic and exhaustive series of trials.”
— FISHER AND YATES [119]

“The use of MacMahon’s result by mere mortals seems doomed.”
— RIORDAN [270]

MacMahon’s formula was nonetheless employed in a simplified form by Saxena [278, 279] to find L_6 and L_7 , although these numbers were found earlier, see Figure 1.1. Another proof of MacMahon’s formula for L_n was given by van Leijenhorst [314], who described it as both “beautiful” and “handsome.” MacMahon had a particularly unorthodox life, even for a mathematician, which can be discovered in his biography [128].

Another way of extracting the value of $L_{k,n}$ from $\text{PER}(X)^n$ was given by Fu [124], Shao and Wei [282] and McKay and Wanless [225]. We will write their formulae in a more general form in (1.15).

Let $\mathcal{B}_{k,n}$ be the set of $k \times n$ $(0, 1)$ -matrices. As identified by Fu [124] and Shao and Wei [282], we can use Inclusion-Exclusion to obtain

$$L_{k,n} = \sum_{A \in \mathcal{B}_{k,n}} (-1)^{\sigma_0(A)} \text{PER}(A)^n, \quad (1.14)$$

where $\sigma_0(A)$ is the number of zeroes in A . Fu essentially gave (1.14), but the summation is split in a different way. It seems that [124] and [282] obtained (1.14) independently as neither paper has mention of the other.

Let c and d be real numbers such that $c \neq 0$ and let $\bar{X} = cX + dJ$ where J is the all-1 matrix. It follows that $L_{k,n}$ is the coefficient of $c^{kn} \prod_{i=1}^k \prod_{j=1}^n x_{ij}$ in $\text{PER}(\bar{X})^n$. We claim that

$$L_{k,n} = c^{-kn} \sum_{A \in \mathcal{B}_{k,n}} (-1)^{\sigma_0(A)} \left(\text{PER}(\bar{A})^n + f(\text{PER}(\bar{A})) \right) \quad (1.15)$$

where $\bar{A} = cA + dJ$ and f is any polynomial of degree at most $n - 1$. If we let $g = g(A)$ be any summand of $f(\text{PER}(\bar{A}))$ when fully expanded, then g has integral degree in each a_{ij} and total degree at most $k(n - 1)$. Therefore g cannot vary with every a_{ij} , otherwise it would have degree kn . Hence $\sum_{A \in \mathcal{B}_{k,n}} (-1)^{\sigma_0(A)} g(A) = 0$ and so $\sum_{A \in \mathcal{B}_{k,n}} (-1)^{\sigma_0(A)} f(\text{PER}(\bar{A})) = 0$.

Equation (1.15) yields the formula of McKay and Wanless [225] when $c = 2$, $d = -1$ and $k = n$. There were various other formulae for L_n and $L_{k,n}$ given by Shao and Wei [282], which are all special cases of (1.15). There are 2^{kn} matrices $A \in \mathcal{B}_{k,n}$ which makes (1.15) impractical for enumeration.

Fu [124] also gave the equation

$$L_{k,n} = \sum_{A \in \mathcal{B}_{k,n}} (-1)^{\sigma_0(A)} \binom{n^2 - kn + \sigma_0(A)}{\sigma_0(A)} \text{PER}(A)^k$$

which has been rearranged and a problem corrected – the last equation of [124] should have $f_{n(n-r)+k}$ instead of $f_{n(n-r)}$.

Jucys [174] constructed an algebra \mathcal{A}_n over \mathbb{C} , with the “magic squares” as a basis, which were actually $n \times n$ non-negative integer matrices with row and column sums equal to n . Multiplication in \mathcal{A}_n was defined using a “structure constant,” which, in one case, was L_n . An isomorphism was identified between \mathcal{A}_n and a subalgebra of the group algebra of the symmetric group S_{n^2} over \mathbb{C} . Representation theory was then used to give an expression for L_n in terms of eigenvalues of a particular element of \mathcal{A}_n .

“ It seems to us that for obtaining the general formulas for the eigenvalues... some further developments of Young’s substitutional analysis are needed. ”

— JUCYS [174]

Light Jr [207] (see also [206]) gave an equation for the number of “truncated Latin rectangles” which, for Latin rectangles, simplifies to

$$L_{k,n} = \sum_{i=0}^n (-1)^i \binom{n}{i} (n-i)! a_{k,i,n}$$

where $a_{k,i,n}$ is the number of $k \times i$ matrices with symbols from a set of cardinality n such that each row does not have a repeated symbol and each column has at least one repeated symbol.

Let \mathcal{M}_n be the set of partitions of n into parts of size at least 2. For $\mu \in \mathcal{M}_n$, let X_μ be the number of $2 \times n$ Latin rectangles $L = (l_{ij})$ with derangement $l_{0i} \mapsto l_{1i}$ having cycle structure μ . In fact

$$X_\mu = \frac{n!^2}{\prod_i (s_i(\mu)! \cdot i^{s_i(\mu)})},$$

where $s_i(\mu)$ is the number of copies of i in the partition μ . According to Theorem 1.2.15, each L counted by X_μ admits the same number of completions C_μ to a Latin square. Denés and Mullen [75] gave a formula for L_n which is essentially

$$L_n = \sum_{\mu \in \mathcal{M}_n} X_\mu \cdot C_\mu.$$

We will now reproduce Doyle's [81] formula for $K_{k,n}$, which he gives for $2 \leq k \leq 4$. We will consolidate it into a concise general form. Let \mathcal{R} be the set of non-negative integer vectors $\vec{s} = (s_i)_{1 \leq i \leq 2^{k-1}}$ such that $\sum_i s_i = n$. For $1 \leq i \leq 2^{k-1}$, let $\Delta_i = (\delta_{ij})_{1 \leq j \leq 2^{k-1}}$, where δ_{ij} is the Kronecker δ -function. For any non-negative integer i let $b_j(i)$ be the j -th binary digit of i , for example $(b_j(3))_{j \geq 1} = (1, 1, 0, 0, 0, \dots)$. Let $\|\vec{s}\| = \sum_{i,j} s_i b_j(i)$. Then

$$K_{k,n} = \sum_{\vec{s} \in \mathcal{R}} (-1)^{\|\vec{s}\|} \binom{n}{s_1, s_2, \dots, s_{2^{k-1}}} \prod_{i=1}^{2^{k-1}} g(\vec{s} - \Delta_i)^{s_i} \quad (1.16)$$

where subtraction of vectors is component-wise and for $\vec{a} = (a_1, a_2, \dots, a_{2^{k-1}})$

$$g(\vec{a}) = \sum_{P \in \mathcal{P}_{k-1}} \prod_{p \in P} (-1)^{|p|-1} (|p| - 1)! f_p(\vec{a}) \quad (1.17)$$

where \mathcal{P}_{k-1} be the set of partitions of $\{1, 2, \dots, k-1\}$ and

$$f_p(\vec{a}) = \sum_{i: b_j(i)=0 \forall j \in p} a_i$$

for all $p \subseteq \{1, 2, \dots, k-1\}$.

The coefficients in (1.17) were not given by Doyle in full generality, although he did state how to obtain them, that is by Möbius Inversion on the lattice of partitions of $\{1, 2, \dots, k-1\}$ (see [272, p. 360], for example).

“The expressions get uglier and uglier at an exponential rate as k increases... When you come right down to it, no one really wants to know how many k -line Latin rectangles there are anyway.”
— DOYLE [81]

For a fixed k , the function $g(\vec{a})$ is a 2^{k-1} -variate polynomial. Therefore the computational complexity of (1.16) is bounded above by $|\mathcal{R}|h(k, n) \leq n^{2^{k-1}}h(k, n)$ for some polynomial h . According to Wilf [330], the problem of enumerating $k \times n$ Latin rectangles for a fixed k is therefore p -solved – there exists an algorithm that returns $R_{k,n}$ in polynomial-time in n (rather than the length of n).

“Wilf arrived at this definition after he refereed a paper proposing a “formula” for the answer to [what is L_n ?], and realizing that its “computational complexity” exceeds that of the caveman’s formula of direct counting.”
— ZEILBERGER [342]

The author has used (1.16) to find the values of $R_{4,n}$ for $n \leq 80$ (Sloane’s [290] A000573), $R_{5,n}$ for $n \leq 25$, as listed in Appendix A.3 and

$$R_{6,12} = 16790769154925929673725062021120$$

and

$$R_{6,13} = 4453330421956050777867897829494620160.$$

Computing $R_{6,n}$ for $1 \leq n \leq 13$ took just under two months. The C code has been uploaded here [302]; it uses the GMP library [138]. In Appendix A.3 we also list some values of $R_{4,n}$.

There are some other published formulae for the number of Latin rectangles that will not be given explicitly in this thesis because they are similar to (1.16), in that they found by a combination of Inclusion-Exclusion and Möbius Inversion. These are by Nechvatal [244, 245], Gessel [131] (see also [130]), Athreya, Pranesachar and Singhi [12] and Pranesachar [263]. In a 2007 article, de Gennaro [70] claimed to have found a formula for $R_{k,n}$ and wrote

“Until now... no explicit formula is known which permits the calculation of $K_{k,n}$ whatever the value of k .
— DE GENNARO [70]

This misbelief highlights the need for this survey.

We will now introduce a new formula for $L_{k,n}$ whose complexity lies in computing subgraphs of a given graph. Actually, we arrive at this formula using standard techniques in graph theory [329]. Let $G = G_{k,n}$ be the rook's graph introduced in Section 1.2.2. We identified that $L_{k,n}$ is the number of proper vertex-colourings of G with colour set \mathbb{Z}_n . Let $E(G)$ be the edge set of G . For each non-empty $\mathcal{E} \subseteq E(G)$ let $\mathcal{S}_{\mathcal{E}}$ denote the set of improper vertex-colourings of G such that if $uv \in \mathcal{E}$ then u and v receive the same colour. Let \mathcal{S}_{\emptyset} be the set of all n^{kn} vertex-colourings of G . Then

$$L_{k,n} = |\mathcal{S}_{\emptyset}| - \left| \bigcup_{\mathcal{E} \subseteq E(G): \mathcal{E} \neq \emptyset} \mathcal{S}_{\mathcal{E}} \right|.$$

By Inclusion-Exclusion

$$L_{k,n} = \sum_{\mathcal{E} \subseteq E(G)} (-1)^{|\mathcal{E}|} |\mathcal{S}_{\mathcal{E}}|.$$

For any $\mathcal{E} \subseteq E(G)$ let $H_{\mathcal{E}}$ be the graph on the same vertex set as G , but with edge set \mathcal{E} . Then $|\mathcal{S}_{\mathcal{E}}| = n^{c(H_{\mathcal{E}})}$, where $c(H_{\mathcal{E}})$ is the number of connected components of $H_{\mathcal{E}}$. Hence

$$L_{k,n} = \sum_{\mathcal{E} \subseteq E(G)} (-1)^{|\mathcal{E}|} n^{c(H_{\mathcal{E}})}. \quad (1.18)$$

There are $|E(G)| = n \binom{k}{2} + k \binom{n}{2}$ edges in G and $2^{|E(G)|}$ subsets of $E(G)$. While each individual summand of (1.18) is simple to compute, there are too many terms in the sum for practical use.

For any graph H , let $\xi_{k,n}(H)$ be the number of subgraphs of $G_{k,n}$ that are isomorphic to H . Let Γ be a set of isomorphism class representatives of graphs without isolated vertices; here we include the empty graph in Γ which has no vertices, edges and components. Then

$$L_{k,n} = \sum_{H \in \Gamma} (-1)^{|E(H)|} n^{c(H) + kn - |V(H)|} \xi_{k,n}(H)$$

where $V(H)$ is the vertex set of H and $E(H)$ is the edge set of H . It appears that $\xi_{k,n}$ is a difficult function to compute, thus making this formula for $L_{k,n}$ impractical also. A result of Alon [3] implies that $\xi_{n,n}(H) = O(n^{2|V(H)|})$ for any fixed $H \in \Gamma$ as $n \rightarrow \infty$.

As for asymptotic formulae, Godsil and McKay [135, 136] proved

$$L_{k,n} \sim n!^k \left(n(n-1) \cdots (n-k+1)/n^k \right)^n (1-k/n)^{-n/2} \exp(-k/2)$$

as $n \rightarrow \infty$ with $k = o(n^{6/7})$ improving on the work of [93, 298, 335, 338] (see also [297, 299] and [139, 140, 141]). For a history of earlier asymptotic enumerations of Latin rectangles also see [135, 136]. Comtet [64, p. 183] said that even estimating L_n when $n \rightarrow \infty$ “seems to be an extremely difficult combinatorial problem.” However, van Lint and Wilson [315, p. 162] showed that $\frac{1}{n} L_n^{1/n^2} \rightarrow \exp(-2)$ (see also [288]). This is not a particularly satisfying result since, for example, (1.2) and Stirling’s Approximation imply

$$\lim_{n \rightarrow \infty} \frac{1}{n} R_n^{1/n^2} = \lim_{n \rightarrow \infty} \frac{1}{n} L_n^{1/n^2} = \exp(-2),$$

despite L_n and R_n differing by a factor of $n!(n-1)!$. Timashov [312] made the following conjecture.

Conjecture 1.3.1.

$$R_n \sim \frac{1}{2} (2\pi)^{3n/2} \exp(-2n^2 + 3n/2 - 1) n^{n^2 - n/2 - 1}. \quad (1.19)$$

Conjecture 1.3.1 corresponds well with the estimates in Figure 1.3 on page 8, most of which were published after Timashov made Conjecture 1.3.1. For example, Figure 1.3 lists the estimates $R_{50} \approx 3.06 \times 10^{2123}$ and $R_{100} \approx 1.78 \times 10^{11396}$ by Zhang and Ma [344], whereas the right-hand side of (1.19) is approximately 3.02×10^{2123} and 1.76×10^{11396} when $n = 50$ and $n = 100$, respectively.

1.4 Outline

We will now summarise the author’s contributions to the study of the number of Latin rectangles and related combinatorial objects in this thesis. Along the way, we will uncover new interesting research directions and make new goals.

Chapter 2 follows and extends the work in [308] finding divisors of, and congruences for, $R_{k,n}$. In Theorem 2.2.1 we show that $(k-1)!$ divides $R_{k,n}$ when $k \leq \lfloor n/2 \rfloor$ and in Theorem 2.2.2 we show that $\lfloor n/2 \rfloor!$ divides $R_{k,n}$ when $\lfloor n/2 \rfloor < k \leq n$. In Theorems 2.3.1 and 2.3.2 we give the machinery that enables us to deduce numerous congruences for $R_{k,n}$. In Corollary 2.3.3 we show that if p is a prime and $p < k$ then the largest a such that p^a divides $R_{k,n}$ increases at least linearly with n , with k fixed. We eventually reach Theorem 2.4.6 which states that $R_{k,n} \equiv ((-1)^{k-1} (k-1)!)^{n-1} \pmod{n}$. In particular, this means that if n is prime, then $R_{k,n} \equiv 1 \pmod{n}$ for $1 \leq k \leq n$ and if n is composite then $R_{k,n} \equiv 0 \pmod{n}$ if and only if k is larger than the greatest prime divisor of n .

In Section 2.5 we study the generalisation of Latin rectangles to an arbitrary number of dimensions, which we call Latin hypercuboids. We also consider certain subsets of Latin

hypercuboids. Theorem 2.5.6 gives a factorial divisor for the cardinalities of a very general class of subsets of Latin hypercuboids. Corollary 2.5.8 shows that R_n^{EVEN} and R_n^{ODD} are both divisible by $(\lceil n/2 \rceil - 1)!$ for all n . Corollary 2.5.9 gives a divisor for the number of Latin squares without proper subsquares. Theorem 2.5.11 shows that there is a unique reduced $4 \times 4 \times \cdots \times 4$ Latin hypercube that admits a cyclic automorphism based on the 3-cycle that fixes the first index. This leads to Corollary 2.5.12, where we prove a special case of the generalisation of the Alon-Tarsi Conjecture by Dougherty and Szczepanski [80].

In Section 2.6 we apply the theory developed earlier in Chapter 2 to give divisors for the number of decompositions of the labelled complete graph into one-factors, triangles and Hamilton cycles. Finally, In Section 2.7 we show that the methodology of Drisko in proving the $p + 1$ case, for odd prime p , of the Alon-Tarsi Conjecture (Conjecture 1.2.9) cannot be extended to encompass the $n + 1$ case, for composite n . Theorem 2.7.2 also gives new divisors for R_n in some cases.

We then move on to the study of orthomorphisms and partial orthomorphisms of \mathbb{Z}_n , as defined in Chapter 3. We use z_n to denote the number of canonical orthomorphisms and $\omega(n, d) = n^2 \chi(n, d)/d^2$ to denote the number of partial orthomorphisms of \mathbb{Z}_n whose domains have cardinality $n - d$.

Chapter 3 follows the work of [304] and [305] which study the numbers z_n and $\omega(n, d)$ and apply the results to find congruences for $R_{k,n}$. In Theorem 3.2.1 we find the congruence

$$R_{k,n} \equiv \chi(p, n - p) \frac{(n - p)!(n - p - 1)!^2}{(n - k)!} R_{k-p, n-p} \pmod{p}$$

when p is a prime and $n \geq k \geq p + 1$. We compute the values of $\chi(n, d)$ listed in Figure 3.3, enabling us to calculate some previously unknown congruences for R_n , which are listed in Figure 3.4.



Goal: *Improve our knowledge of the numbers z_n and $\omega(n, d)$.*

We develop techniques for computing $\omega(n, d)$ exactly in Sections 3.2.2 and 3.2.3. Starting with Theorem 3.2.4, we show that for each a there exists μ_a such that, on each congruence class modulo μ_a , $\omega(n, n - a)$ is determined by a polynomial of degree $2a$ in n . We give the coefficients of these polynomials for $1 \leq a \leq 6$ in Figure 3.5, and find an asymptotic formula for $\omega(n, n - a)$ as $n \rightarrow \infty$, for arbitrary fixed a in Theorem 3.2.9.

We introduce an interesting class of orthomorphism of \mathbb{Z}_n , which we call d -compound, where d divides n (defined in Section 3.3). We develop the theory of d -compound orthomorphisms and, in particular, the subclasses of compatible and polynomial orthomorphisms.

We prove that every canonical d -compound orthomorphism of \mathbb{Z}_n can be constructed uniquely from d orthomorphisms of \mathbb{Z}_t and 1 orthomorphism of \mathbb{Z}_d . This enables us to show that there are precisely $t^{d-1} z_d z_t^d$ canonical d -compound orthomorphisms of \mathbb{Z}_n .

In Corollary 3.3.7, we show that $R_{n+1} \equiv z_n \equiv -2 \pmod{n}$ for prime n and $R_{n+1} \equiv z_n \equiv 0 \pmod{n}$ for composite n . In Section 3.3.2 we improve the current knowledge of $z_n \pmod{3}$, expanding upon a result of McKay, McLeod and Wanless [221]. In Theorem 3.3.8 we provide a congruence for z_n which we use to compute $z_n \pmod{3}$ for all $n \leq 60$. Moreover, if $n \geq 5$ and $n \not\equiv 1 \pmod{3}$ then $z_n \equiv 0 \pmod{3}$. Theorem 3.3.9 states that $z_n \equiv 1 \pmod{3}$ when $n = 2 \cdot 3^k + 1$ is prime.

We develop the theory of compatible and polynomial orthomorphisms in Section 3.3.3. Let λ_n and π_n be the number of canonical compatible and canonical polynomial orthomorphisms, respectively. We find a formula for λ_n in Theorem 3.3.14 and in Theorem 3.3.15 we find necessary and sufficient conditions for $\lambda_n = \pi_n$. In Section 3.3.4 we find some new sufficient conditions for when a partial orthomorphism can be completed to an orthomorphism. In Section 3.3.5 we classify when two compound orthomorphisms are orthogonal.

Chapter 4 considers questions relating to autotopisms of Latin squares [303, 307]. In Section 4.1.1 we give an upper bound on the maximum size of an autotopism group of a Latin square. Consequently, we find an asymptotic divisor of R_n as $n \rightarrow \infty$. Specifically, Corollary 4.1.2 states that, for a fixed prime q , q^a divides R_n where $a = \frac{n}{q-1} - O(\log^2 n)$ as $n \rightarrow \infty$. Using a similar technique, we give an upper bound on the maximum number of subsquares of a Latin square in Section 4.2.

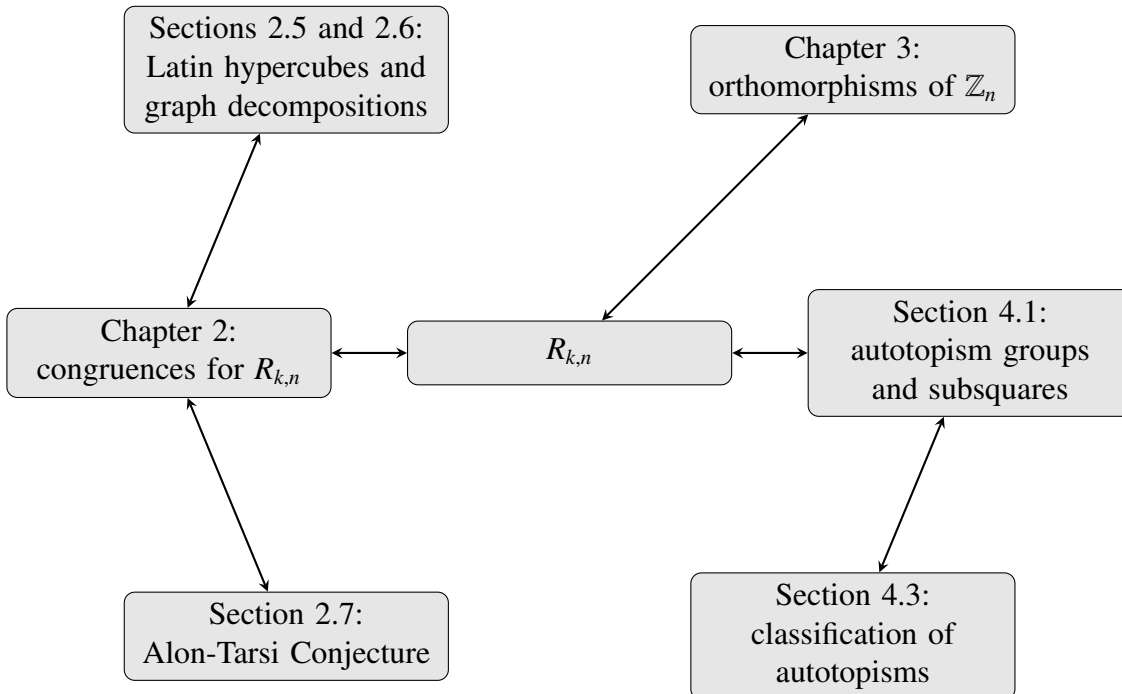


Goal: Find conditions for when an isotopism is an autotopism of some Latin square.

The remainder of Chapter 4 extends previous results classifying which isotopisms $\theta \in \mathcal{I}_n$ are autotopisms of some Latin square. For all $\theta \in \mathcal{I}_n$, let $\Delta(\theta)$ be the number of Latin squares L of order n with $\theta \in \text{Atop}(L)$. For example, Theorems 4.3.8 and 4.3.11 give strong necessary conditions for when $\Delta(\theta) > 0$. Corollary 4.3.9 is a generalisation of Lemma 1.2.8. In Section 4.3.4 we give necessary and sufficient conditions for when $\Delta(\theta) > 0$ where $\theta = (\eta, \eta, \eta) \in \mathcal{I}_n$ such that η consists of cycles of the same length and possibly some fixed points. In Section 4.3.4 we give necessary and sufficient conditions for when $\Delta(\theta) > 0$ where $\theta = (\eta, \eta, \eta) \in \mathcal{I}_n$ such that η consists of two non-trivial cycles and possibly some fixed points.

Finally, in Chapter 5 we list some interesting open problems and ideas for future research that are relevant to this thesis.

We depict the structure of this thesis below.



CHAPTER 2

Divisors of the number of Latin rectangles

We will now commence our study into congruences involving, and divisors of, the numbers $R_{k,n}$, $K_{k,n}$ and $L_{k,n}$. In the beginning of this chapter we follow the work in [308], but in Sections 2.5 and 2.6 we will expand upon this work. Afterwards, in Section 2.7 we will study congruences for the number of even and odd Latin squares, which relates to the Alon-Tarsi Conjecture, following the work of [306]. We will primarily use the symbol set $[n] = \{1, 2, \dots, n\}$. We begin with a “proof template” in Section 2.1 which aids us in finding divisors of and congruences for $R_{k,n}$ which we later apply to different combinatorial enumeration problems. We prove several results giving divisors of $R_{k,n}$. For example, in Theorems 2.2.1 and 2.2.2 we show that $(k-1)!$ divides $R_{k,n}$ when $k \leq \lfloor n/2 \rfloor$ and $\lfloor n/2 \rfloor!$ divides $R_{k,n}$ when $\lfloor n/2 \rfloor < k \leq n$. This extends a result of McKay and Wanless [225], who proved Theorem 2.2.2 for Latin squares.

Theorem 2.2.1 is then extended in Theorem 2.2.5 in the special case $n \geq 3k$. In Theorems 2.3.1 and 2.3.2, we establish recurrences that determine the congruence class of $R_{k,n} \pmod{t}$ and $K_{k,n} \pmod{t}$ for a range of different t , which yields several useful corollaries. Let p be a prime. In Corollary 2.3.3 we find a lower bound on the largest power of p dividing $R_{k,n}$ and $K_{k,n}$ when $p < k$. We can compare this lower bound to the divisors of $R_{k,n}$ in Figures A.4 and A.5, when $k \in \{4, 5\}$. In Corollary 2.3.6 we show that $R_{k,n+d} \equiv (-1)^{k-1} (k-1)! R_{k,n} R_{k,d} \pmod{d}$ if $k \leq n$. Corollary 2.3.6 generalises earlier results by Riordan [269] and Carlitz [46] who dealt with the case $k = 3$.

In Theorem 2.4.6 we find that $R_{k,n} \equiv ((-1)^{k-1} (k-1)!)^{n-1} \pmod{n}$ for all k and n . This implies that if n is prime, then $R_{k,n} \equiv 1 \pmod{n}$ for $1 \leq k \leq n$ and if n is composite then $R_{k,n} \equiv 0 \pmod{n}$ if and only if k is larger than the greatest prime divisor of n .

In Section 2.5 the proof template is used to find divisors for subsets of Latin hypercuboids, a generalisation of Latin rectangles to arbitrary dimensions. Some results are applicable to Latin squares and rectangles, which are a special class of Latin hypercuboid. Theorem 2.5.6 gives a factorial divisor of the size of a very general class of subsets of Latin hypercuboids. In Corollary 2.5.12 we prove a special case of a conjecture by Dougherty and Szczepanski [80].

In Section 2.6 we apply the template of Section 2.1 to find divisors of the number of graph factorisations. Let G denote the labelled complete graph on n vertices. We give divisors for (a) the number of one-factorisations of G in Theorem 2.6.3, (b) the number of Steiner triple

systems in Theorem 2.6.5 and (c) the number of Hamilton cycle decompositions of G in Theorem 2.6.6.

In Section 2.7 we modify the techniques developed in this chapter to be applicable to the numbers R_n^{EVEN} and R_n^{ODD} . Drisko [83] proved the $p + 1$ case, for odd prime p , of the Alon-Tarsi Conjecture. The aim of Section 2.7 is to reach Theorem 2.7.6, where we show that Drisko's method cannot be extended to include the $n + 1$ case, for composite n . Theorem 2.7.2 also gives a divisor for R_n , greater than that of Theorem 1.1.5, in some cases.

2.1 Proof template

Many of the proofs in this chapter follow the same basic strategy. We have some set of Latin rectangles C and wish to calculate $|C| \pmod{\mu}$ for some integer μ . Typically, C will be the set of reduced $k \times n$ Latin rectangles and we will often use L to denote an arbitrary Latin rectangle in C . We choose a group of isotopisms G that acts on C such that μ divides $|G|$. For each $L \in C$, let $G(L)$ denote the orbit of L under G , namely $G(L) = \{\theta(L) : \theta \in G\} \subseteq C$.

If there exist distinct $\theta_1, \theta_2 \in G$ such that $\theta_1(L) = \theta_2(L)$ then $\theta_2^{-1} \circ \theta_1 \in G$ is a non-trivial autotopism of L . Therefore if L does not admit a non-trivial autotopism in G (i.e. $|\text{Atop}(L) \cap G| = 1$) then $|G(L)| = |G| \equiv 0 \pmod{\mu}$. Hence any $L \in C$ such that $|G(L)| \not\equiv 0 \pmod{\mu}$ must admit a non-trivial autotopism in G .

We identify a subset $\mathcal{A} \subseteq C$ such that:

- \mathcal{A} contains every $L \in C$ that admits a non-trivial autotopism in G .
- \mathcal{A} is closed under the action of G .
- Members of \mathcal{A} are characterised by some special structure, usually a subrectangle in a particular position.

With \mathcal{A} satisfying these conditions, μ divides $|C \setminus \mathcal{A}|$ and hence $|C| \equiv |\mathcal{A}| \pmod{\mu}$ and $\gcd(\mu, |\mathcal{A}|)$ divides $|C|$. We then either calculate $|\mathcal{A}|$ explicitly, evaluate $|\mathcal{A}| \pmod{\mu}$ or find some divisor of $|\mathcal{A}|$. We typically do this by defining an equivalence relation on \mathcal{A} which utilises the special structure possessed by the elements of \mathcal{A} .

2.2 Factorial divisors

In this section we prove that certain factorials divide $R_{k,n}$. We use $m = \lfloor n/2 \rfloor$.

Theorem 2.2.1. $\gcd(k!, (k-1)!R_{k,n-k}R_k)$ divides $R_{k,n}$ when $k \leq m$.

Proof. This proof follows the template in Section 2.1. Let G be the group of isotopisms of the form $\theta = (\varepsilon, \beta, \beta)$ such that β fixes $[n-k]$ pointwise. Let C be the set of reduced $k \times n$ Latin rectangles and $\mu = |G| = k!$. Let $L = (l_{ij}) \in C$ and let A denote the square submatrix formed by the last k columns of L .

Suppose that L admits a non-trivial autotopism $\theta = (\varepsilon, \beta, \beta) \in G$. Let F denote the fixed points of β and $F^* = [n] \setminus F$ denote its complement. Since θ is non-trivial there exists $j \in F^*$. By Lemma 1.2.7, $l_{ij} \in F^*$ for all $1 \leq i \leq k$. Hence $|F^*| \geq k$ and so $F^* = [n] \setminus [n-k]$. By Lemma 1.2.8, A is a subsquare of L .

Let $\mathcal{A} = \{L \in C : A \text{ is a subsquare of } L\}$. Note that \mathcal{A} is closed under the action of G and hence $\gcd(k!, |\mathcal{A}|)$ divides $|C| = R_{k,n}$. By construction, $|\mathcal{A}| = R_{k,n-k}K_k = (k-1)!R_{k,n-k}R_k$, by (1.1). \square

Corollary 2.4.4 will classify when k divides R_k and it will follow that $k!$ divides $R_{k,n}$ for all composite $k \leq m$. For prime k , the largest divisor proved by Theorem 2.2.1 will be $(k-1)!$ unless k divides $R_{k,n-k}$, as it does, for example, when $n = 12$ and $k = 5$ (see Figure 1.1). Theorem 2.2.1 is extended in Theorem 2.2.5 in the special case $n \geq 3k$.

Theorem 2.2.1 provides a divisor for the number of “thin” Latin rectangles, where $k \leq m$. Next, we prove a similar result for “fat” Latin rectangles, where $m < k \leq n$, by extending the techniques that were used in [225] for the case $k = n$.

Theorem 2.2.2. *When $m < k \leq n$, $R_{k,n}$ is divisible by $m!$. If n is odd and $m+1 < k \leq n$ and $m+1$ is composite, then $(m+1)!$ divides $R_{k,n}$.*

Proof. This proof follows the template in Section 2.1. Let G be the group of isomorphisms $\theta = (\alpha, \alpha, \alpha)$ such that α fixes $\{1, 2, \dots, k-r\} \cup \{k+1, k+2, \dots, n\}$ pointwise, for some $1 \leq r < k$ to be specified later. Let C be the set of reduced $k \times n$ Latin rectangles and $\mu = |G| = r!$.

Suppose that $L = (l_{ij}) \in C$ admits a non-trivial automorphism $\theta = (\alpha, \alpha, \alpha)$ in G . Let F denote the fixed points of α and let $F^* = [n] \setminus F$ denote its complement. Since θ is non-trivial there exists $i \in F^*$. If $j \in F$ then $l_{ij} \in F^*$, by Lemma 1.2.7. Hence

$$n - r \leq |F| \leq |F^*| \leq r. \quad (2.1)$$

We now consider two choices for r .

Case I: $r = m$. This case requires $k > m$. If n is odd we contradict (2.1), so it is sufficient to choose $\mathcal{A} = \emptyset$ in order to deduce that $m!$ divides $|C|$.

Next we consider even $n = 2m$. We must have $F = \{1, 2, \dots, k-r\} \cup \{k+1, k+2, \dots, n\}$ and $F^* = \{k-r+1, k-r+2, \dots, k\}$ to satisfy (2.1). Furthermore the $m \times m$ submatrix A , formed by the rows and columns indexed by F^* , is a subsquare of L . We let $\mathcal{A} = \{L \in C : A \text{ is a subsquare of } L\}$, which is closed under the action of G .

We define the Latin rectangles equivalent to $L \in \mathcal{A}$ to be those formed by replacing A by one of the L_m Latin squares on the same symbols. Since $m!$ divides L_m by (1.1), $m!$ also divides $|\mathcal{A}|$ and hence $m!$ divides $|C| = R_{k,n}$.

Case II: Odd $n = 2m+1$ and $r = m+1$. This case requires $k > m+1$. By (2.1) and since $|F| + |F^*| = n$, we must have $|F^*| = m+1$ and $|F| = m$. Let A denote the $(m+1) \times (m+1)$ submatrix of L formed by the rows and columns indexed by F^* , and let B denote the $(m+1) \times m$ submatrix formed by the remainder of the entries in those rows.

The submatrix B contains only symbols in F^* and therefore A contains one symbol from F^* in each row. Furthermore, A contains one symbol from F^* in each column, otherwise there exists a column of A without a symbol from F^* , contradicting $|F| = m$. Let $\mathcal{A} \subseteq C$ be the set of Latin rectangles with submatrices A and B of this description. Note that \mathcal{A} is closed under the action of G .

We define two Latin rectangles $L_1, L_2 \in \mathcal{A}$ to be equivalent if:

- The first $k-r$ rows are identical in L_1 and L_2 and

- For each column c the set of symbols which occur in c is the same for L_1 and L_2 .

We will now enumerate the Latin rectangles equivalent to any given $L \in \mathcal{A}$. Let D denote the set of cells of A that contain a symbol in F^* . We can replace A by one of K_{m+1} Latin squares of order $m+1$ on the symbols $\{0\} \cup F$ such that the zeroes occur in the cells in D . We then restore the original contents of D .

Irrespective of the previous replacements, we now can replace B by the transpose of one of the $K_{m,m+1} = K_{m+1}$ normalised $m \times (m+1)$ Latin rectangles on the same symbols. Then we replace the symbols in D appropriately so that the set of symbols in each row is $[n]$, which is a unique replacement. Then we permute the columns of A so that the set of symbols in each column is the same as in L , for which there is a unique permutation.

Therefore L is equivalent to K_{m+1}^2 Latin rectangles. Hence K_{m+1}^2 divides $|\mathcal{A}|$ and so $\gcd(\mu, K_{m+1}^2)$ divides $|C| = R_{k,n}$. Therefore by (1.1), $\gcd((m+1)!, m!^2)$ divides $R_{k,n}$. Note that $m!$ is divisible by $m+1$ unless $m+1$ is prime or $m+1 = 4$. In the latter case $n = 2m+1 = 7$ and Figure 1.2 implies that $R_{5,7}$ and $R_{6,7} = R_{7,7}$ are divisible by $4!$. \square

In Figure 2.1 we compare the results of Theorems 2.2.1 and 2.2.2 with the greatest factorial divisor of $R_{k,n}$ from the known data, listed in Figure 1.2. We omit $R_{1,n} = 1$ and $R_n = R_{n-1,n}$. Let $\psi = \psi(k, n)$ denote the greatest integer such that $\psi!$ divides $R_{k,n}$. Theorems 2.2.1 (dark) and 2.2.2 (light) provide a lower bound on ψ . For $n \leq 11$ this bound is the actual value of ψ , except for the entries marked with an asterisk, where Theorem 2.2.2 only proves that $(\psi - 1)!$ divides $R_{k,n}$.

McKay and Wanless [225] also showed that $7!$ divides R_{13} , which is the first case when $n = 2m+1$ such that $m+1$ is prime and $(m+1)!$ divides R_n . Judging from the results in Figure 2.1, it would not be surprising if $9!$ divides R_{13} , in which case Theorem 2.2.2 (which gives the divisor $6!$ of R_{13}) is well short of best possible.

We later show, in Figure 3.4 on page 76, that 11 does not divide R_{13} , which gives an upper bound on the maximum factorial divisor. In fact, Figures 2.1 and 3.4 together show that 11 does not divide R_n for all $n \leq 21$ whereas Theorem 2.2.2 implies that 11 divides R_n for all $n \geq 22$.

Corollary 2.2.3. *If n is composite and $k > m$ then n divides $R_{k,n}$.*

Proof. Since n is composite, $n = \lambda q$ for some prime $q \leq m$ and $2 \leq \lambda \leq m$. By Theorem 2.2.2, $m!$ divides $R_{k,n}$ and therefore $R_{k,n} \equiv 0 \pmod{n}$ except possibly when $\lambda = q$ and $m < 2q$. If $n = q^2$, then $m = \lfloor q^2/2 \rfloor < 2q$ only if $q = 2$ or 3 , that is when $n = 4$ or 9 , and these cases are resolved by Figure 2.1. \square

We determine when n divides $R_{k,n}$ in Corollary 2.4.5 and in Theorem 2.4.6 we give a formula for $R_{k,n} \pmod{n}$ for all $k, n \in \mathbb{N}$.

Corollary 2.2.4. *If k is composite then k divides $R_{k,n}$.*

Proof. Case I: $k \leq m$. Theorem 2.2.1 implies that $\gcd(k!, (k-1)!R_k)$ divides $R_{k,n}$. When $k = 4$, $R_4 = 4$ divides $R_{4,n}$ and when $k > 4$, k divides $(k-1)!$, since k is composite. Therefore k divides $R_{k,n}$ when $k \leq m$.

Case II: $m < k \leq n$. Theorem 2.2.2 implies that k divides $R_{k,n}$ except possibly when $k = p^2$ for some prime $p > m/2$. But then $2p > m = \lfloor n/2 \rfloor \geq \lfloor p^2/2 \rfloor$, which can only be satisfied in the following cases that are resolved by Figure 2.1: when $k = 4$ and $n \in \{4, 5, 6, 7\}$, and when $k = 9$ and $n \in \{9, 10, 11\}$. \square

n, k	$R_{k,n}$	ψ
3, 2	1	1
4, 2	3	1
3	2^2	2
5, 2	11	1
3	$2 \cdot 23$	2
4	$2^3 \cdot 7$	2
6, 2	53	1
3	$2^3 \cdot 7 \cdot 19$	2
4	$2^3 \cdot 3^2 \cdot 7 \cdot 13$	4^*
5	$2^6 \cdot 3 \cdot 7^2$	4^*
7, 2	$3 \cdot 103$	1
3	$2^4 \cdot 2237$	2
4	$2^5 \cdot 3 \cdot 19 \cdot 709$	4^*
5	$2^8 \cdot 3 \cdot 5^2 \cdot 587$	5^*
6	$2^{10} \cdot 3 \cdot 5 \cdot 1103$	5^*
8, 2	$13 \cdot 163$	1
3	$2^6 \cdot 26153$	2
4	$2^6 \cdot 3 \cdot 159 \cdot 14713$	4
5	$2^{11} \cdot 3 \cdot 23 \cdot 192529$	4
6	$2^{11} \cdot 3 \cdot 7 \cdot 173 \cdot 45077$	4
7	$2^{17} \cdot 3 \cdot 1361291$	4

n, k	$R_{k,n}$	ψ
9, 2	$11 \cdot 37 \cdot 41$	1
3	$2^5 \cdot 13 \cdot 167 \cdot 1489$	2
4	$2^7 \cdot 3^4 \cdot 20025517$	4
5	$2^{11} \cdot 3^4 \cdot 13 \cdot 52251029$	4
6	$2^{14} \cdot 3^5 \cdot 3253351007$	4
7	$2^{15} \cdot 3^2 \cdot 61 \cdot 12923 \cdot 965171$	4
8	$2^{21} \cdot 3^2 \cdot 5231 \cdot 3824477$	4
10, 2	$3^2 \cdot 16481$	1
3	$2^6 \cdot 23 \cdot 61 \cdot 90821$	2
4	$2^8 \cdot 3^3 \cdot 71 \cdot 271 \cdot 1106627$	4
5	$2^{16} \cdot 3^6 \cdot 19 \cdot 97 \cdot 8483617$	4
6	$2^{14} \cdot 3^3 \cdot 5 \cdot 26053 \cdot 15110358097$	6^*
7	$2^{20} \cdot 3^3 \cdot 5 \cdot 509 \cdot 2458531126109$	6^*
8	$2^{21} \cdot 3^3 \cdot 5 \cdot 11 \cdot 13^2 \cdot 37 \cdot 1381 \cdot 159597187$	6^*
9	$2^{28} \cdot 3^2 \cdot 5 \cdot 31 \cdot 37 \cdot 1468457 \cdot 547135293937$	6^*
11, 2	1468457	1
3	$2^7 \cdot 13 \cdot 23 \cdot 20851549$	2
4	$2^{10} \cdot 3^2 \cdot 1823 \cdot 8569184461$	4
5	$2^{13} \cdot 3^2 \cdot 29 \cdot 168293 \cdot 20936295857$	4
6	$2^{17} \cdot 3^2 \cdot 5 \cdot 31 \cdot 2334139 \cdot 225638611943$	6^*
7	$2^{21} \cdot 3^2 \cdot 5 \cdot 9437 \cdot 269623520098467133$	6
8	$2^{28} \cdot 3^2 \cdot 5 \cdot 97 \cdot 73488673152815765447$	6
9	$2^{32} \cdot 3^3 \cdot 5 \cdot 61 \cdot 7487 \cdot 260951 \cdot 42053669617$	6
10	$2^{35} \cdot 3^4 \cdot 5 \cdot 2801 \cdot 2206499 \cdot 62368028479$	6

FIGURE 2.1: Prime factorisation of $R_{k,n}$ for $2 \leq k < n \leq 11$ and the greatest integer ψ such that $\psi!$ divides $R_{k,n}$.

The converse of Corollary 2.2.4 is false. For example, $R_{5,7} = 11270400 \equiv 0 \pmod{5}$. The following theorem extends Theorem 2.2.1 in the special case $n \geq 3k$.

Theorem 2.2.5. *Suppose $k, n, r \in \mathbb{N}$ where $n \geq 2k + r$ and $k \leq r < 2k$. Then $(k-1)!$ divides $R_{k,n}$ where P denotes the product of all composite numbers c such that $k \leq c \leq r$.*

Proof. This proof follows the template in Section 2.1. Let G be the group of isotopisms of the form $\theta = (\varepsilon, \beta, \beta)$ such that β fixes $[n-r]$ pointwise. Let C be the set of reduced $k \times n$ Latin rectangles and $\mu = (k-1)!$.

Suppose that $L \in C$ admits a non-trivial autotopism $\theta = (\varepsilon, \beta, \beta) \in G$. Let A denote the submatrix formed by the last r columns of L . Lemma 1.2.8 implies that the columns of L whose indices are fixed by β form a subrectangle of L . Consequently, the columns of L whose indices are not fixed by β form a $k \times i$ subrectangle of L in A for some $k \leq i \leq r$.

For all $k \leq i \leq r$, let $\mathcal{A}_i = \{L \in C : A \text{ contains a } k \times i \text{ subrectangle of } L\}$ and let $\mathcal{A} = \cup_i \mathcal{A}_i$. Note that each \mathcal{A}_i is closed under the action of G and so $|C| \equiv |\mathcal{A}| \pmod{\mu}$. Since $r < 2k$, the \mathcal{A}_i are disjoint and so $|\mathcal{A}| = \sum_{k \leq i \leq r} |\mathcal{A}_i|$.

By construction

$$|\mathcal{A}_i| = \binom{r}{i} K_{k,i} R_{k,n-i} = \frac{r!}{i(r-i)!(i-k)!} R_{k,i} R_{k,n-i},$$

by (1.1).

Since $n \geq 2k + r \geq 2k + i$ for all $k \leq i \leq r$, we find $k \leq \lfloor (n-i)/2 \rfloor$. Therefore by Theorem 2.2.1, $(k-1)!$ divides $R_{k,n-i}$ and we know that $(r-i)!(i-k)!$ divides $(r-k)!$ which divides $(k-1)!$ since $r < 2k$.

If i is prime then μ divides $r!/i$, since $k \leq i \leq r$, and so μ divides $|\mathcal{A}_i|$. If i is composite, then i divides $R_{k,i}$ by Corollary 2.2.3 since $i \leq r < 2k$, and therefore $r!$ divides $|\mathcal{A}_i|$.

Hence μ divides $|\mathcal{A}_i|$ for all $k \leq i \leq r$ and so $R_{k,n} = |C| \equiv |\mathcal{A}| = \sum_{k \leq i \leq r} |\mathcal{A}_i| \equiv 0 \pmod{\mu}$. \square

2.3 Recurrence congruences

In this section we establish congruences for $R_{k,n}$ and $K_{k,n}$ modulo t for a range of $t \in \mathbb{N}$. With the results presented in this section, we use the convention that $R_{k,n} = K_{k,n} = 0$ whenever $n < k$. We will also use the following notation throughout this section. Let $n = b_0 + b_1 + \dots + b_s$ be a partition of the integer n where $s \geq 1$. Let $t = \prod_{1 \leq i \leq s} b_i$ and $t' = b_0 t$. For any $I \subseteq \{0, 1, \dots, s\}$, let $\|I\| = \sum_{i \in I} b_i$. Let Q be the set of partitions of the set $\{0, 1, \dots, s\}$ into at least two parts. For $U \in Q$, define $u_0 = u_0(U)$ to be the part of U containing 0. For any integer $r \geq 2$, let $\text{gpd}(r)$ denote the greatest prime divisor of r .

Theorem 2.3.1. *If $b_0 \geq k$ then*

$$R_{k,n} \equiv \sum_{U \in Q} (-1)^{|U|} (|U| - 1)! R_{k, \|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k, \|u\|} \pmod{t}.$$

Proof. This proof follows the template in Section 2.1. Let C be the set of reduced $k \times n$ Latin rectangles and let $L \in C$.

Let $b_0^* = 0$ and for $1 \leq i \leq s$, let $b_i^* = b_{i-1}^* + b_{i-1}$. Let M_i be the submatrix of L consisting of the b_i columns $b_i^* + 1, b_i^* + 2, \dots, b_i^* + b_i$.

Suppose $U \in Q$. If, for each $u \in U$, the submatrix $\cup_{j \in u} M_j$ is a subrectangle of L , then we say L is U -decomposable and that U is a *decomposition* of L . For all $U, V \in Q$ we write $V \triangleleft U$ and $U \triangleright V$ whenever V is a refinement of U and $V \neq U$. Call U an *irreducible* decomposition of L if there does not exist $V \triangleleft U$ such that L is V -decomposable. For all $U \in Q$, let $\mathcal{A}_U = \{L \in C : U \text{ is an irreducible decomposition of } L\}$. Let $\mathcal{A} = \cup_{U \in Q} \mathcal{A}_U$.

Define the b_i -cycle $\beta_i = (b_i^* + 1, b_i^* + 2, \dots, b_i^* + b_i)$. Let G be the group of order t generated by the isotopisms $(\varepsilon, \beta_i, \beta_i)$ for $1 \leq i \leq s$. Since $k \leq b_0$, G acts on C . Suppose $L \in C$ admits a non-trivial autotopism $\theta \in G$. Lemma 1.2.8 implies that the columns fixed by θ form a subrectangle of L and hence $L \in \mathcal{A}$. Note that \mathcal{A}_U is closed under the action of G for all $U \in Q$ and hence $R_{k,n} = |C| \equiv |\mathcal{A}| \pmod{t}$.

The key observation is that every $L \in \mathcal{A}$ admits exactly one irreducible decomposition. Therefore $\{\mathcal{A}_U\}_{U \in Q}$ partitions \mathcal{A} and so $|\mathcal{A}| = \sum_{U \in Q} |\mathcal{A}_U|$, giving

$$R_{k,n} \equiv \sum_{U \in Q} |\mathcal{A}_U| \pmod{t}.$$

In order to count $|\mathcal{A}_U|$, we first count the total number of U -decomposable $L \in \mathcal{A}_U$, which is $R_{k, \|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k, \|u\|}$ and then subtract the number of $L \in \mathcal{A}$ that have some irreducible decomposition $V \triangleleft U$ of L , giving

$$|\mathcal{A}_U| = R_{k, \|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k, \|u\|} - \sum_{V \triangleleft U} |\mathcal{A}_V|. \quad (2.2)$$

By repeated use of (2.2) we obtain

$$\sum_{U \in Q} |\mathcal{A}_U| = \sum_{U \in Q} c_U R_{k, \|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k, \|u\|}$$

for integers c_U . We next show that $c_U = (-1)^{|U|}(|U| - 1)!$ by induction on $|U|$. If $|U| = 2$ then $c_U = 1$ by (2.2) since $V \triangleleft U$ implies $|V| > |U|$. Now assume that $c_W = (-1)^{|W|}(|W| - 1)!$ for all $W \triangleright U$. By (2.2),

$$c_U = 1 - \sum_{W \triangleright U} c_W = 1 - \sum_{i=2}^{|U|-1} (-1)^i (i-1)! S_2(|U|, i)$$

where $S_2(\cdot, \cdot)$ denotes the Stirling number of the second kind. The identity $\sum_{i=1}^{|U|} (-1)^i (i-1)! S_2(|U|, i) = 0$ then gives $c_U = (-1)^{|U|}(|U| - 1)!$. \square

It is possible to provide a similar proof for normalised $k \times n$ Latin rectangles. Since the proof is analogous, it is omitted.

Theorem 2.3.2.

$$K_{k,n} \equiv \sum_{U \in Q} (-1)^{|U|}(|U| - 1)! \prod_{u \in U} K_{k, \|u\|} \pmod{t'}.$$

Theorems 2.3.1 and 2.3.2 provide numerous interesting corollaries, which we will now present.

Corollary 2.3.3. *Suppose p is prime and $n \in \mathbb{N}$. If $d \geq k > p$ then $p^{\lfloor n/p \rfloor}$ divides $R_{k,n+d}$ and $K_{k,n}$.*

Proof. When $n < p$, $R_{k,n+d}$ and $K_{k,n}$ are both divisible by $p^{\lfloor n/p \rfloor} = 1$, so assume $n \geq p$ and hence $a := \lfloor n/p \rfloor \geq 1$. Choose $b_0 = n - sp$ and $b_1 = b_2 = \dots = b_s = p$ where $s = a - 1$ if p divides n and $s = a$ otherwise. By Theorem 2.3.2 and induction on n , $K_{k,n} \equiv 0 \pmod{p^a}$. Similarly, $R_{k,n+d} \equiv 0 \pmod{p^a}$ follows from Theorem 2.3.1, if we instead use $b_0 = n + d - ap \geq k$. \square

For fixed k , Corollary 2.3.3 implies that for any prime $p < k$ the largest $x \in \mathbb{N}$ such that p^x divides $R_{k,n}$ increases at least linearly with n . This can be compared with the data in Appendix A.3 when $k \in \{4, 5\}$.

Corollary 2.3.4. *Let $d, k, n \in \mathbb{N}$ be such that $d \geq k > \text{gpd}(n)$. Then n divides $R_{k,n+d}$ and $K_{k,n}$.*

Proof. Note that $R_{k,n+d} \equiv R_{k,d}K_{k,n} \pmod{n}$ by Theorem 2.3.1. Since $k > \text{gpd}(n)$, if n is prime then $K_{k,n} = 0$ and hence $R_{k,n+d} \equiv 0 \pmod{n}$. So assume n is composite. If p^x divides n , for some $x \in \mathbb{N}$ and prime p , then $p^{n/p}$ divides $R_{k,n+d}$ and $K_{k,n}$, by Corollary 2.3.3. However, $n/p \geq p^{x-1} \geq x$ if $x \geq 2$ and $n/p \geq x$ if $x = 1$. Hence p^x divides $p^{n/p}$ which in turn divides $K_{k,n}$ and $R_{k,n+d}$. The result follows since p^x was an arbitrary prime power divisor of n . \square

A complete determination of when n divides $R_{k,n}$ is given later, in Corollary 2.4.5.

Corollary 2.3.5. *If $k > \text{gpd}(t')$ then $K_{k,n} \equiv 0 \pmod{t'}$ and if $b_0 \geq k > \text{gpd}(t)$ then $R_{k,n} \equiv 0 \pmod{t}$.*

Proof. The result follows from Theorems 2.3.1 and 2.3.2 by induction on s . Note that if $s = 1$ then $R_{k,n} \equiv R_{k,b_0}K_{k,b_1} \equiv 0 \pmod{t}$ and $K_{k,n} \equiv K_{k,b_0}K_{k,b_1} \equiv 0 \pmod{t'}$, using Corollary 2.3.4. \square

We can use Theorem 2.3.1 and Corollary 2.3.5 repeatedly with the same values of k and n but with various partitions of n . For example, suppose we seek congruences involving $R_{6,20}$. There are various sequences $(b_i)_{i=0}^s$ with $s \geq 1$ that satisfy $b_0 \geq 6$ and $n = \sum_{i=0}^s b_i = 20$, but produce different values of t . The order of the subsequence $(b_i)_{i=1}^s$ does not affect the outcomes of Theorem 2.3.1 and Corollary 2.3.5. Also, there is little advantage in choosing a composite b_i when $i \geq 1$, since a composite term can be replaced by its prime factorisation and b_0 and s increased accordingly to preserve $n = \sum_{0 \leq i \leq s} b_i$. In Figure 2.2, we choose the subsequence $(b_i)_{i=1}^s$ to be a single prime repeated s times. See Figure 2.1 for the values of $R_{k,n}$ for $1 \leq n \leq 11$. We also use the value of $R_{6,13}$ given in Section 1.3.1. Recall that $K_{k,n} = (n-1)!R_{k,n}/(n-k)!$ by (1.1).

In the case of powers of 5 dividing $R_{6,20}$, we can actually prove a larger divisor by using Theorem 2.3.2 rather than Theorem 2.3.1. When $(b_i)_{i=0}^s = (5, 5, 5, 5)$, Theorem 2.3.2 gives $K_{6,20} \equiv 0 \pmod{5^4}$ and so $360R_{6,20} \equiv 0 \pmod{5^4}$ by (1.1). Therefore $R_{6,20} \equiv 0 \pmod{5^3}$. When combined with the congruences in Figure 2.2, this establishes that $R_{6,20} \equiv 2903040000 \pmod{9081072000}$, by the Chinese Remainder Theorem.

A quirk of Corollary 2.3.5 is that, for a given n , it provides an increasing prime power divisor of $R_{k,n}$ with decreasing k . For example, it implies that $R_{7,11} \equiv R_{6,11} \equiv 0 \pmod{2^2}$, $R_{5,11} \equiv R_{4,11} \equiv 0 \pmod{2^3}$ and $R_{3,11} \equiv 0 \pmod{2^4}$. In Figure 2.1, the greatest power of 2 dividing $R_{k,n}$ usually increases with k , although $R_{6,10}$ is an exception.

The following is a special case of Theorem 2.3.1, using (1.1).

$(b_i)_{i=0}^s$	Congruence for $R_{6,20}$
$(6, 2, 2, 2, 2, 2, 2)$	$0 \pmod{2^7}$
$(8, 3, 3, 3, 3)$	$0 \pmod{3^4}$
$(10, 5, 5)$	$0 \pmod{5^2}$
$(6, 7, 7)$	$R_{6,6}K_{6,14} + 2R_{6,13}K_{6,7} - 2R_{6,6}K_{6,7}^2 \equiv 14 \pmod{7^2}$
$(9, 11)$	$R_{6,9}K_{6,11} \equiv 3 \pmod{11}$
$(7, 13)$	$R_{6,7}K_{6,13} \equiv 3R_{6,13} \equiv 3 \pmod{13}$

FIGURE 2.2: Congruences for $R_{6,20}$ implied by Theorem 2.3.1.

Corollary 2.3.6. *If $k \leq n$ then $R_{k,n+d} \equiv (-1)^{k-1}(k-1)!R_{k,n}R_{k,d} \pmod{d}$ for all $d \in \mathbb{N}$.*

In particular, Corollary 2.3.6 implies the following.

Corollary 2.3.7. *If $k \leq n$ and d divides $R_{k,n}$ then d divides $R_{k,n+d}$.*

Upon inspection of Figure 2.1 we see that $R_{3,n}$ is indivisible by 3 for $3 \leq n \leq 5$ and indivisible by 5 for $3 \leq n \leq 7$. Therefore Corollary 2.3.6 implies that 3 and 5 do not divide $R_{3,n}$ for any $n \geq 3$. In this way, Corollary 2.3.6 can be used to also discover indivisibility properties of $R_{k,n}$. In fact, the primes $p < 100$ that do not divide $R_{3,n}$ for all $n \geq 3$ are $p \in \{3, 5, 11, 29, 37, 41, 43, 53, 67, 79, 83, 97\}$, which were found using (1.12) and Corollary 2.3.6.

In the next section we will see that Corollary 2.3.6 generalises the congruence $R_{3,n+t} \equiv 2^t R_{3,n} \pmod{t}$ for all $t \geq 1$ by Carlitz [46] (see also [269]).

2.4 Modulo n

We turn our attention to the value of $R_{k,n} \pmod{n}$, which is listed in Figure 2.3 for small values of k and n . For $n \leq 11$ the values of $R_{k,n}$ have been explicitly calculated (see Figure 1.2), while $R_{k,n}$ for $k \leq 5$ can be enumerated by (1.16) (see also Appendix A.3). The remaining values are established later, in Theorem 2.4.6.

Our first theorem for this section shows that the $k = 3$ case of Corollary 2.3.6 includes the congruences of Riordan [269] and Carlitz [46].

Theorem 2.4.1.

- For $n \geq 2$, $R_{2,n} \equiv (-1)^{n-1} \pmod{n}$ and $R_{2,n}$ is odd.
- For $n \geq 3$, $R_{3,n} \equiv 2^{n-1} \pmod{n}$ and $R_{3,n} \equiv 2^{n-1}(1 - n - n^2) \pmod{3}$.

Proof. By (1.11), $R_{2,n} \equiv -D_n = -n! \sum_{i=0}^n (-1)^i / i! \equiv (-1)^{n-1} \pmod{n}$. Euler [98] proved the recurrence $D_n = (n-1)(D_{n-1} + D_{n-2})$ with $D_1 = 0$ and $D_2 = 1$. Therefore $D_n \equiv 0 \pmod{2}$ for odd n and by induction, $D_n \equiv 1 \pmod{2}$ for even n . Hence $R_{2,n} = D_n / (n-1) = D_{n-1} + D_{n-2} \equiv 1 \pmod{2}$.

The summands in (1.12) are integer multiples of n except possibly for when $n-2 \leq k \leq n$, which is when $(i, j, k) \in \{(0, 0, n), (1, 0, n-1), (0, 1, n-1), (2, 0, n-2), (1, 1, n-2), (0, 2, n-2)\}$. Hence

$$R_{3,n} \equiv \frac{2^{n-1}}{(n-1)(n-2)}(2 + n - 3n) + \frac{2^{n-2}n}{n-2}(2 - 6 + 6) = 2^{n-1} \pmod{n}.$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$k = 1$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2		1	1	3	1	5	1	7	1	9	1	11	1	13	1	15	1	17	1	19	1	21
3			1	0	1	2	1	0	4	2	1	8	1	2	4	0	1	14	1	8	4	2
4				0	1	0	1	0	0	4	1	0	1	8	6	0	1	0	1	4	15	16
5					1	0	1	0	0	4	1	0	1	10	6	0	1	0	1	4	9	2
6						0	1	0	0	0	1	0	1	6	0	0	1	0	1	0	15	12
7							1	0	0	0	1	0	1	6	0	0	1	0	1	0	15	16
8								0	0	0	1	0	1	0	0	0	1	0	1	0	0	20
9									0	0	1	0	1	0	0	0	1	0	1	0	0	16
10										0	1	0	1	0	0	0	1	0	1	0	0	10
11											1	0	1	0	0	0	1	0	1	0	0	10
12												0	1	0	0	0	1	0	1	0	0	0

FIGURE 2.3: Values of $R_{k,n} \pmod n$ for some small values of k and n .

The summands in (1.12) are integer multiples of 3 except possibly for when $n - 2 \leq k \leq n$ or $(i, j, k) \in \{(0, 3, n - 3), (1, 3, n - 4)\}$. Similarly to the modulo n case, this yields $R_{3,n} \equiv 2^{n-1} - 2^{n-3}10n - 2^{n-4}56n(n - 3) \equiv 2^{n-1}(1 - n - n^2) \pmod 3$. \square

We now make an interesting observation, that will lead to the evaluation of $R_{k,p} \pmod p$ for all primes p , in Theorem 2.4.3.

Lemma 2.4.2. *Let p be a prime, and let $Z_{k,p}$ denote the number of reduced $k \times p$ Latin rectangles that are isotopic to a subrectangle of the Cayley table of \mathbb{Z}_p . Then $Z_{k,p} = (p - 2)!$ when $1 < k \leq p$.*

Proof. Each reduced $2 \times p$ Latin rectangle L can be interpreted as a permutation σ_L in 2-row format. It is easy to show that L is isotopic to a subrectangle of \mathbb{Z}_p if and only if σ_L is a p -cycle. There are $(p - 2)!$ different p -cycles that map 1 to 2, therefore $Z_{2,p} = (p - 2)!$.

Let $\text{Atop}(\mathbb{Z}_p)$ be the autotopism group of the Cayley table of \mathbb{Z}_p . The autotopism group of the Cayley table of a finite group has been described by, for example, Bailey [13]. As a corollary $|\text{Atop}(\mathbb{Z}_p)| = p^2(p - 1)$ and so

$$Z_{p,p} = \frac{(p!)^3}{p!(p - 1)!|\text{Atop}(\mathbb{Z}_p)|} = (p - 2)!.$$

Each reduced $k \times p$ Latin rectangle isotopic to a subrectangle of the Cayley table of \mathbb{Z}_p can easily be extended to a $(k + 1) \times p$ such Latin rectangle. Hence

$$(p - 2)! = Z_{2,p} \leq Z_{3,p} \leq \cdots \leq Z_{p,p} = (p - 2)!,$$

from which the result follows. \square

Theorem 2.4.3. *Let p be a prime and $1 \leq k \leq p$. Then $R_{k,p} \equiv 1 \pmod p$.*

Proof. It will be assumed that $k > 1$ since $R_{1,p} = 1$. Let G be the group of isotopisms generated by $(\varepsilon, \beta, \beta)$ where $\beta = (1, 2, \dots, p)$. Our proof follows the basic template in Section 2.1,

except that G acts on the set of normalised $k \times p$ Latin rectangles, while we choose C to be the set of reduced $k \times p$ Latin rectangles.

For any isotopy class I , let $\text{Norm}(I)$ be the number of normalised Latin rectangles in I and let $\text{Red}(I)$ be the number of reduced Latin rectangles in I . Then $\text{Norm}(I) = \text{Red}(I)(p-1)!/(p-k)!$. If $|\text{Atop}(L) \cap G| = 1$ for all normalised $L \in I$, then p divides $\text{Norm}(I)$ and so p also divides $\text{Red}(I)$. Let \mathcal{A} be the set of reduced $k \times p$ Latin rectangles that are isotopic to a Latin rectangle that admits a non-trivial autotopism in G . Hence $R_{k,p} = |C| \equiv |\mathcal{A}| \pmod{p}$.

If a Latin rectangle L admits a non-trivial autotopism in G , then $(\varepsilon, \beta, \beta)$ is an autotopism of L , since p is prime. Therefore, in each row of L the symbols occur in cyclic order, so L is isotopic to a subrectangle of the Cayley table of \mathbb{Z}_p . So \mathcal{A} is precisely the set of reduced $k \times p$ Latin rectangles that are isotopic to a subrectangle of the Cayley table of \mathbb{Z}_p . By Lemma 2.4.2 and Wilson's Theorem $|\mathcal{A}| = Z_{k,p} = (p-2)! \equiv 1 \pmod{p}$. \square

Theorem 2.4.3 and Corollary 2.3.6 imply that $R_{k,n+p} \equiv (-1)^{k-1}(k-1)!R_{k,n} \pmod{p}$ for prime $p \geq k$. Together Theorem 2.4.3 and Corollary 2.2.3 show the surprising fact that $R_n \pmod{n}$ is an indicator variable for primality of n .

Corollary 2.4.4. $R_n \equiv 0 \pmod{n}$ for composite n and $R_n \equiv 1 \pmod{n}$ for prime n .

Corollaries 2.3.6 and 2.4.4 imply that $R_{k,n+k} \equiv -R_{k,n} \pmod{k}$, when $n \geq k$. Hence $R_{p,\lambda p} \equiv (-1)^{\lambda-1} \pmod{p}$ for any prime p and $\lambda \geq 1$, by Theorem 2.4.3.

Corollary 2.4.5. $R_{k,n} \equiv 0 \pmod{n}$ if and only if $k > \text{gpd}(n)$.

Proof. Let $q = \text{gpd}(n)$. If $n = q$ then Theorem 2.4.3 says that $R_{k,q} \equiv 1 \not\equiv 0 \pmod{q}$ for all $1 \leq k \leq q = n$. So assume $n = \lambda q$ where $\lambda \geq 2$. By Theorem 2.4.3 and repeated application of Corollary 2.3.6, $R_{k,n} \equiv (-1)^{(\lambda-1)(k-1)}(k-1)!^{\lambda-1} \pmod{q}$. If $k \leq q$ this congruence is non-zero, so $R_{k,n} \not\equiv 0 \pmod{n}$.

Conversely we will show that $R_{k,n} \equiv 0 \pmod{n}$ when $k > q$. The $m < k \leq n$ case is precisely Corollary 2.2.3, so assume $q < k \leq m$.

Suppose p^x is a prime power divisor of n . If $x = 1$ then Corollary 2.3.6 implies that $R_{k,n} \equiv (-1)^{k-1}(k-1)!R_{k,n-p}R_{k,p} \equiv 0 \pmod{p}$, since $p < k$. So assume $x \geq 2$. If $n \geq 2px$ then $n \geq m+px \geq k+px$ and so Corollary 2.3.3 implies that $R_{k,n} \equiv 0 \pmod{p^x}$. But $n \geq p^x \geq 2px$ for all n except $n \in \{4, 8, 9\}$. These cases are resolved by Figure 2.1. \square

We now give an exact formula for $R_{k,n} \pmod{n}$ for all $k, n \in \mathbb{N}$, which even includes when $k > n$ where $R_{k,n} = 0$.

Theorem 2.4.6. If $k, n \in \mathbb{N}$, then $R_{k,n} \equiv ((-1)^{k-1}(k-1)!)^{n-1} \pmod{n}$.

Proof. Let $a = (-1)^{k-1}(k-1)!$. We want to show that $R_{k,n} \equiv a^{n-1} \pmod{n}$. If $k > n$, then $R_{k,n} = 0 \equiv a^{n-1} \pmod{n}$, so assume $k \leq n$.

Let $x, y \in \mathbb{N}$ be such that $\text{gcd}(x, y) = 1$ and $R_{k,x} \equiv a^{x-1} \pmod{x}$ and $R_{k,y} \equiv a^{y-1} \pmod{y}$. By Theorem 2.3.1, $R_{k,xy} \equiv aR_{k,x(y-1)}R_{k,x} \equiv a^2R_{k,x(y-2)}R_{k,x}^2 \equiv \dots \equiv a^{y-1}R_{k,x}^y \equiv a^{y-1}a^{y(x-1)} \equiv a^{xy-1} \pmod{x}$. By symmetry, $R_{k,xy} \equiv a^{xy-1} \pmod{y}$. Since x and y are coprime, $R_{k,xy} \equiv a^{xy-1} \pmod{xy}$. Observe that this argument is still valid even if k is greater than x or y . It is therefore sufficient to show that

$$R_{k,p^s} \equiv a^{p^s-1} \pmod{p^s}$$

for an arbitrary prime p and all $s \in \mathbb{N}$.

If $k > p$ then Corollary 2.4.5 implies that

$$R_{k,p^s} \equiv 0 \equiv a^{p^s-1} \pmod{p^s}.$$

Therefore assume $k \leq p$. Observe that $K_{k,p^s} \equiv aR_{k,p^s} \pmod{p^s}$ by (1.1). It is sufficient to show that $K_{k,p^s} \equiv a^{p^s} \pmod{p^s}$ since p does not divide a .

When $s = 1$, Theorem 2.4.3 and Fermat's Little Theorem imply that $K_{k,p} \equiv a \equiv a^{p^s} \pmod{p}$. Now, for the sake of induction, assume $K_{k,p^{s-1}} \equiv a^{p^{s-1}} \pmod{p^{s-1}}$. By applying Theorem 2.3.2 we find that

$$K_{k,p^s} \equiv K_{k,p^s-p^{s-1}}K_{k,p^{s-1}} \equiv K_{k,p^s-2p^{s-1}}K_{k,p^{s-1}}^2 \equiv \cdots \equiv K_{k,p^{s-1}}^p \equiv (cp^{s-1} + a^{p^{s-1}})^p \pmod{p^s}$$

for some integer c . Using the Binomial Theorem, $K_{k,p^s} \equiv a^{p^s} \pmod{p^s}$. \square

Theorem 2.4.6 implies that the converse of Theorem 2.4.3 is false, since $R_{5,25} \equiv 1 \pmod{25}$ for example (the exact value of $R_{5,25}$ is given in Appendix A.3). Furthermore, if n is a Carmichael number and p is the smallest prime that divides n then $R_{k,n} \equiv 1 \pmod{n}$ for $1 \leq k \leq p$.

It would also be interesting to find a formula for $R_{k,n} \pmod{k}$. We know $R_{k,n} \equiv 0 \pmod{k}$ when k is composite by Corollary 2.2.4 and $R_{2,n} \equiv 1 \pmod{2}$ by Theorem 2.4.1. For odd prime k , the comment following Corollary 2.4.4 implies that $R_{k,n} \equiv (-1)^n f_k(n) \pmod{k}$ for all $n \geq k$, where $f_k(n)$ is some polynomial of degree at most $k-1$. We can determine $f_k(n) \pmod{k}$ by Lagrange interpolation using the values of $R_{k,n} \pmod{k}$ for $k \leq n < 2k$. For example, Figure 2.1 tells us that $f_3(n) \equiv n^2 + n - 1 \pmod{3}$ and $f_5(n) \equiv n^4 + 2n^3 + n^2 - 1 \pmod{5}$ and also that $(f_7(n))_{7 \leq n \leq 11} = (6, 5, 2, 3, 2)$.

2.5 Application to subsets of Latin hypercuboids

2.5.1 Introduction

In this section we introduce a generalisation of Latin rectangles to an arbitrary number of dimensions, which we call Latin hypercuboids. We use a modified version of the “proof template” of Section 2.1 to prove congruences satisfied by the number of Latin hypercuboids.

A difficulty of working with Latin hypercuboids in such generality is the necessity of cumbersome notation. We want our Latin hypercuboids to be of arbitrary dimension. So we will consider $a_1 \times a_2 \times \cdots \times a_s$ arrays, for positive integers a_1, a_2, \dots, a_s and let $\vec{a} = (a_1, a_2, \dots, a_s)$. Let $n = \max_i a_i$. We will usually take our symbol set to be $[n] = \{1, 2, \dots, n\}$, although the choice for this set is unimportant for our purposes, provided it possesses a total ordering. We will assume that $n = a_1 \geq a_2 \geq \cdots \geq a_s > 1 = a_{s+1} = a_{s+2}$ and so on. Let $\mathcal{F} = [a_1] \times [a_2] \times \cdots \times [a_s]$. We will index a cell in a Latin hypercuboid by $\vec{u} = (u_1, u_2, \dots, u_s) \in \mathcal{F}$, implying $1 \leq u_i \leq a_i$ for all $1 \leq i \leq s$. For the sake of the readers' eyes, we will sometimes not use a subscript for $l_{\vec{u}}$, taking $l_{\vec{u}} = l\vec{u} = l(\vec{u})$. A *Latin hypercuboid*, or *Latin \vec{a} -cuboid*, is an array $L = (l_{\vec{u}})_{\vec{u} \in \mathcal{F}}$ containing n symbols such that, for all $1 \leq i \leq s$,

$$l(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_s) \neq l(u_1, \dots, u_{i-1}, u'_i, u_{i+1}, \dots, u_s)$$

for distinct $u_i, u'_i \in [a_i]$.

For any $n \in \mathbb{N}$, let $\vec{n}_s = (n, n, \dots, n)$ be of length s . Latin \vec{n}_s -cuboids are an interesting class of Latin hypercuboid. In particular:

- Latin \vec{n}_2 -cuboids are Latin squares of order n .
- Latin \vec{n}_3 -cuboids are called *Latin cubes*.
- Latin \vec{n}_s -cuboids with $s \geq 4$ are called *Latin hypercubes*.

A Latin \vec{d} -cuboid $L = (l_{\vec{d}})$ is called *normalised* if $l(u_1, 1, 1, \dots, 1) = u_1$ for all $u_1 \in [a_1]$ and is called *reduced* if $l(1, 1, \dots, 1, u_i, 1, 1, \dots, 1) = u_i$ for all $1 \leq i \leq s$ and $u_i \in [a_i]$.

In some instances we are interested in the number of Latin \vec{d} -cuboids that satisfy some property P . If P and Q are properties of Latin \vec{d} -cuboids, then define the properties $P \wedge Q$, $P \vee Q$ and $\neg P$ where \wedge , \vee and \neg are the Boolean operators “and,” “or” and “not.” Define the following numbers:

- L_d^P is the number of Latin \vec{d} -cuboids that satisfy P ,
- K_d^P is the number of normalised Latin \vec{d} -cuboids that satisfy P ,
- R_d^P is the number of reduced Latin \vec{d} -cuboids that satisfy P .

If P is omitted then no further conditions are attached – we can assume P is the property “is a Latin \vec{d} -cuboid.” Therefore $L_{(n)} = n!$ and $R_{(n,k)}$ is the number of reduced $k \times n$ Latin rectangles.

The history of the enumeration of Latin \vec{n}_s -cuboids and the associated terminology has been discussed by McKay and Wanless [226], who also provided the number of Latin (n, n, n) -cuboids for $n \leq 6$ and Latin \vec{n}_s -cuboids for $n, s \leq 5$, which is reproduced in Figure 2.4. Krotov, Potapov and Sokolova [196] found a double-exponential lower bound on $L_{\vec{n}_s}$ for any fixed $n \geq 5$ as $s \rightarrow \infty$.

n	$R_{(n,n)}$	$R_{(n,n,n)}$	$R_{(n,n,n,n)}$	$R_{(n,n,n,n,n)}$
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	2^2	2^6	$2^2 \cdot 1783$	$2^4 \cdot 5^3 \cdot 100769$
5	$2^3 \cdot 7$	$2 \cdot 20123$	$2^2 \cdot 7 \cdot 1125127$	$2^3 \cdot 1187 \cdot 5317061$
6	$2^6 \cdot 3 \cdot 7^2$	$2^3 \cdot 3^4 \cdot 7 \cdot 97 \cdot 217981$		
References: [80, 144, 167, 172, 202, 226, 241, 262]				

FIGURE 2.4: Prime factorisation of $R_{\vec{n}_s}$ for $n \leq 6$ and $s \leq 5$.

Other generalisations

Many other generalisations of Latin squares and Latin rectangles exist, of which we will list several examples. In each case, L_n or $L_{k,n}$ arises as the cardinality of a special subset of the objects below. The following survey aims to give an appreciation for the variety of generalisations of Latin squares and Latin rectangles – it is not the author’s intention for it to be comprehensive. We are motivated by Cipra [58] to “try something harder,” in the hope that studying generalisations of Latin squares and rectangles will provide insights into L_n or $L_{k,n}$. Denés and Keedwell [71] also gave a discussion on generalised Latin squares.

We begin with *frequency squares*, which are $n \times n$ matrices in which any given symbol occurs the same number of times in every row and column. They were studied by MacMahon [209], Hedayat and Seiden [154], Finney [118], Brant and Mullen [30], Denés and Mullen [75] and Krčadinac [197] for example (see also [71, Sec. 12.5]). Erdős and Spencer [95] studied transversals of matrices in which “no symbol appears too often” (see also [4]).

Cao, Dinitz, Kreher, Stinson and Wei [45] studied “orthogonality” amongst $k \times n$ matrices with symbols from a set of cardinality s in which each symbol appears (a) in each row either $\lceil n/s \rceil$ or $\lfloor n/s \rfloor$ times and (b) in each column either $\lceil k/s \rceil$ or $\lfloor k/s \rfloor$ times. For example

$$\begin{pmatrix} 1 & 1 & 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 3 & 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Drisko [85] studied transversals in $k \times n$ *row-Latin rectangles*, which are $k \times n$ rectangular matrices with n symbols such that each symbol occurs exactly once in every row. Row-Latin rectangles with $k = n$ are called *row-Latin squares* and were studied by Norton [250], for example. Stein [300] (see also [92]) studied transversals of (a) $n \times n$ matrices with symbols from \mathbb{N} , called *n-squares* and (b) *n-squares* containing exactly n copies of each symbol $1, 2, \dots, n$, called *equi-n-squares*.

The Dinitz Conjecture (Theorem 1.2.11) considers $n \times n$ matrices (l_{ij}) , without repeated symbols in any row or column, such that each l_{ij} is an element of a predetermined set \mathcal{S}_{ij} of cardinality n .

Andersen and Hilton [8, 9, 10] studied $k \times n$ matrices with x symbols in each cell such that each symbol occurs at most p times in each row and at most q times in each column. Cavenagh et al. [50] studied $n \times n$ matrices with x not necessarily distinct symbols in each cell such that each symbol occurs exactly x times in each row and exactly x times in each column. For example

$$\begin{pmatrix} 1,2 & 1,2 & 3,3 & 4,4 \\ 2,3 & 2,3 & 4,4 & 1,1 \\ 1,4 & 3,4 & 1,2 & 2,3 \\ 3,4 & 1,4 & 1,2 & 2,3 \end{pmatrix}.$$

Brier and Bryant [32] studied $r \times s \times t$ arrays $(l_{(i,j,u)})$, on the symbol set $[n]$, such that every subset of $[n]$ of cardinality t is $\{l_{(i,j,u)}\}_{u \in [t]}$ for some $i \in [r]$ and $j \in [s]$. For example

$$\begin{pmatrix} 1 & 5 & 2 & 4 & 3 \\ 2 & 6 & 3 & 5 & 4 \\ 3 & 1 & 4 & 6 & 5 \end{pmatrix}, \begin{pmatrix} 2 & 6 & 1 & 5 & 4 \\ 3 & 1 & 2 & 6 & 5 \\ 4 & 2 & 3 & 1 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 4 & 5 & 6 & 1 \\ 4 & 5 & 6 & 1 & 2 \\ 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 1 & 3 & 2 & 6 \\ 5 & 2 & 4 & 3 & 1 \\ 6 & 3 & 5 & 4 & 2 \end{pmatrix}.$$

Nechvatal [245] considered the number of $k \times n$ matrices with symbols taken from a set of cardinality m without repeated symbols in any row or column; these were also mentioned

in Section 1.2.2. The $k = n$ case of Nechvatal's generalisation was also studied by Light Jr [207] and Mészáros [229].

Shapiro [283] considered $n \times n$ matrices $L = (l_{ij})$ such that $l_{ij} \neq l_{i'j'}$ whenever $x(i - i') \equiv y(j - j') \pmod{n}$ for any $(x, y) \in X$ in some $X \subset \{0, 1, \dots, n-1\} \times \{0, 1, \dots, n-1\}$. For example

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

where $X = \{(0, 1), (1, 0), (1, 1)\}$.

Hilton [158], Deng and Lim [76], Tay [311] and Iranmanesh and Ashrafi [166] studied $n \times n$ matrices in which each cell is assigned a set of symbols such that each symbol appears exactly once in each row and column. Green [140, 141] studied $k \times n$ matrices on n symbols such that each row contains every symbol and each column contains any symbol of B at most once, for some subset B of the symbol set. Shen, Cai, Liu and Kruskal [284, 285] and Hare [153] studied $n \times n$ matrices $L = (l_{ij})$ in which each symbol appears in every row and column and the symbol in position l_{ij} occurs either exactly (a) k times in the i -th row and l times in the j -th column or (b) l times in the i -th row and k times in the j -th column. The following example appears in [285]

$$\begin{pmatrix} 2 & 1 & 3 & 4 & 7 & 8 & 5 & 6 & 2 & 1 & 1 & 2 \\ 3 & 3 & 1 & 1 & 3 & 2 & 1 & 4 & 8 & 5 & 6 & 7 \\ 6 & 7 & 8 & 5 & 4 & 1 & 4 & 1 & 4 & 2 & 3 & 1 \\ 6 & 7 & 8 & 5 & 2 & 3 & 2 & 3 & 1 & 3 & 2 & 4 \\ 4 & 4 & 2 & 2 & 1 & 4 & 3 & 2 & 8 & 5 & 6 & 7 \\ 1 & 2 & 4 & 3 & 7 & 8 & 5 & 6 & 3 & 4 & 4 & 3 \\ 5 & 5 & 6 & 6 & 1 & 2 & 3 & 4 & 8 & 6 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 8 & 7 & 6 & 5 & 7 & 7 & 5 \\ 6 & 7 & 5 & 8 & 8 & 5 & 8 & 5 & 1 & 2 & 3 & 4 \\ 7 & 6 & 8 & 5 & 6 & 7 & 6 & 7 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 & 8 & 6 & 8 & 8 & 6 \\ 8 & 8 & 7 & 7 & 1 & 2 & 3 & 4 & 7 & 5 & 6 & 8 \end{pmatrix}$$

where $\{k, l\} = \{1, 3\}$.

Latin squares $L = (l_{ij})$ of order n are said to *avoid* another $n \times n$ matrix $M = (m_{ij})$ if $l_{ij} \neq m_{ij}$ for all i, j . Avoidance in Latin squares has become an active area of research, for example [47, 52, 56, 68, 146, 255, 254, 219].

There are various applications of Latin cubes, for example in parallel array access [116] and experimental design [117, p. 198] (see also [266]). Latin \vec{n}_s -hypercuboids (Latin hypercubes) are equivalent to maximum distance separable (MDS) codes over an alphabet of size n of length $s + 1$ and minimum distance 2 [203]. Hence $L_{\vec{n}_s}$ is the number of such codes. Laywine and Mullen [203, pp. 224–225] and Soedarmadji [294] showed that $L_{\vec{3}_s} = 3! \cdot 2^{s-1}$ for all s , which amounts to showing that $R_{\vec{3}_s} = 1$ by (2.5).

A construction

We will now observe a basic construction for Latin hypercuboids. Let $X = (x_{\vec{u}})$ and $Y = (y_{\vec{v}})$ be a Latin \vec{a} -cuboid and a Latin \vec{b} -cuboid, respectively, where

- $\vec{a} = (a_1, a_2, \dots, a_s)$ and $\mathcal{F}_1 = [a_1] \times [a_2] \times \dots \times [a_s]$,
- $\vec{b} = (b_1, b_2, \dots, b_t)$ and $\mathcal{F}_2 = [b_1] \times [b_2] \times \dots \times [b_t]$,
- $\vec{a}\vec{b} = (a_1, a_2, \dots, a_s, b_1, b_2, \dots, b_t)$ and $\mathcal{F}_1\mathcal{F}_2 = [a_1] \times [a_2] \times \dots \times [a_s] \times [b_1] \times [b_2] \times \dots \times [b_t]$,
- $\vec{u} \in \mathcal{F}_1$, $\vec{v} \in \mathcal{F}_2$ and $\vec{w} \in \mathcal{F}_1\mathcal{F}_2$ and $\vec{u}\vec{v} = (u_1, u_2, \dots, u_s, v_1, v_2, \dots, v_t)$.

We construct a Latin $\vec{a}\vec{b}$ -cuboid $L = (l_{\vec{w}})$ from X and Y by a direct-product-like construction. Let $n = \max(\{a_i\}_{1 \leq i \leq s} \cup \{b_i\}_{1 \leq i \leq t})$. We let $l_{\vec{w}}$ be the element in $[n]$ congruent to $x(\vec{u}) + y(\vec{v}) \pmod{n}$ whenever $\vec{w} = \vec{u}\vec{v}$.

There are some properties that L inherits from X and Y . For example, L is reduced if X and Y are reduced. Furthermore, the same L cannot be produced in this way by a different pair (X, Y) of reduced hypercuboids. Therefore, for any $I \subseteq [s]$, we obtain the primitive lower bound

$$R_{\vec{a}} \geq R_{(a_i)_{i \in I}} R_{(a_i)_{i \in [s] \setminus I}}. \quad (2.3)$$

For example, (2.3) implies that $R_{\vec{n}_s} \geq R_{(n,n)}^{\lfloor s/2 \rfloor}$.

If X or Y cannot be completed to a Latin \vec{n}_s cuboid, then L cannot be completed to a Latin \vec{n}_{s+t} -cuboid. Horák [159] gave a construction for Latin $(n, n, n-2)$ -cuboids that cannot be completed to an (n, n, n) -cuboid when n is a power of 2 and $n \geq 8$. Fu [123] constructed a Latin $(n, n, n-2)$ -cuboid that cannot be extended to an (n, n, n) -cuboid for all $n \geq 12$, which was extended by Kochol [188] (see also [189]) to include all $n \geq 6$. Kochol [190] constructed a Latin $(n, n, n-d)$ -cuboid that cannot be extended to an (n, n, n) -cuboid, when $n \geq 2d+1$ such that $d \geq 3$.

Kochol's result, combined with our direct-product-like construction, shows that there exists Latin $(n, n, \dots, n, n-d)$ -cuboids, for all $s \geq 3$ and $n \geq 2d+1$ where $d \geq 3$, that cannot be extended to an \vec{n}_s -cuboid. This construction was alluded to by McKay and Wanless [226].

Isotopism and parastrophy

The notions of isotopism and parastrophy generalise naturally to Latin hypercuboids. An ordered $(s+1)$ -tuple of permutations $\vec{\theta} = (\theta_0, \theta_1, \dots, \theta_s)$ will denote a mapping of Latin \vec{a} -cuboids $L = (l_{\vec{u}})$ such that $\vec{\theta}(L) = (l'_{\vec{u}})$ is defined by $l'(\theta_1(u_1), \theta_2(u_2), \dots, \theta_s(u_s)) = \theta_0(l_{\vec{u}})$ for all $\vec{u} \in \mathcal{F}$. For $\vec{\theta}(L)$ to be well-defined we require that θ_i fix $[a_i]$ setwise for all $1 \leq i \leq s$. We wish to caution the reader, that we now place the symbol permutation θ_0 at the first coordinate in $\vec{\theta}$, contrary to our use of isotopisms for Latin squares and Latin rectangles. The mapping $\vec{\theta}$ is called an *isotopism*, and we say $\vec{\theta}(L)$ is *isotopic* to L . The set of Latin \vec{a} -cuboids isotopic to L is called the *isotopy class* of L . If $\vec{\theta}(L) = L$ then $\vec{\theta}$ is called an *autotopism* of L .

If $\vec{\theta}$ is an isotopism such that $\theta_0 = \theta_1 = \dots = \theta_s = \alpha$ for some permutation α then $\vec{\theta}$ is called an *isomorphism* and will be denoted $\vec{\alpha}_s$. An isomorphism $\vec{\alpha}_s$ such that $\alpha(1) = 1$ and α fixes each $[a_i]$ setwise will map reduced Latin \vec{a} -cuboids to reduced Latin \vec{a} -cuboids. If $\vec{\theta}$ is both an isomorphism and an autotopism of L then $\vec{\theta}$ is called an *automorphism* of L . The identity permutation is still denoted ε and any isotopism other than $\vec{\varepsilon}_s$ is called *non-trivial*.

Clearly, every Latin \vec{d} -cuboid is isotopic to a normalised Latin \vec{d} -cuboid. However, for some choices of \vec{d} there exist Latin \vec{d} -cuboids that are not isotopic to any reduced Latin \vec{d} -cuboid, for example the Latin $(4, 2, 2)$ -cuboid

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}_{u_3=1} \quad \begin{bmatrix} 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}_{u_3=2}.$$

If L is a Latin \vec{d} -cuboid that is not isotopic to a reduced Latin \vec{d} -cuboid, then we call L an *irreducible* Latin \vec{d} -cuboid. We call $\vec{v} \in \mathcal{F}$ a *reducing cell* of a Latin \vec{d} -cuboid L , if the relation \subseteq is a total ordering on

$$\mathcal{Q}_{\vec{v}}(L) := \left\{ \{l(v_1, v_2, \dots, v_{i-1}, u_i, v_{i+1}, v_{i+2}, \dots, v_s) : u_i \in [a_i]\} : i \in [s] \right\}.$$

In the above example $\mathcal{Q}_{(1,1,1)} = \{\{1, 2, 3, 4\}, \{1, 2\}, \{1, 3\}\}$ and so \subseteq is not a total ordering in this case. Observe that, if \vec{v} is a reducing cell of L and $\vec{\theta}$ is an isotopism that maps \vec{v} to \vec{w} in $\vec{\theta}(L)$, then \vec{w} is a reducing cell of $\vec{\theta}(L)$.

Theorem 2.5.1. *A Latin \vec{d} -cuboid $L = (l_{\vec{u}})$ is isotopic to a reduced Latin \vec{d} -cuboid if and only if L has a reducing cell.*

Proof. Given a reducing cell $\vec{v} \in \mathcal{F}$, we will find an isotopic reduced Latin \vec{d} -cuboid.

Step 1: We choose $\vec{\theta} = (\theta_0, \theta_1, \dots, \theta_s)$ so that $\theta_1(v_1) = \theta_2(v_2) = \dots = \theta_s(v_s) = 1$. In this case, since \vec{v} is a reducing cell of L , $(1, 1, \dots, 1)$ is a reducing cell of $L' := \vec{\theta}(L)$.

Step 2: We apply a symbol permutation to L' , to obtain a Latin \vec{d} -cuboid $L'' = (l''_{\vec{u}})$, such that $l''(1, 1, \dots, 1) = 1$ and $\mathcal{Q}_{(1,1,\dots,1)}(L'') = \{[a_1], [a_2], \dots, [a_s]\}$. This is possible since $(1, 1, \dots, 1)$ is a reducing cell of L' .

Step 3: Finally we apply an isotopism $\vec{\theta}''$ to L'' with $\theta''_0 = \varepsilon$, to obtain the Latin \vec{d} -cuboid $L^* = (l^*_{\vec{u}})$, so that $l^*(1, 1, \dots, 1, u_i, 1, 1, \dots, 1) = u_i$ for all $i \in [s]$. This is possible, since $l''(1, 1, \dots, 1) = 1$. Thus we have found a reduced Latin \vec{d} -cuboid L^* isotopic to L .

Conversely, if $\vec{\theta}(L)$ is a reduced Latin \vec{d} -cuboid for some isotopism $\vec{\theta}$, then $(1, 1, \dots, 1)$ is a reducing cell of $\vec{\theta}(L)$. Therefore, $(\theta_1^{-1}(1), \theta_2^{-1}(1), \dots, \theta_s^{-1}(1))$ is a reducing cell of L . \square

Other notions of reducibility exist in the theory of so-called n -ary quasigroups [193, 194, 195, 196].

Lemma 2.5.2. *Let P be the property “ $(1, 1, \dots, 1)$ is a reducing cell” and let $Q = \neg P$. Then*

$$L_{\vec{d}} = n!K_{\vec{d}} = n! \prod_{i=1}^{s-1} \frac{(a_i - 1)!}{(a_i - a_{i+1})!} R_{\vec{d}} + n!K_{\vec{d}}^Q. \quad (2.4)$$

Proof. It is straightforward to observe that $L_{\vec{d}} = n!K_{\vec{d}}$. We will now simplify the terms in the expression $L_{\vec{d}} = L_{\vec{d}}^P + L_{\vec{d}}^Q$. This proof is similar to the proof of (1.1).

Given a reduced Latin \vec{d} -cuboid L we can construct Latin \vec{d} -cuboids from L satisfying P by applying any isotopism $\vec{\theta} = (\theta_0, \theta_1, \dots, \theta_s)$ where (a) $\theta_s = \varepsilon$ and (b) for all $1 \leq i \leq s-1$ both $\theta_i(1) = 1$ and θ_i fixes $[a_i]$ setwise. Thus creating $n! \prod_{i=1}^{s-1} (a_i - 1)!$, not necessarily distinct, Latin \vec{d} -cuboids that satisfy P .

Conversely, given a Latin \vec{d} -cuboid satisfying P , we can construct reduced Latin \vec{d} -cuboids $L = (l_{\vec{u}})$ by applying any isotopism $\vec{\theta}$ where (a) $\theta_s = \varepsilon$, (b) θ_0 permutes $[n]$ such that

$l(1, 1, \dots, 1, u_s) = u_s$ for all $u_s \in [a_s]$ and $\{l_{(1,1,\dots,1,u_i,1,1,\dots,1)} : u_i \in [a_i]\} = [a_i]$ for all $i \in [s]$ and (c) θ_i is such that $l_{(1,1,\dots,1,u_i,1,1,\dots,1)} = u_i$ for all $1 \leq i \leq s-1$ and $u_i \in [a_i]$. Thus creating $\prod_{i=1}^{s-1} (a_i - a_{i+1})!$, not necessarily distinct, reduced Latin \vec{d} -cuboids.

Hence $R_{\vec{d}}^P n! \prod_{i=1}^{s-1} (a_i - 1)! = L_{\vec{d}}^P \prod_{i=1}^{s-1} (a_i - a_{i+1})!$. This establishes the coefficient of $R_{\vec{d}} = R_{\vec{d}}^P$ in (2.4). For the remaining term $L_{\vec{d}}^Q = L_{\vec{d}} - L_{\vec{d}}^P$, observe that the group of all isotopisms consisting only of symbol permutations acts on the set of Latin \vec{d} -cuboids that satisfy Q with each orbit having size $n!$ and containing a unique normalised representative. \square

Equation (2.4) is a generalisation of (1.1) to Latin hypercuboids. If $a_1 = a_2 = \dots = a_{s-1}$ then every cell of a Latin \vec{d} -cuboid is a reducing cell. Hence $K_{\vec{d}}^Q = 0$ in (2.4) in many important cases, including Latin rectangles, Latin squares, Latin cubes and Latin hypercubes. Therefore

$$L_{\vec{n}_s} = n! K_{\vec{n}_s} = n!(n-1)!^{s-1} R_{\vec{n}_s}. \quad (2.5)$$

Additional properties

If L is a Latin \vec{d} -cuboid and M is a subarray of L that is also a Latin \vec{c} -cuboid, then M is called a \vec{c} -subcuboid of L . Here it is not required that $c_1 \geq c_2 \geq \dots \geq c_s$. Note that a (c_1, c_2) -subcuboid might not be a Latin rectangle, since we defined a $k \times n$ Latin rectangle to require $k \leq n$.

We will call a \vec{c} -subcuboid *proper* if $c_i < n$ for all $i \in [s]$ and at least two of the $c_i > 1$. This definition is motivated by the definition of proper subsquares in Latin rectangles, in that we want “proper” to exclude those subarrays that are automatically subcuboids.

If $L = (l_{\vec{u}})$ is a Latin \vec{d} -cuboid, then a *diagonal* is a set of a_s entries of L such that if \vec{u} and \vec{v} are distinct entries in the diagonal then $u_i \neq v_i$ for all $i \in [s]$. A diagonal that consists of a_s distinct symbols is called a *transversal*. The reader should be aware that there are other published definitions for the term transversal in Latin cubes and hypercubes, for example by Beljavskaja and Murathudjaev [20] and Heinrich [155].

Let L be a Latin \vec{n}_s -cuboid. If we fix u_i for all i except when $i = j$ then $(l_{\vec{u}})_{u_j \in [a_j]}$ is called a *line* of L . This definition comes from [226] and [80]. Each line can be considered to be a permutation of $[n]$ and therefore has a sign. The *sign* of L is the product of the signs of all sn^{s-1} lines of L . If $\epsilon(L) = +1$ then L is said to be an *even* Latin \vec{n}_s -cuboid, otherwise L is said to be an *odd* Latin \vec{n}_s -cuboid. We can generalise (1.6) to give

$$\epsilon(\vec{\theta}(L)) = \epsilon(L) \epsilon^{sn^{s-1}}(\theta_0) \prod_{i \in [s]} \epsilon^{n^{s-1}}(\theta_i) \quad (2.6)$$

for any isotopism $\vec{\theta}$.

Define the following properties: **EVEN** = “is an even Latin \vec{n}_s -cuboid” and **ODD** = “is an odd Latin \vec{n}_s -cuboid.”

If n is even, then each isotopy class of Latin \vec{n}_s -cuboids comprises entirely of Latin \vec{n}_s -cuboids of the same sign. Therefore, when n is even,

$$L_{\vec{n}_s}^P = n!(n-1)!^{s-1} R_{\vec{n}_s}^P, \quad (2.7)$$

where $P \in \{\text{EVEN}, \text{ODD}\}$.

Let L be an arbitrary Latin \vec{n}_s -cuboid where n is odd. Choose $\vec{\theta} = (\theta_0, \theta_1, \dots, \theta_s)$ such that $\theta_0 = \theta_1 = \dots = \theta_{s-1} = \varepsilon$ and θ_s is a transposition. Then (2.6) implies that $\epsilon(L) = -\epsilon(\vec{\theta}(L))$. Therefore, when n is odd and $n \geq 3$,

$$L_{\vec{n}_s}^{\text{EVEN}} = L_{\vec{n}_s}^{\text{ODD}} = \frac{1}{2}L_{\vec{n}_s} = \frac{1}{2}n!(n-1)!^{s-1}R_{\vec{n}_s} \quad (2.8)$$

by (2.5). Equations (2.7) and (2.8) generalise (1.7) and (1.8) to Latin cubes and Latin hypercubes.

Dougherty and Szczepanski [80] made the following conjecture.

Conjecture 2.5.3. $L_{\vec{n}_s}^{\text{EVEN}} \neq L_{\vec{n}_s}^{\text{ODD}}$ when n is even and $s \geq 2$.

The $s = 2$ case of Conjecture 2.5.3 is the Alon-Tarsi Conjecture (Conjecture 1.2.9 on page 21). Drisko [83] and Glynn [134] proved the Alon-Tarsi Conjecture for $n = p + 1$ and $n = p - 1$, respectively, for odd prime p . It is trivial to show that Conjecture 2.5.3 holds for $n = 2$ using (2.7) since $R_{\vec{2}_s} = 1$ and we prove the $n = 4$ case in Corollary 2.5.12. By computer enumeration, Ian Wanless (private communication) found that $R_{(6,6,6)}^{\text{EVEN}} = 92793745368 \neq 3116150784 = R_{(6,6,6)}^{\text{ODD}}$.

2.5.2 Divisors of the number of Latin hypercuboids

We will now introduce the mathematical machinery that we will later use to establish divisibility properties for R_d^P and the related numbers in (2.4). First we generalise Lemma 1.2.7 for use in an arbitrary number of dimensions.

Lemma 2.5.4. *Suppose $\vec{\theta}$ is an autotopism of a Latin (a_1, a_2, \dots, a_s) -cuboid. If any s of the following statements are true for some $\vec{u} \in \mathcal{F}$, then all $s + 1$ statements are true.*

- u_1 is fixed by θ_1 • u_2 is fixed by θ_2 • \dots • u_s is fixed by θ_s • $l_{\vec{u}}$ is fixed by θ_0

Usually we will use isotopisms $\vec{\theta} = (\theta_0, \theta_1, \dots, \theta_s)$ such that θ_i fixes 1 for all $0 \leq i \leq s$ when Lemma 2.5.4 is quite useful for studying those cells that have many coordinates equal to 1. Observe that for any Latin \vec{d} -cuboid $L = (l_{\vec{u}})$ the matrix $M = (m_{(u_1, u_2)})$ defined by $m_{(u_1, u_2)} = l_{(u_1, u_2, 1, 1, \dots, 1)}$ is an $a_1 \times a_2$ Latin rectangle embedded within L .

We will now modify the “proof template” of Section 2.1 to be applicable to Latin hypercubes. Let C be a set of Latin \vec{d} -cuboids and let $C_P \subseteq C$ be the subset of all Latin \vec{d} -cuboids in C that satisfy property P . For any $L \in C_P$ and group of isotopisms G that acts on C , let $\text{Atop}_G(L) = \text{Atop}(L) \cap G$ be the group of autotopisms of L in G and let $G(L) = \{\vec{\theta}(L) : \vec{\theta} \in G\} \subseteq C$ be the orbit of L under the action of G .

Lemma 2.5.5. *Let P be a property of Latin \vec{d} -cuboids that is invariant under the action of G .*

- (a) *Suppose $|\text{Atop}_G(L)| = 1$ for every $L \in C_P$. Then $|G|$ divides $|C_P|$.*
- (b) *Instead, suppose P is satisfied by every $L \in C$ such that $|\text{Atop}_G(L)| > 1$. Then $|C| \equiv |C_P| \pmod{|G|}$.*

Proof. Since P is invariant under G , C_P is closed under the action of G .

Assuming the conditions of (a), the action of G partitions C_P into orbits of size $|G(L)| = |G|/|\text{Atop}_G(L)| = |G|$ for all $L \in C_P$, by the Orbit-Stabiliser Theorem. Hence $|G|$ divides $|C_P|$.

Now assume the conditions of (b) and let $\mathcal{A} = C \setminus C_P$. It follows that \mathcal{A} is also closed under the action of G and every $L \in C$ with $|\text{Atop}_G(L)| > 1$ is not in \mathcal{A} . Hence we can apply part (a) of the lemma, with the property “ $\in \mathcal{A}$,” and obtain that $|G|$ divides $|\mathcal{A}| = |C| - |C_P|$. \square

Lemma 2.5.5 is a generalisation of the template of Section 2.1 which we used to establish numerous theorems concerning divisibility properties of the number of Latin rectangles.

Theorem 2.5.6. *Let C be the set of all Latin \vec{d} -cuboids, where $s \geq 2$. Suppose there exists x in the range $1 \leq x \leq n$ such that either $a_i \leq x$ or $a_i \geq x + r$ for all $1 \leq i \leq s$ for some $r \leq \lfloor n/2 \rfloor - 1$. Let $R = \{x + 1, x + 2, \dots, x + r\}$ and H_R be the group of all isomorphisms $\vec{\alpha}_s$ such that α fixes $[n] \setminus R$ pointwise. Let P be a property of Latin \vec{d} -cuboids that is invariant under H_R . Then $r!$ divides $|C_P|$.*

Proof. Suppose, seeking a contradiction, that $L = (l_{ij}) \in C_P$ admits a non-trivial automorphism $\vec{\alpha}_s \in H_R$. Let F denote the fixed points of α and let $F^* = [n] \setminus F$ denote its complement. Consider the line X formed with u_1 variable, while u_2 is some element of $[a_2]$ not fixed by α and $u_i = 1$ for $3 \leq i \leq s$. Since $u_3, u_4, \dots, u_s \in F$ and $u_2 \in F^*$, Lemma 2.5.4 implies that if $u_1 \in F$ then $l_{i1} \in F^*$. Therefore, $|F| \leq |F^*| = n - |F|$ and so $|F| \leq n/2$. However, we have assumed that $|F| \geq n - r > n/2$, giving a contradiction. Therefore $|\text{Atop}_{H_R}(L)| = 1$ for all $L \in C_P$. By Lemma 2.5.5(a), $r!$ divides $|C_P|$. \square

In Theorem 2.5.6, typically we would want r to be as large as possible, however for some choices of P it might be necessary to choose r less than its maximum allowed value, which is also acceptable.

Theorem 2.5.7. *Suppose n is even and $n = a_1 = a_2 = \dots = a_{s-1} \geq a_s > \lfloor n/2 \rfloor$. Assume the conditions of Theorem 2.5.6, except with $r = \lfloor n/2 \rfloor$ and $x = 1$. For $L = (l_{ij}) \in C$ let M be the subarray of L with $\lfloor n/2 \rfloor + 1 \leq u_i \leq \min(n, a_i)$ for all $i \in [s]$. Let Q be the property “ M is a subcuboid.” Then $|C_P| \equiv |C_{P \wedge Q}| \pmod{r!}$.*

Proof. We continue from the proof of Theorem 2.5.6. It remains true that $|F| \leq n/2$, however, now we have only assumed that $|F| \geq n/2$, hence $|F| = n/2$. By Lemma 2.5.5(b), it is sufficient to show, for all $L \in C_P$ with $\vec{\theta} \in \text{Atop}(L)$, that M is a subcuboid. But this follows from Lemma 2.5.4, which implies that M must only contain fixed symbols. \square

Theorem 2.5.6 provides a factorial divisor for certain subsets of Latin \vec{d} -cuboids. We will now list some properties P that are invariant under the action of H_R . In this case, if $a_s \geq \lfloor n/2 \rfloor$ then $(\lfloor n/2 \rfloor - 1)!$ divides $L_{\vec{d}}^P$ by Theorem 2.5.6.

- “is isotopic to L ” or “is isomorphic to L ,” for any Latin \vec{d} -cuboid L .
- “is reduced” or “is normalised.”
- “has an autotopism group of cardinality t .”
- “contains exactly t Latin \vec{c} -subcuboids.”
- “contains t transversals.”
- “for all $i \in [a_s]$ the entry in cell (i, i, \dots, i) is 1.”

- “for all $i \in [a_s]$ the entry in cell (i, i, \dots, i) is i .”
- “cannot be extended to a Latin cube.”

In the cases where t was used in the above list, we assume $t \geq 0$. Furthermore we may replace “exactly t ” with “ $\geq t$ ” or “ $\leq t$.” For Latin \vec{n}_s -cuboids we may append to the list “is even” and “is odd.”

We highlight the following case for later use; we find that the sign of a Latin (n, n) -cuboid (a Latin square of order n), is invariant under H_R by (2.6).

Corollary 2.5.8. *Both $R_{(n,n)}^{\text{EVEN}}$ and $R_{(n,n)}^{\text{ODD}}$ are divisible by $(\lceil n/2 \rceil - 1)!$ for all n .*

Furthermore, if P and T are properties invariant under H_R , then so are $P \wedge T$, $P \vee T$ and $\neg P$. To illustrate, the number of reduced even Latin squares of order n , that do not contain an intercalate but contain a transversal, is divisible by $(\lceil n/2 \rceil - 1)!$. Be aware that in some cases L_a^P may actually be the empty set, where $L_a^P = 0$ is divisible by every positive integer.

Let $m = \lfloor n/2 \rfloor$. In some cases, we can prove the factorial divisor $m!$ of $L_{\vec{n}_s}^P$ using Theorem 2.5.7. However this requires that we can evaluate $L_{\vec{n}_s}^{P \wedge Q} \pmod{m!}$. We list some examples of P which are appropriate below. In these cases $L_{\vec{n}_s}^{P \wedge Q} \equiv 0 \pmod{m!}$ since M can be replaced by any of the $L_{\vec{m}_s} = m!(m-1)!^{s-1} R_{\vec{m}_s}$ Latin \vec{m}_s -cuboids of order m on the same symbols as M , by (2.4).

- “contains a proper \vec{m}_s -subcuboid.”
- “contains a transversal outside of M .”

For the following corollary, we make use of the convention that $a_i \geq 2$ whenever $1 \leq i \leq s$. We continue to assume that $n = a_1 \geq a_2 \geq \dots \geq a_s$.

Corollary 2.5.9. *Let P be the property “does not contain a proper subcuboid.” Then $(a_s - 2)!$ divides R_a^P .*

Proof. Let G be the group of isomorphisms $\vec{\alpha}_s$ such that α fixes $\{1, a_s, a_s + 1, \dots, n\}$ pointwise. Let C_P be the set of reduced Latin \vec{a} -cuboids that do not contain a proper subcuboid. Then G acts on C_P . For all $L \in C_P$, $|G(L)| = |G| = (a_s - 2)!$ otherwise L admits a non-trivial automorphism in G and hence L contains a proper subcuboid, as a consequence of Lemma 2.5.4. Hence $R_a^P = |C_P| \equiv 0 \pmod{|G|}$ by Lemma 2.5.5(a). \square

We also list the following special case of Corollary 2.5.9.

Corollary 2.5.10. *The number of reduced Latin squares of order n that do not contain a proper subsquare is divisible by $(n - 2)!$ for all $n \geq 2$.*

2.5.3 Latin hypercubes of order four

In this section we prove that $R_{\vec{4}_s}^{\text{EVEN}} \equiv 1 \pmod{3}$ and $R_{\vec{4}_s}^{\text{ODD}} \equiv 0 \pmod{3}$ for all s . We are motivated by Figure 2.4 where we can observe that $R_{(4,4)} \equiv R_{(4,4,4)} \equiv R_{(4,4,4,4)} \equiv R_{(4,4,4,4,4)} \equiv 1 \pmod{3}$. Potapov and Krotov [262] proved that

$$3^{s+1} 2^{2^s+1} \leq L_{\vec{4}_s} \leq (3^{s+1} + 1) 2^{2^s+1}$$

when $s \geq 5$. In [194] they showed that Latin $\vec{4}_s$ -cuboids can be classified as either “permutibly reducible” or “semilinear.”

Let $\mathcal{F}_s = (\mathbb{Z}_2 \times \mathbb{Z}_2)^s$ and $\vec{u} = (u_1, u_2, \dots, u_s)$ denote an arbitrary element of \mathcal{F}_s . We will now use \mathcal{F}_s to index a Latin $\vec{4}_s$ -cuboid. We define a reduced $\vec{4}_s$ -cuboid $E_s = (e_{\vec{u}})$ by $e_{\vec{u}} = \sum_{i=1}^s u_i$ with addition component-wise modulo 2. For example, E_2 is given in Figure 2.5.

$$\begin{pmatrix} 00 & 01 & 10 & 11 \\ 01 & 00 & 11 & 10 \\ 10 & 11 & 00 & 01 \\ 11 & 10 & 01 & 00 \end{pmatrix}$$

FIGURE 2.5: The Latin $(4, 4)$ -cuboid E_2 .

Theorem 2.5.11. *The only reduced $\vec{4}_s$ -cuboid of order 4 that admits the automorphism $\vec{\alpha}_s$ where $\alpha = (01 \ 10 \ 11)$ is E_s .*

Proof. For any $\vec{u} \in \mathcal{F}_s$, and $i \in \mathbb{Z}_2 \times \mathbb{Z}_2$, we define $c_i = c_i(\vec{u})$ by $c_i = i$ if there is an odd number of coordinates of \vec{u} that are 01 and $c_i = 00$ otherwise. The symbol in cell \vec{u} in E_s is therefore $c_{01} + c_{10} + c_{11}$. We inspect the eight possibilities for this sum and find that $\alpha(c_{01} + c_{10} + c_{11}) = \alpha(c_{01}) + \alpha(c_{10}) + \alpha(c_{11})$ in every case. Therefore, $\vec{\alpha}_s$ is indeed an automorphism of E_s .

For brevity, we will call any reduced $\vec{4}_s$ -cuboid of order 4 that admits the automorphism $\vec{\alpha}_s$ a $(4, s, \alpha)$ -array. Observe that the theorem holds when $s \leq 2$. Assume, for the sake of induction, that E_t is the only $(4, t, \alpha)$ -array for some $t \geq 2$. Let $M = (m_{\vec{u}})$ be any $(4, t+1, \alpha)$ -array. Let $E_{t+1} = (e_{\vec{u}})$. We will now show that $m_{\vec{u}} = e_{\vec{u}}$ for all $\vec{u} \in \mathcal{F}_{t+1}$.

Consider the array C formed when $u_j = 00$ is fixed, for some $1 \leq j \leq t+1$, and the u_i are variable when $i \neq j$. Then, by the inductive assumption, C is a $(4, t, \alpha)$ -array and so $C = E_t$. Therefore, if $\vec{u} \in \mathcal{F}_{t+1}$ such that \vec{u} has a coordinate 00, then $m_{\vec{u}} = e_{\vec{u}}$.

Now suppose \vec{u} is such that $u_x = 01$, $u_y = 10$ and $u_z = 11$ for some $1 \leq x, y, z \leq t+1$. For $j \in \{x, y, z\}$, let $\vec{w}(j)$ be \vec{u} except with j -th coordinate changed to 00. Then $m_{\vec{u}} \neq m_{\vec{w}(j)} = u_1 + u_2 + \dots + u_{t+1} - u_j$ for all $j \in \{x, y, z\}$. Since $m_{\vec{w}(x)}$, $m_{\vec{w}(y)}$ and $m_{\vec{w}(z)}$ are all distinct, $m_{\vec{u}}$ is uniquely determined. Hence $m_{\vec{u}} = e_{\vec{u}}$.

For any $\vec{u} \in \mathcal{F}_{t+1}$, define $\Gamma(\vec{u}) = \{u_i : 1 \leq i \leq t+1\}$. We have not yet proved that $m_{\vec{u}} = e_{\vec{u}}$ for $\vec{u} \in \mathcal{F}_{t+1}$ such that $\Gamma(\vec{u}) \in \{\{01, 10\}, \{01, 11\}, \{10, 11\}\}$ or $|\Gamma(\vec{u})| = 1$. It is sufficient to show that $m_{\vec{u}} = e_{\vec{u}}$ for all $\vec{u} \in \mathcal{F}_{t+1}$ such that $\Gamma(\vec{u}) = \{01, 10\}$, because then (a) the symbols in cell \vec{u} when $\Gamma(\vec{u}) \in \{\{01, 11\}, \{10, 11\}\}$ will be determined by the automorphism $\vec{\alpha}_s$ and (b) the symbols in cells \vec{u} when $|\Gamma(\vec{u})| = 1$ are then uniquely determined by the remainder of M .

Assume \vec{u} has $\Gamma(\vec{u}) = \{01, 10\}$. Choose $1 \leq x, y \leq t+1$ such that $v_x = 01$ and $v_y = 10$. Construct \vec{w} from \vec{u} by changing u_x to 00. Construct \vec{w}' from \vec{u} by changing u_y to 00. Then $m_{\vec{u}} \neq m_{\vec{w}} = c_{10} + c_{01} - 01$ and $m_{\vec{u}} \neq m_{\vec{w}'} = c_{10} + c_{01} - 10$. Consequently

$$m_{\vec{u}} \in \{c_{10} + c_{01}, c_{10} + c_{01} - 11\} = \begin{cases} \{00, 11\} & \text{if } t \text{ is odd} \\ \{01, 10\} & \text{if } t \text{ is even,} \end{cases} \quad (2.9)$$

since $\vec{u} \in \mathcal{F}_{t+1}$ and $\Gamma(\vec{u}) = \{01, 10\}$.

Now let $\vec{v} \in \mathcal{F}_{t+1}$ be such that $\Gamma(\vec{v}) = \Gamma(\vec{u}) = \{01, 10\}$ and $c_{01}(\vec{u}) = c_{01}(\vec{v})$. We will show that $m_{\vec{u}} = m_{\vec{v}}$. It is sufficient to show that $m_{\vec{u}} = m_{\vec{v}}$ only when \vec{u} differs from \vec{v} at precisely

two coordinates. Let \vec{x} be one of the vectors that differs from both \vec{u} and \vec{v} at precisely one coordinate. Then $m_{\vec{x}} \neq m_{\vec{u}}$ and $m_{\vec{x}} \neq m_{\vec{v}}$. We know that $\{m_{\vec{u}}, m_{\vec{v}}, m_{\vec{x}}\}$ is a set of cardinality at most 2 by (2.9). Therefore if $m_{\vec{u}} \neq m_{\vec{v}}$ we reach a contradiction. So $m_{\vec{u}} = m_{\vec{v}}$.

Now define $\vec{p}, \vec{q}, \vec{r}, \vec{s} \in \mathcal{F}_{t+1}$ by

$$\begin{aligned} \bullet \vec{p} &= (\underbrace{01, 01, \dots, 01}_t, 10), & \bullet \vec{r} &= (\underbrace{10, 10, \dots, 10}_t, 01), \\ \bullet \vec{q} &= (\underbrace{10, 10, \dots, 10}_t, 11), & \bullet \vec{s} &= (\underbrace{10, 10, \dots, 10}_{t-1}, 01, 01). \end{aligned}$$

When t is even, assume, seeking a contradiction, that $m_{\vec{p}} = 01$. It follows that $m_{\vec{q}} = 10$ since $\vec{\alpha}_s$ is an automorphism of M . Hence $m_{\vec{r}} \neq 10$ and therefore $m_{\vec{r}} = 01$ by (2.9). Hence $m_{\vec{s}} = 10$, contradicting that $m_{\vec{p}} = m_{\vec{s}}$ (which is true as $c_{01}(\vec{p}) = c_{01}(\vec{s})$). Therefore, by (2.9), $m_{\vec{p}} = 10 = e_{\vec{p}}$.

When t is odd, assume, seeking a contradiction, that $m_{\vec{p}} = 00$. It follows that $m_{\vec{q}} = 00$ since $\vec{\alpha}_s$ is an automorphism of M . Hence $m_{\vec{r}} \neq 00$ and therefore $m_{\vec{r}} = 11$ by (2.9). This contradicts that $m_{\vec{p}} = m_{\vec{s}}$ (which is true as $c_{01}(\vec{p}) = c_{01}(\vec{s})$). Therefore, by (2.9), $m_{\vec{p}} = 11 = e_{\vec{p}}$.

For each \vec{u} with $\Gamma(\vec{u}) = \{01, 10\}$, either $m_{\vec{u}} = m_{\vec{p}}$, or \vec{u} belongs to a line in which every other symbol has already been determined. Hence $m_{\vec{u}} = e_{\vec{u}}$ for all $\vec{u} \in \mathcal{F}_{t+1}$ with $\Gamma(\vec{u}) = \{01, 10\}$. \square

Corollary 2.5.12. $R_{4_s}^{\text{EVEN}} \equiv 1 \not\equiv 0 \equiv R_{4_s}^{\text{ODD}} \pmod{3}$.

Proof. Let C_x be the set of reduced Latin $\vec{4}_s$ -cuboids of sign $x \in \{+1, -1\}$. Let $\alpha = (01 \ 10 \ 11)$. The group $\langle \alpha \rangle$, generated by α , acts on $C := C_{+1} \cup C_{-1}$ by isomorphism $(\alpha, \alpha, \dots, \alpha)$. Moreover, (2.6) implies $\langle \alpha \rangle$ preserves the sign of L . The group $\langle \alpha \rangle$ partitions C into parts of size 3 or 1, with every Latin hypercube in the same part having the same sign. The Latin hypercubes in parts of size 1 admit the automorphism $\vec{\alpha}_s$.

Theorem 2.5.11 implies that there is a unique part of size 1 containing E_s . Each line of E_s is either $(00, 01, 10, 11)$, $(01, 00, 11, 10)$, $(10, 11, 00, 01)$ or $(11, 10, 01, 00)$, which give rise to even permutations. Hence E_s is even for all s and we can deduce that $R_{4_s}^{\text{ODD}} \equiv 0 \pmod{3}$ and $R_{4_s}^{\text{EVEN}} \equiv 1 \pmod{3}$. \square

Corollary 2.5.12 and (2.7) imply a special case of Conjecture 2.5.3 by Dougherty and Szczepanski [80]. Specifically, $L_{4_s}^{\text{EVEN}} \neq L_{4_s}^{\text{ODD}}$ for all $s \geq 1$.

2.6 Application to graph decompositions

2.6.1 Introduction

In this section we will apply an analogue of the template of Section 2.1 to find divisors of the number of various graph decompositions. In this section, we will use K_n to denote the complete graph on n vertices. Consequently, the notation K_n will not be available for us to use as the number of normalised Latin squares of order n , but (1.2) allows us to use $L_n/n!$ instead. We use H to denote a labelled simple graph and G to denote a subgroup of the automorphism group of H . Let $V(H)$ be the vertex set of H and $E(H)$ be the edge set of H .

A *decomposition* D of a graph H is a set of subgraphs of H whose edge sets partition $E(H)$. Let $\text{Aut}(H)$ denote the automorphism group of H . Then $\text{Aut}(H)$ acts on the set of all decompositions of H by permuting the vertex labels. Two decompositions D and D' of H are called *isomorphic* if there exists $\alpha \in \text{Aut}(H)$ such that $\alpha(D) = D'$. If $\alpha \in \text{Aut}(H)$ such that, for some decomposition D of H , we have $\alpha(D) = D$ then α is called an *automorphism* of D . We use $\text{Aut}(D)$ to denote the group of automorphisms of D and we use $\text{Aut}_G(D) = \text{Aut}(D) \cap G$ for any $G \leq \text{Aut}(H)$. Any permutation other than the identity ε is called *non-trivial*.

Lemma 2.6.1. *Let \mathcal{D} be a set of decompositions of H that is closed under the action of $\text{Aut}(H)$ and let $G \leq \text{Aut}(H)$ such that $|\text{Aut}_G(D)| = 1$ for all $D \in \mathcal{D}$. Then $|G|$ divides $|\mathcal{D}|$.*

Lemma 2.6.1 is a special case of the following lemma.

Lemma 2.6.2. *Let \mathcal{D} be a set of decompositions of H that is closed under the action of $\text{Aut}(H)$ and let $G \leq \text{Aut}(H)$. Let $\mathcal{T} = \{D \in \mathcal{D} : |\text{Aut}_G(D)| > 1\}$ and $\mathcal{S} \subseteq \mathcal{D}$ such that $\mathcal{T} \subseteq \mathcal{S}$ and \mathcal{S} is closed under the action of G . Then $\gcd(|G|, |\mathcal{S}|)$ divides $|\mathcal{D}|$.*

Proof. The action of G partitions $\mathcal{D} \setminus \mathcal{S}$ into orbits of cardinality $|G|$ by the Orbit-Stabiliser Theorem. \square

2.6.2 One-factorisations

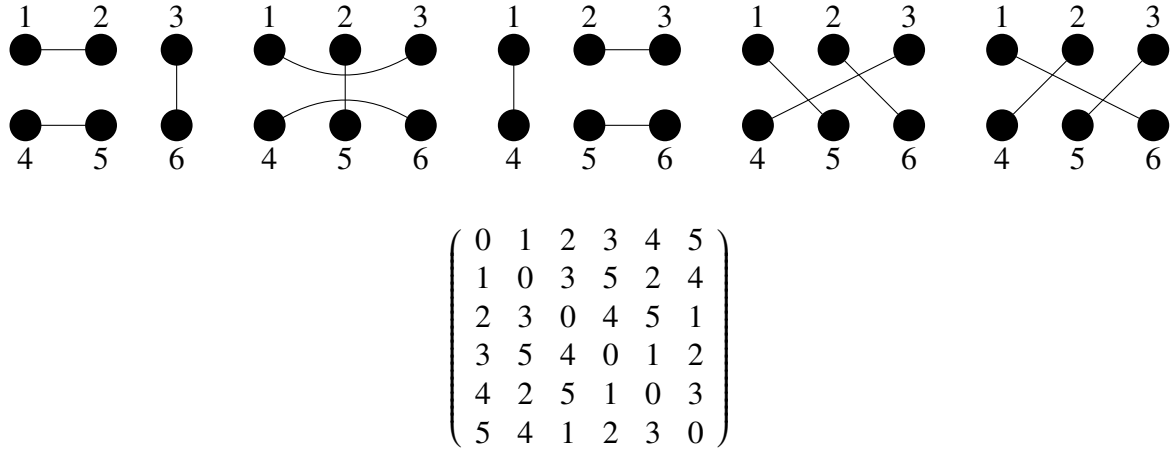
Recall that a *one-factor* of a graph H is a 1-regular spanning subgraph and a *one-factorisation* is a decomposition of H into a set of one-factors. Let $f_1(n)$ denote the number of one-factorisations of K_n . For $n \geq 2$, the complete graph K_n admits a one-factorisation if and only if n is even. We give an example of a one-factorisation of K_6 in Figure 2.6.

Recall that a Latin square $L = (l_{ij})$ is called unipotent if l_{ii} is independent of $i \in \mathbb{Z}_n$. From a one-factorisation of K_n , with vertices labelled by $0, 1, \dots, n-1$, we can construct a symmetric unipotent reduced Latin square L of order n (SURLS) defined by $\sum_{1 \leq c \leq n-1} cA_c$ where A_c is the adjacency matrix of the one-factor with 0 and c adjacent. Here we use cA_c to denote A_c with each symbol multiplied by c . Conversely, a SURLS defines a unique one-factorisation of K_n , with each non-zero symbol defining a one-factor. This bijection is also identified in [208, 228], for example. Hence $f_1(n)$ is the number of SURLS of order n [203, Thm 7.15]. Some values of $f_1(n)$ are given in Figure 2.7 (Sloane's [290] A000438) along with a list of relevant references.

Theorem 2.6.3. *Let $n = 2m$ for some $m \geq 3$. Then $f_1(n)$ is divisible by every odd d in the range $1 \leq d \leq n-3$. Moreover, $m!$ divides $f_1(n)$.*

Proof. Let \mathcal{D} be the set of all one-factorisations of K_n . Let $V(K_n) = \{v_1, v_2, \dots, v_n\}$ be the vertex set of K_n . Suppose α is an automorphism of a one-factorisation $D \in \mathcal{D}$. Let F denote the set of fixed vertices of α and let $F^* = V(K_n) \setminus F$ denote its complement. Then D cannot contain both (a) an edge with both endpoints in F and (b) an edge with precisely one endpoint in F^* . An example of a one-factor that cannot be in D is illustrated in Figure 2.8. Consequently $|F|$ must be even or $|F| = 1$.

Let G be a group of permutations of $V(K_n)$ generated by an r -cycle α , for some odd r . Since n is even, $|\text{Aut}_G(D)| = 1$ for all $D \in \mathcal{D}$, otherwise we contradict that $|F|$ must be even. Lemma 2.6.1 implies that $|G|$ divides $|\mathcal{D}| = f_1(n)$, proving the first claim in the theorem.

FIGURE 2.6: An example of a one-factorisation of K_6 and the corresponding SURLS.

n	$f_1(n)$	Factorisation	References
2	1	1	
4	1	1	
6	6	$2 \cdot 3$	
8	6240	$2^5 \cdot 3 \cdot 5 \cdot 13$	[77]
10	1225566720	$2^9 \cdot 3^3 \cdot 5 \cdot 7 \cdot 17 \cdot 149$	[129]
12	252282619805368320	$2^{16} \cdot 3^4 \cdot 5 \cdot 7 \cdot 1357857947$	[78]
14	98758655816833727741338583040	$2^{25} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11 \cdot 10486655975019043$	[178]
16	$\approx 1.48 \cdot 10^{44}$		
18	$\approx 1.52 \cdot 10^{63}$		[78]

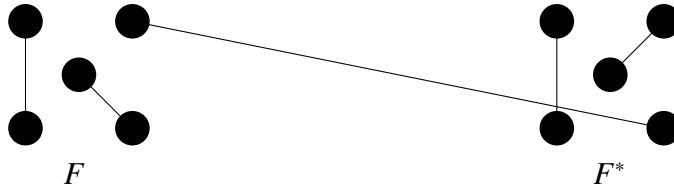
FIGURE 2.7: Some values of $f_1(n)$ and an approximation for $f_1(16)$ and $f_1(18)$.

Now suppose instead that G is the group of all permutations of $V(K_n)$ that fix the vertices v_1, v_2, \dots, v_m . Let \mathcal{S} be the set of one-factorisations $D \in \mathcal{D}$ that admit a non-trivial automorphism $\alpha \in G$. We know that $\gcd(m!, |\mathcal{S}|)$ divides $f_1(n)$ by Lemma 2.6.2. Again, we will let F denote the fixed points of α and let $F^* = V(K_n) \setminus F$ denote its complement. So $|F| \geq m$.

Suppose $v \in F$ and consider some one-factor $d \in \mathcal{D}$ where v is adjacent to a vertex in F^* . Then, in the one-factor d , every vertex in F is adjacent to a vertex in F^* , requiring $|F| \leq |F^*|$. However, since $|F| \geq m$, it must be that $|F| = |F^*|$. Therefore every one-factorisation $D \in \mathcal{S}$ contains a one-factorisation of $K_{m,m}$, the complete bipartite graph with vertex bipartition $\{v_1, v_2, \dots, v_m\} \cup \{v_{m+1}, v_{m+2}, \dots, v_n\}$. We define the one-factorisations equivalent to D to be those formed by replacing the one-factorisation of $K_{m,m}$ in D with any other one-factorisation of $K_{m,m}$. The number of one-factorisations of $K_{m,m}$ is $L_m/m!$, the number of normalised Latin squares of order m , as identified in Section 1.2.2. Therefore $L_m/m!$ divides $|\mathcal{S}|$.

Equation (1.2) with Theorem 2.4.6 implies that (a) $(m-1)!$ divides $L_m/m!$ and (b) $m!$ divides $L_m/m!$ if m is composite. When m is an odd prime, the first claim in the theorem implies that m divides $f_1(n)$. In any case, we find that $m!$ divides $f_1(n)$. \square

Theorem 2.6.3 implies that $f_1(14)$ is divisible by $2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$; Figure 2.7 gives the prime

FIGURE 2.8: An example of a one-factor that cannot be in D .

factorisation of $f_1(14)$.

2.6.3 Cycle decompositions

A survey of cycle decompositions of the complete graph was given by Bryant [40]. Let $c_k(n)$ denote the number of decompositions of K_n into k -cycles. A *Steiner triple system* of order n is a decomposition of K_n into triangles (i.e. K_3 subgraphs). So $c_3(n)$ is the number of Steiner triple systems of order n . It is well-known that a Steiner triple system of order n exists if and only if $n \equiv 1$ or $3 \pmod{6}$ [62]. The non-zero values of $c_3(n)$ for $3 \leq n \leq 19$ are given in Figure 2.9 (Sloane's A001201) along with a list of relevant references.

Lemma 2.6.4. *Let H be a graph with n vertices and let (a_1, a_2, \dots, a_t) be a sequence of integers. Suppose H admits a decomposition $D = \{d_1, d_2, \dots, d_t\}$ where each d_i is an a_i -cycle. Then*

- $3 \leq a_i \leq n$ for all $1 \leq i \leq t$,
- the number of edges in H is $a_1 + a_2 + \dots + a_t$ and
- each vertex of H has even degree.

Lemma 2.6.4 states some obvious necessary conditions for a decomposition D of H , consisting of d_i -cycles for $1 \leq i \leq t$, to exist. Alspach [6] conjectured that the three conditions in Lemma 2.6.4 are also sufficient in the specific cases $H = K_n$ for odd n and $H = K_n - I$ for even n (the graph obtained from the complete graph K_n after deletion of the edges in a one-factor I).

n	$c_3(n)$	Factorisation	References
3	1	1	
7	30	$2 \cdot 3 \cdot 5$	
9	840	$2^3 \cdot 3 \cdot 5 \cdot 7$	
13	1197504000	$2^9 \cdot 3^5 \cdot 5^3 \cdot 7 \cdot 11$	
15	60281712691200	$2^{11} \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13^2 \cdot 1117$	[63, 150, 328]
19	1348410350618155344199680000	$2^{25} \cdot 3^6 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 740429309$	[177]

FIGURE 2.9: The non-zero values of $c_3(n)$ for $3 \leq n \leq 19$.

Theorem 2.6.5. *Let $n = 2m + 1$ for some $m \geq 1$. Then $c_3(n)$ is divisible by every odd d in the range $1 \leq d \leq n - 2$. Moreover, $m!$ divides $c_3(n)$.*

Proof. Let \mathcal{D} be the set of all Steiner triple systems of K_n . Let $V(K_n) = \{v_1, v_2, \dots, v_n\}$ be the vertex set of K_n . Suppose α is an automorphism of a Steiner triple system $D \in \mathcal{D}$. Let F denote the set of fixed vertices of α and let $F^* = V(K_n) \setminus F$ denote its complement. Then D cannot have a triangle with exactly two vertices in F and one in F^* . Therefore every vertex in F is in exactly $|F^*|/2$ triangles with the other two vertices in F^* . Thus, if $|F| > 0$, we require that (a) $|F| \cdot |F^*|/2 \leq \binom{|F^*|}{2}$ and (b) $|F^*|$ is even.

Let G be a group of permutations of $V(K_n)$ that acts on \mathcal{D} . If G is the group of permutations that fixes v_1, v_2, \dots, v_{m+1} , then any $\alpha \in G$ cannot satisfy (a). If G is the group generated by a cycle of odd length less than n , then any $\alpha \in G$ cannot satisfy (b). In either case, Lemma 2.6.1 implies that $|G|$ divides $c_3(n)$. \square

For example, Theorem 2.6.5 proves that $c_3(19)$ is divisible by $2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$; Figure 2.9 gives the prime factorisation of $c_3(19)$.

Given a Steiner triple system, we may construct a totally symmetric idempotent Latin square $L = (l_{ij})$ with l_{ij} the unique element in the triangle $\{i, j, l_{ij}\}$ when $i \neq j$. Such a Latin square is called a *Steiner Latin square*. Colbourn and Rosa [62] gave the Steiner Latin square in Figure 2.10 corresponding to the Steiner triple system $\{013, 026, 045, 124, 156, 235, 346\}$.

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

FIGURE 2.10: A Steiner Latin square of order 7.

We will now discuss Hamilton cycle decompositions of the complete graph. A *Hamilton cycle* of a graph on n vertices is an n -cycle subgraph, so $c_n(n)$ is the number of decompositions of K_n into Hamilton cycles.

In any Hamilton cycle decomposition of K_n , the $n(n-1)/2$ edges of K_n are partitioned in parts of size n . Therefore n must be odd if $c_n(n) > 0$. In fact, it is well-known (see [40] for example) that there exists a Hamilton cycle decomposition of K_n if and only if n is odd. Therefore $c_n(n) > 0$ if and only if n is odd.

Theorem 2.6.6. *If $n \geq 2$ then $c_n(n)$ is divisible by $(n-2)!$.*

Proof. The theorem is trivially true when $2 \leq n \leq 4$, so assume $n \geq 5$. Let \mathcal{D} be the set of all Hamilton cycle decompositions of K_n . Let G be the group of permutations of $V(K_n) = \{v_1, v_2, \dots, v_n\}$ such that the vertices v_1 and v_2 are fixed. Then G acts on \mathcal{D} . For all $D \in \mathcal{D}$ there exists a unique $d \in D$ containing the edge between v_1 and v_2 . Therefore, $|\text{Aut}(D)| = 1$ for all $D \in \mathcal{D}$. By Lemma 2.6.1, $|G| = (n-2)!$ divides $c_n(n)$. \square

Let D be a Hamilton cycle decomposition of K_n , where $n \geq 3$, with vertices labelled $0, 1, \dots, n-1$. Each $d \in D$ corresponds to a pair of n -cycles α and α^{-1} with i and j adjacent in d implying either $\alpha(i) = j$ or $\alpha(j) = i$. From D we can therefore construct a sharply

transitive set S (as defined in Section 1.2.2), with $\varepsilon \in S$, such that $\alpha \in S$ and $\alpha^{-1} \in S$ whenever α is an n -cycle defined by some $d \in D$. From S we can construct a unique reduced Latin square $L = (l_{ij})$ of order n , defined by $l_{ij} = \alpha_i(j)$, where $\alpha_i \in S$ is the permutation satisfying $\alpha_i(0) = i$. This correspondence is illustrated in Figure 2.11.

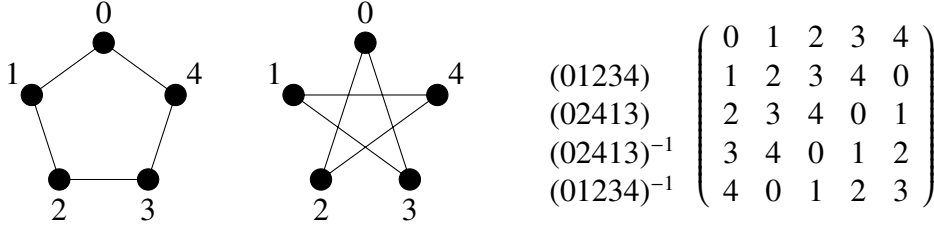


FIGURE 2.11: A Hamilton cycle decomposition of K_5 and the corresponding Latin square.

2.7 On the Alon-Tarsi Conjecture

2.7.1 Introduction

In this section we extend Theorem 1.2.10 by Drisko [83]. We deal only with Latin squares and take their symbol set to be \mathbb{Z}_n . Theorem 2.7.2 also improves Theorem 1.1.5 by McKay and Wanless [225] in some cases, giving a divisor for the number of Latin squares. We follow the work of [306] and use the definitions of Section 1.2.5. Drisko showed that $L_{p+1}^{\text{EVEN}} \not\equiv L_{p+1}^{\text{ODD}} \pmod{p^3}$ when p is an odd prime and made the following remark.

“This strongly suggests that the conjecture [the Alon-Tarsi Conjecture] should hold for all even integers. How might one prove the other cases? The general results and approach... could still be applied. The most promising cases seem to be $p^k + 1, \dots$ but one might also try $p + 3$ or even $pq + 1$, where $p \neq q$ are odd primes.”

— DRISKO [83]

In Corollary 2.7.7 we will prove that $L_{n+1}^{\text{EVEN}} \equiv L_{n+1}^{\text{ODD}} \pmod{t^3}$ for all $1 \leq t \leq n$ except when $t = n$ and n is prime, which includes all of the unresolved cases suggested by Drisko. Despite this obstacle, further progress has been made on the Alon-Tarsi Conjecture [134].

2.7.2 A modified proof template

We specialise the proof template in Section 2.1 to be applicable to Latin squares of a given sign. We have that G is a group of isotopisms that acts on a set \mathcal{C} of Latin squares and $\mathcal{A} \subseteq \mathcal{C}$ such that G acts on \mathcal{A} and if $|\text{Atop}(L) \cap G| > 1$ for some $L \in \mathcal{C}$, then $L \in \mathcal{A}$. Unless otherwise specified, we will assume $\mathcal{A} = \{L \in \mathcal{C} : |\text{Atop}(L) \cap G| > 1\}$. Here we only require that $\mu = |G|$.

Now we require the extra condition that G be *sign-preserving* on C , that is, $\epsilon(\theta(L)) = \epsilon(L)$ for all $\theta \in G$ and $L \in C$. For $x \in \{+1, -1\}$ we define $C_x = \{L \in C : \epsilon(L) = x\}$ and $\mathcal{A}_x = \{L \in \mathcal{A} : \epsilon(L) = x\}$. If G is sign-preserving on C , then G acts on both C_{+1} and C_{-1} individually. Similarly, since \mathcal{A} is closed under the action of G , if G is sign-preserving on C , then G acts on both \mathcal{A}_{+1} and \mathcal{A}_{-1} individually. Moreover, $|C_x| \equiv |\mathcal{A}_x| \pmod{|G|}$ for $x \in \{+1, -1\}$. In particular, when C is the set of all reduced Latin squares of order n and G is sign-preserving on C , we have that $R_n^{\text{EVEN}} \equiv |\mathcal{A}_{+1}| \pmod{|G|}$ and $R_n^{\text{ODD}} \equiv |\mathcal{A}_{-1}| \pmod{|G|}$.

To ensure that G is sign-preserving, we take G to consist only of isomorphisms; see (1.6). If C is the set of all reduced Latin squares of order n , to ensure that G acts on C , we insist that each $(\alpha, \alpha, \alpha) \in G$ has $\alpha(0) = 0$.

We illustrate the use of the modified proof template in the following example.

Example 2.7.1. $R_9^{\text{EVEN}} \equiv R_9^{\text{ODD}} \pmod{9}$.

Proof. Let C be the set of all reduced Latin squares of order 9. Let C_1 be the group generated by $(\alpha_1, \alpha_1, \alpha_1)$ where $\alpha_1 = (0)(1)(2)(3, 4, 5)(6, 7, 8)$ and let C_2 be the group generated by $(\alpha_2, \alpha_2, \alpha_2)$ where $\alpha_2 = (0)(1)(2)(3, 4, 5)^2(6, 7, 8)$. Let G be the group generated by $(\alpha_1, \alpha_1, \alpha_1)$ and $(\alpha_2, \alpha_2, \alpha_2)$. So G is a sign-preserving group of order $|G| = 9$ and G acts on C . Hence $R_9^{\text{EVEN}} \equiv |\mathcal{A}_{+1}| \pmod{9}$ and $R_9^{\text{ODD}} \equiv |\mathcal{A}_{-1}| \pmod{9}$.

Latin squares $L \in \mathcal{A}$ satisfy either $\text{Atop}(L) \cap G = C_1$ or $\text{Atop}(L) \cap G = C_2$. It is impossible for $G \leq \text{Atop}(L)$ since then $(0)(1)(2)(3)(4)(5)(6, 7, 8) \in \text{Atop}(L)$, when Lemma 1.2.8 implies L has a subsquare of order 6, contradicting Lemma 1.2.4. Using a backtracking algorithm, we found that the number of $L \in \mathcal{A}_x$ with $\text{Atop}(L) \cap G = C_i$ is 943488 in all four cases: $i \in \{1, 2\}$ and $x \in \{+1, -1\}$. Hence $|\mathcal{A}_{+1}| \equiv 0 \equiv |\mathcal{A}_{-1}| \pmod{9}$.

Another way to prove $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$ is by switching partial rows. If $L \in \mathcal{A}$ then the first three rows of $L = (l_{ij})$ have the following form, by Lemma 1.2.8.

0	1	2	3	4	5	6	7	8
1	2	0	·	·	·	a	b	c
2	0	1	·	·	·	d	e	f

Case I: If $\{a, b, c\} = \{d, e, f\}$ then we can switch the partial rows $(a, b, c) \leftrightarrow (d, e, f)$ to create a Latin square L' which has $\epsilon(L') = -\epsilon(L)$. See [322] for details on the effect of cycle switching on the sign of a Latin square.

Case II: If $\{a, b, c\} = \{6, 7, 8\}$ and $\{d, e, f\} = \{3, 4, 5\}$, then we can switch the partial rows $(6, 7, 8) \leftrightarrow (a, b, c)$ and then apply an isotopism of the form $(\epsilon, (6, 7, 8)^r, \epsilon)$ so that we form a reduced Latin square L' . Again $\epsilon(L') = -\epsilon(L)$ by (1.6).

Case III: The case $\{a, b, c\} = \{3, 4, 5\}$ and $\{d, e, f\} = \{6, 7, 8\}$ is handled as in Case II but with a, b, c replaced by d, e, f .

Combining the three cases, we form a partition of \mathcal{A} into parts $\{L, L'\}$ which have $\epsilon(L') = -\epsilon(L)$. Hence $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. \square

2.7.3 Congruences for Latin squares

We begin this section with the following theorem, which arose in the study of R_n^{EVEN} and R_n^{ODD} , but gives a divisor for R_n . The proofs of the subsequent three theorems are related.

Theorem 2.7.2. *Let $n \geq 1$, p be an odd prime and $c \geq 1$ such that $n/2 > (c-1)p$. Then $\gcd((n-cp-1)!^2 R_{n-cp}, p^c)$ divides R_n .*

Proof. This proof follows the template of Section 2.7.2. Let C be the set of all reduced Latin squares of order n . For $t \in \{0, 1, \dots, c-1\}$ define α_t to be the permutation $(1+pt, 2+pt, \dots, p+pt)$. Let G be the group of isomorphisms generated by the $(\alpha_t, \alpha_t, \alpha_t)$, so $|G| = p^c$.

Consider the structure of any $L \in C$ which admits a non-trivial automorphism $\theta \in G$. By Lemma 1.2.8 the rows and columns whose indices are fixed by θ form a subsquare M of order at least $n-cp$. Furthermore, the structure of G implies that the order of M is congruent to $n \pmod{p}$. Lemma 1.2.4 implies that the order of M is no more than $n/2 = n - n/2 < n - (c-1)p$, by assumption. Hence the order of M must be exactly $n-cp$ and therefore M must be formed by the rows and columns whose indices are $0, cp+1, cp+2, \dots, n-1$. Let $\mathcal{A} = \{L \in C : M \text{ is a subsquare of } L\}$.

We will partition \mathcal{A} into equivalence classes of cardinality $(n-cp-1)!^2 R_{n-cp}$. Two Latin squares L and L' in \mathcal{A} are equivalent if L' can be constructed from L by the following steps.

- (a) Apply some permutation to the set of partial rows $\{(l_{i1}, l_{i2}, \dots, l_{i(cp)}) : cp+1 \leq i \leq n-1\}$.
- (b) Apply some permutation to the set of partial columns $\{(l_{1j}, l_{2j}, \dots, l_{(cp)j}) : cp+1 \leq j \leq n-1\}$.
- (c) Replace the subsquare M by any of the R_{n-cp} reduced subsquares on the same symbol set.

The operations (a)–(c) are independent and generate unique Latin squares that have M as a subsquare. Hence each equivalence class is of cardinality $(n-cp-1)!^2 R_{n-cp}$. \square

Theorem 2.7.2 slightly improves some cases of Theorem 1.1.5 by McKay and Wanless [225]. Specifically, for some primes p there is a finite list of values of n for which we can now prove that p^{a+1} divides R_n , for some a , using Theorem 2.7.2, whereas Theorem 1.1.5 only proves that p^a divides R_n . The first such examples are when $p = 3$, when Theorem 2.7.2 implies that 3^2 divides R_{10} and 3^3 divides R_{15} and R_{16} whereas Theorem 1.1.5 shows only that 3 divides R_{10} and 3^2 divides R_{15} and R_{16} .

Theorem 2.7.3. *Let $n \geq 1$, p be a prime and $c \geq 2$ be an even integer such that $n/2 > (c-1)p$. Then $\gcd((n-cp-1)!^2, p^c)$ divides R_n^{EVEN} and R_n^{ODD} .*

Proof. The proof is similar to that of Theorem 2.7.2, but we do not use operation (c) in partitioning \mathcal{A} . The sign of a Latin square is invariant under the operations (a) and (b), since cp is even. Hence $(n-cp-1)!^2$ divides $|\mathcal{A}_{+1}|$ and $|\mathcal{A}_{-1}|$. \square

Theorem 2.7.4. *Let $n \geq 1$, p be an odd prime and $c \geq 1$ be an odd integer such that $n/2 > (c-1)p$ and $n \geq cp+3$. Then $R_n^{\text{EVEN}} \equiv R_n^{\text{ODD}} \pmod{p^c}$.*

Proof. The proof is similar to that of Theorem 2.7.2, except that equivalence on \mathcal{A} is instead defined by switching the pair of partial rows

$$(l_{(cp+1)1}, l_{(cp+1)2}, \dots, l_{(cp+1)(cp)}) \leftrightarrow (l_{(cp+2)1}, l_{(cp+2)2}, \dots, l_{(cp+2)(cp)}),$$

which both exist since $n \geq cp+3$. Since cp is odd, this equivalence partitions \mathcal{A} into parts $\{L, L'\}$, in which $\epsilon(L) = -\epsilon(L')$. Hence $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. \square

Theorem 2.7.5. *Let p be a prime and $n \geq p + 2$. Then $R_n^{\text{EVEN}} \equiv R_n^{\text{ODD}} \pmod{p}$.*

Proof. Figure 1.14 and Corollary 2.5.8 implies that the theorem is true when $p = 2$, so assume that p is an odd prime. Theorem 2.7.4 implies that this case is true when $n \geq p + 3$, so assume $n = p + 2$. The remainder of this proof is similar to that of Theorem 2.7.2 except that we have assumed $c = 1$ and we define $\mathcal{A} = \{L \in \mathcal{C} : (\alpha, \alpha, \alpha) \in \text{Aut}(L)\}$, where $\alpha = (0)(1, 2, \dots, p)(p + 1)$. From $L \in \mathcal{A}$ we construct L' in the following way.

- (a) Switch the partial columns $(l_{10}, l_{20}, \dots, l_{p0}) \leftrightarrow (l_{1(p+1)}, l_{2(p+1)}, \dots, l_{p(p+1)})$ to obtain the Latin square L^* .
- (b) Apply the unique isotopism of the form $\theta = (\tau, \varepsilon, \varepsilon)$ so that $L' = \theta(L^*)$ is reduced.

We observe that $\tau = \alpha^a$ for some a since $(\alpha, \alpha, \alpha) \in \text{Aut}(L)$ and α fixes 0 and $p + 1$. Hence $\varepsilon(L^*) = \varepsilon(\theta(L^*))$ since α is an even permutation. However step (a) causes $\varepsilon(L) = -\varepsilon(L^*)$, hence $\varepsilon(L) = -\varepsilon(L')$. Finally, observe that $L' \in \mathcal{A}$. Hence we have partitioned \mathcal{A} into $\{L, L'\}$ where $\varepsilon(L) = -\varepsilon(L')$. It follows that $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. \square

We can now combine previous results to give the following theorem.

Theorem 2.7.6. *If $2 \leq t \leq n - 1$, then $R_n^{\text{EVEN}} \not\equiv R_n^{\text{ODD}} \pmod{t}$ if and only if $t = n - 1$ is prime.*

Proof. *Case I:* $t = n - 1$ is prime. Figure 1.14 lists $R_3^{\text{EVEN}} \not\equiv R_3^{\text{ODD}} \pmod{2}$. If t is an odd prime, then Theorem 1.2.10 and (1.7) imply that $R_n^{\text{EVEN}} \not\equiv R_n^{\text{ODD}} \pmod{t}$.

Case II: t is a prime such that $t \leq n - 2$. This case is precisely Theorem 2.7.5.

Case III: t is composite. Corollary 2.5.8 implies that $R_n^{\text{EVEN}} \equiv 0 \equiv R_n^{\text{ODD}} \pmod{t}$ unless possibly if

$$(t, n) \in \{(4, 5), (4, 6), (4, 7), (4, 8), (9, 10), (9, 11), (9, 12)\}.$$

The $t = 4$ cases are resolved in Figure 1.14. The $t = 9$ cases are resolved by Theorem 2.7.3 when $c = 2$ and $p = 3$. \square

In [83], Drisko worked with L_{p+1}^{EVEN} and L_{p+1}^{ODD} modulo p^3 for prime p . For comparison, we give the following theorem which is implied by Theorem 2.7.6, (1.7) and (1.8).

Corollary 2.7.7. *Let $t \leq n$. Then $L_{n+1}^{\text{EVEN}} \not\equiv L_{n+1}^{\text{ODD}} \pmod{t^3}$ if and only if $t = n$ is prime.*

As for R_n^{EVEN} and R_n^{ODD} modulo n , we give the following theorem.

Theorem 2.7.8. *$R_n^{\text{EVEN}} \equiv R_n^{\text{ODD}} \pmod{n}$ if n is composite.*

Proof. Corollary 2.5.8 implies that $R_n^{\text{EVEN}} \equiv 0 \equiv R_n^{\text{ODD}} \pmod{n}$ whenever $(\lceil n/2 \rceil - 1)! \equiv 0 \pmod{n}$. When $(\lceil n/2 \rceil - 1)! \not\equiv 0 \pmod{n}$ is precisely when $n \in \{8, 9\} \cup \{2p : p \text{ is a prime}\}$. Figure 1.14 shows that $R_n^{\text{EVEN}} \equiv R_n^{\text{ODD}} \pmod{n}$ when $n \in \{4, 8\}$. Example 2.7.1 resolves the $n = 9$ case.

Now assume that $n = 2p$ for some odd prime p . The rest of this proof follows the template of Section 2.7.2. Let \mathcal{C} be the set of all reduced Latin squares of order n . Let $G \leq \mathcal{I}_n$ be the group of isomorphisms generated by $\theta := (\alpha, \alpha, \alpha)$ where $\alpha = (0)(1, 2, \dots, p)(p + 1)(p + 2) \cdots (n - 1)$.

Let $P = \{1, 2, \dots, p\}$ and $P^* = \mathbb{Z}_n \setminus P$. If $L = (l_{ij}) \in \mathcal{A}$, then Lemma 1.2.8 implies that the submatrix formed by the rows and columns whose indices are in P^* is a subsquare of L . We can therefore switch the two partial columns

$$(l_{1(p+1)}, l_{2(p+1)}, \dots, l_{p(p+1)}) \leftrightarrow (l_{1(p+2)}, l_{2(p+2)}, \dots, l_{p(p+2)})$$

to generate a distinct Latin square $L' \in \mathcal{A}$ for which $\epsilon(L) = -\epsilon(L')$. These columns exist since $p \geq 3$ implying $n \geq p + 3$. Hence $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. \square

A result of Glynn [134] implies that $R_n^{\text{EVEN}} \not\equiv R_n^{\text{ODD}} \pmod{n+1}$ if $n+1$ is an odd prime.

CHAPTER 3

Orthomorphisms and partial orthomorphisms

An *orthomorphism* of \mathbb{Z}_n is a permutation $\sigma : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ such that the mapping $\sigma^* : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$, defined by $\sigma^*(i) \equiv \sigma(i) - i \pmod{n}$ for all $i \in \mathbb{Z}_n$, is also a permutation. In fact, orthomorphisms are defined on any group $(G, +)$ similarly: an orthomorphism σ is a permutation of G such that $i \mapsto \sigma(i) - i$ is also a permutation. The interested reader should consult Evans [109]. However, we will focus only on orthomorphisms of \mathbb{Z}_n . If σ is an orthomorphism, then σ^* is called a *complete mapping*. An orthomorphism σ is called *canonical* if $\sigma(0) = 0$. Let z_n be the number of canonical orthomorphisms of \mathbb{Z}_n . Then the total number of orthomorphisms of \mathbb{Z}_n is nz_n .

In this chapter we mainly follow the work in [304] and [305], although the work in Section 3.3.5 does not appear in either of these papers. We find that Latin rectangles with cyclic automorphisms give rise to partial orthomorphisms. This enables us, in Theorem 3.2.1, to give a congruence relating the number of partial orthomorphisms $\omega(n, d)$ to the number of Latin rectangles $R_{k,n}$. We compute several small values of $\omega(n, d)$ which gives some previously unknown congruences for R_n , as given in Figure 3.4.

In Section 3.2.2 we employ the theory of systems of linear congruences to study the number $\omega(n, d)$ of partial orthomorphisms of \mathbb{Z}_n of deficit d . In particular, we show that $\omega(n, n - a)$ is determined by a finite set of polynomials for each a . In Section 3.2.3 we use a graph theoretic approach to find these polynomials for $1 \leq a \leq 6$ and give an asymptotic formula for $\omega(n, n - a)$ for fixed a as $n \rightarrow \infty$.

In Section 3.3 we introduce d -compound orthomorphisms and study their properties. For example, Property 3.3.1 and (3.13) classifies and enumerates the d -compound orthomorphisms of \mathbb{Z}_{dt} . Through the study of d -compound orthomorphisms we are able to find several interesting corollaries. In Corollary 3.3.7, we show that $R_{n+1} \equiv z_n \equiv -2 \pmod{n}$ for prime n and $R_{n+1} \equiv z_n \equiv 0 \pmod{n}$ for composite n , extending a result of Clark and Lewis [59]. In Theorem 3.3.8 we give a congruence for z_n which we use to compute $z_n \pmod{3}$ for all $n \leq 60$. Moreover, if $n \geq 5$ and $n \not\equiv 1 \pmod{3}$ then $z_n \equiv 0 \pmod{3}$. In Theorem 3.3.9 we additionally show that $z_n \equiv 1 \pmod{3}$ if $n = 2 \cdot 3^k + 1$ is prime. This extends a result of McKay, McLeod and Wanless [221] who proved the following theorem.

Theorem 3.0.9. *If L is the Cayley table of a group G of order $n \not\equiv 1 \pmod{3}$, then the number of transversals of L is divisible by 3.*

In Section 3.1 we will see that, when $G = \mathbb{Z}_n$, Theorem 3.0.9 implies that $nz_n \equiv 0 \pmod{3}$ when $n \not\equiv 1 \pmod{3}$ (although this is obviously true when 3 divides n).

We introduce two classes of d -compound orthomorphism, called compatible and polynomial. Let λ_n and π_n be the number of canonical compatible and canonical polynomial orthomorphisms respectively. We find a formula for λ_n in Theorem 3.3.14 and in Theorem 3.3.15 we show that $\lambda_n = \pi_n$ for odd n if and only if $n = 3^a 5^b p_1 p_2 \cdots p_r$ for $a \leq 3$, $b \leq 2$, $r \geq 0$ and distinct primes $p_i \geq 7$.

In Section 3.3.4 we give some new sufficient conditions for a partial orthomorphism to have a completion to a d -compound orthomorphism. Grüttmüller [142, 143] and Cavenagh, Härmäläinen and Nelson [51] have also researched this area. The new conditions, Theorems 3.3.20 and 3.3.21, provide an inductive-like step for arbitrary sized domains. Theorem 3.3.23 gives necessary and sufficient conditions for when two d -compound orthomorphisms are orthogonal.

3.1 Introduction

Euler [97, pp. 103–105] showed that $z_n = 0$ if and only if n is even¹ and listed the orthomorphisms of \mathbb{Z}_n for all $n \leq 7$ [97, pp. 100–109]. The value of z_n for odd $n \leq 25$ is listed in Figure 3.2 (Sloane's [290] A003111), sourced from McKay, McLeod and Wanless [221] who give credit to Shieh [286], Hsiang, Shieh and Chen [161] and Shieh via private correspondence. They also note the curious values of $z_n \pmod{8}$.

Bounds on z_n were found by Cooper and Kovalenko [65, 67, 192], McKay, McLeod and Wanless [221] and Cavenagh and Wanless [53]. Hence

$$(3.246)^n < z_n \leq (0.614)^n n! \quad (3.1)$$

for sufficiently large odd n . There are conjectured bounds on z_n by Vardi [318] (Conjecture 3.1.1) and Clark and Lewis [59] (Conjecture 3.1.2). See [221] and [324] for more details. Some estimates for z_n were given by Cooper, Gilchrist, Kovalenko and Novakovic [66] and Kuznetsov [198, 199]. Kuznetsov referred to a complete mapping as a “good permutation.” The reader should be aware that the papers [66] and [67] have received varying citations, likely due to differences in translation. Hsiang, Hsu and Shieh [160] considered the complexity of the orthomorphism counting problem.

Conjecture 3.1.1. *There exists $c_1, c_2 \in \mathbb{R}$ with $0 < c_1 < c_2 < 1$ such that $c_1^n n! \leq nz_n \leq c_2^n n!$ for all odd $n \geq 3$.*

Conjecture 3.1.2. $z_n \geq (n-2) \cdot (n-4) \cdots 3 \cdot 1$ for odd n .

If σ is an orthomorphism, we define its *difference equation* $\partial\sigma$ by $\partial\sigma(i) \equiv \sigma(i) - \sigma(i-1) \pmod{n}$ for all $i \in \mathbb{Z}_n$. The difference equation of a canonical orthomorphism is sufficient information to determine the orthomorphism itself.

Two Latin squares $L = (l_{ij})$ and $L' = (l'_{ij})$ of order n are called *orthogonal* if the cardinality of $\{(l_{ij}, l'_{ij}) : i, j \in \mathbb{Z}_n\}$ is n^2 , that is, each ordered pair of symbols $(s, t) \in \mathbb{Z}_n \times \mathbb{Z}_n$ satisfies

¹Euler's result will be generalised later by Theorem 4.3.16 in the context of automorphisms of Latin squares.

$(s, t) = (l_{ij}, l'_{ij})$ for unique $i, j \in \mathbb{Z}_n$. A set S of Latin squares is called a set of *mutually-orthogonal Latin squares*, or *MOLS* for short, if any two distinct $L, L' \in S$ are orthogonal. If L and L' are orthogonal, then L' is said to be an *orthogonal mate* of L .

Motivation for studying orthomorphisms of groups stems from the search for sets of MOLS. It was for this reason that Euler [97, pp. 100–131] studied orthomorphisms of \mathbb{Z}_n , which he called *formules directrices*.

Mann [215] showed that the Cayley table of a finite group G has an orthogonal mate if G admits a complete mapping. Evans [109, p. 1] attributed [215] as the origin of complete mappings and [173] as the origin of the term “orthomorphism.”

The relationship between MOLS and orthomorphisms was studied extensively by Evans [101, 102, 103, 104, 105, 106, 107, 108, 110], and also by Johnson, Dulmage and Mendelsohn [173], Franklin [120, 121] and Wanless [323]. See Bedford [18, 19] for a survey of results on the applications of orthomorphisms to orthogonal Latin squares.

We list some important transformations of orthomorphisms in Figure 3.1. For example, for any given orthomorphism σ there exists a unique g such that $i \mapsto \sigma(i) + g$ is a canonical orthomorphism – it is when $g = -\sigma(0)$. We denote the *translation* of σ by $T_g[\sigma]$ where $T_g[\sigma](i) \equiv \sigma(i + g) - \sigma(g) \pmod{n}$ for any $g \in \mathbb{Z}_n$. Equivalently, $T_g[\sigma] = \alpha^{-\sigma(g)} \circ \sigma \circ \alpha^g$ where $\alpha = (0, 1, \dots, n-1)$. We let \mathcal{G} denote the *group of translations*. The translation $T_g[\sigma]$ has difference equation $\partial T_g[\sigma]$ such that $\partial T_g[\sigma](i) = \partial \sigma(i + g)$.

Let $A = (a_{ij})$ be the Latin square of order n defined by $a_{ij} \equiv -i - j \pmod{n}$. Any orthomorphism $\sigma : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ corresponds to a transversal of A consisting of the entries $(i, \sigma(i) - i, -\sigma(i))$ for all $i \in \mathbb{Z}_n$. Since A is a totally symmetric Latin square, the parastrophy group generates six, not necessarily distinct, orthomorphisms from σ . These transformations are also listed in Figure 3.1.

Elevation	$i \mapsto \sigma(i) + g$	for any $g \in \mathbb{Z}_n$
Translation	$i \mapsto \sigma(i + g) - \sigma(g)$	for any $g \in \mathbb{Z}_n$
Reflection	$i \mapsto \sigma(-i) + i$	
Inversion	$\sigma(i) \mapsto i$	
Parastrophy	$i \mapsto \sigma(i)$	ε
	$i \mapsto -\sigma(i) + i$	(cs)
	$-\sigma(i) \mapsto -i$	(rs)
	$-\sigma(i) \mapsto -\sigma(i) + i$	(rcs)
	$\sigma(i) - i \mapsto -i$	(rsc)
	$\sigma(i) - i \mapsto \sigma(i)$	(rc)

FIGURE 3.1: Transformations of an orthomorphism σ of \mathbb{Z}_n .

A *partial orthomorphism* is an injection $\nu : S \rightarrow \mathbb{Z}_n$ for some $S \subseteq \mathbb{Z}_n$ such that $i \mapsto \nu(i) - i$ is also an injection. We say ν has *deficit* $d := n - |S|$. Hence an orthomorphism is a partial orthomorphism of deficit 0. This terminology comes from Wanless [323] who also studied partial orthomorphisms in connection with Latin squares that admit cyclic automorphisms (see also [41]). Let $\omega(n, d)$ be the number of partial orthomorphisms of deficit d . Not all partial orthomorphisms can be embedded in an orthomorphism, for example the partial orthomorphism of \mathbb{Z}_5 such that $0 \mapsto 0$, $1 \mapsto 2$ and $2 \mapsto 1$.

Sometimes we will use partial orthomorphisms $\nu : S \rightarrow \mathbb{Z}_n$ that satisfy $\nu(i) \notin \{0, i\}$ for all $i \in S$, which we will call (n, d) -partial orthomorphisms (where d is the deficit). Let $\chi(n, d)$ be the number of (n, d) -partial orthomorphisms. For an (n, d) -partial orthomorphism ν to exist, d must satisfy $1 \leq d \leq n$. We will take $\chi(n, n) = 1$ when $n \geq 1$ and $\chi(n, d) = 0$ when $d > n \geq 1$.

Example 3.1.3. *There exists an (n, d) -partial orthomorphism for all $1 \leq d \leq n$. Hence $\chi(n, d) > 0$ for all $1 \leq d \leq n$.*

Proof. A simple example of an $(n, 1)$ -partial orthomorphism ν for odd n is $i \mapsto 2i \pmod{n}$ for $1 \leq i < n$. For even n let ν be defined by $i \mapsto 2i + 1 \pmod{n}$ for $0 \leq i < n/2$ and $i \mapsto 2i \pmod{n}$ for $n/2 < i < n$. By restricting the domain of ν we can construct an (n, d) -partial orthomorphism for any $1 \leq d \leq n$. \square

For even $n \geq 2$, $\chi(n, 1) > 0$ whereas $z_n = 0$. Some values of $\chi(n, 1)$ are listed in Figure 3.2 (Sloane's [290] A006609). Notice the curiously large power of 2 dividing $\chi(n, 1)$ for even n , which we are currently unable to explain.

The following theorem was given by Wanless [323].

Theorem 3.1.4. *For even $n \geq 2$, the domain of any $(n, 1)$ -partial orthomorphism ν is $\mathbb{Z}_n \setminus \{n/2\}$. For odd $n \geq 1$, every $(n, 1)$ -partial orthomorphism σ has domain $S = \mathbb{Z}_n \setminus \{0\}$. Therefore $\chi(n, 1) = z_n$ for odd n .*

Corollary 3.1.5. $\chi(n, 1) \equiv z_n \equiv n \pmod{2}$ for $n \geq 3$.

Proof. A proof that $z_n \equiv n \pmod{2}$, for all n , was attributed to Levitskaya [204] by Novakovich [252]; there were also proofs given by Clark and Lewis [59] and McKay, McLeod and Wanless [221]. Theorem 3.1.4 asserts that $\chi(n, 1) = z_n$ for odd n .

Give an $(n, 1)$ -partial orthomorphism of \mathbb{Z}_n for even $n \geq 2$, Theorem 3.1.4 implies that we can define another $(n, 1)$ -partial orthomorphism by $\nu(i) - i + n/2 \mapsto \nu(i)$ for all $i \in S$. These two $(n, 1)$ -partial orthomorphisms are the same only if $i \equiv \nu(i) - i + n/2 \pmod{n}$ for all $i \in S$, which is impossible if $\nu(i) + n/2$ is odd for any $i \in S$. Therefore, for even $n \geq 4$, $\chi(n, 1) \equiv z_n \equiv n \pmod{2}$. \square

A set Q of cardinality n together with two binary operations \bullet and \otimes is called a *neofield* of order n , denoted (Q, \bullet, \otimes) , if

- (Q, \bullet) is a loop with identity e ,
- $(Q \setminus \{e\}, \otimes)$ is a group and
- \otimes is both left and right distributive over \bullet .

A neofield (Q, \bullet, \otimes) is called *cyclic* if $(Q \setminus \{e\}, \otimes)$ is a cyclic group.

Keedwell [179, 180] showed that orthogonal Latin squares can be generated from certain types of cyclic neofields. Bedford [17] (see also [181]) constructed orthogonal Latin squares using left neofields (left neofields are the same as neofields except that it is not assumed that \otimes is right distributive over \bullet). See Paige [258] and Hsu [162] for more information about neofields. Drisko [83] (see Sections 1.2.5 and 2.7) used cyclic neofields to establish a result on the number of even and odd Latin squares. Evans [109, p. 14] (see also Paige [257]) gave results tantamount to the following theorem.

Theorem 3.1.6. *For all $n \geq 1$, $\chi(n, 1)$ is the number of cyclic neofields of order $n + 1$.*

n	$\chi(n, 1)$	Factorisation	(mod 3)	(mod 8)	(mod n)
1	1	1	1	1	0
2	1	1	1	1	1
3	1	1	1	1	1
4	2	2	2	2	2
5	3	3	0	3	3
6	8	2^3	2	0	2
7	19	19	1	3	5
8	64	2^6	1	0	0
9	225	$3^2 \cdot 5^2$	0	1	0
10	928	$2^5 \cdot 29$	1	0	8
11	3441	$3 \cdot 31 \cdot 37$	0	1	9
12	17536	$2^7 \cdot 137$	1	0	4
13	79259	79259	2	3	11
14	454016	$2^7 \cdot 3547$	2	0	10
15	2424195	$3^3 \cdot 5 \cdot 17957$	0	3	0
16	15628288	$2^{11} \cdot 13 \cdot 587$	1	0	0
17	94471089	$3 \cdot 31490363$	0	1	15
18	679156224	$2^9 \cdot 3 \cdot 139 \cdot 3181$	0	0	6
19	4613520889	$2837 \cdot 1626197$	1	1	17
20	36563599360	$2^{14} \cdot 5 \cdot 446333$	1	0	0
21	275148653115	$3 \cdot 5 \cdot 7^2 \cdot 3347 \cdot 111847$	0	3	0
22	?	?			
23	19686730313955	$3 \cdot 5 \cdot 1312448687597$	0	3	21
24	?	?			
25	1664382756757625	$5^3 \cdot 13315062054061$	2	1	0

FIGURE 3.2: Some values of $\chi(n, 1)$ and its prime factorisation. When n is odd $z_n = \chi(n, 1)$ and when n is even $z_n = 0$.

3.1.1 Equivalences

We will now identify some of the combinatorial objects equivalent (in some sense) to orthomorphisms. Let $\alpha = (0, 1, \dots, n-1)$ and $\beta = (0)(1, 2, \dots, n)$. If L is a Latin square of order n such that (α, α, α) is an automorphism, then L is called a *diagonally cyclic* Latin square or a DCLS. If L is a reduced Latin square of order $n+1$ such that (β, β, β) is an automorphism, then L is called a reduced *bordered diagonally cyclic* Latin square or a reduced BDCLS. Note that the first row of a DCLS and the second row of a reduced BDCLS are sufficient to completely determine the square. See [323] for more information about diagonally cyclic Latin squares.

If n is odd, then there exists a natural bijection between canonical orthomorphisms σ of \mathbb{Z}_n and the following combinatorial objects:

- Idempotent DCLSs of order n .
 - We can construct an idempotent DCLS $L = (l_{ij})$ from σ by assigning the first row such that $l_{0j} = \sigma(j)$ for $j \in \mathbb{Z}_n$. Conversely, the first row of an arbitrary idempotent DCLS uniquely defines a canonical orthomorphism.
- Reduced unipotent BDCLSs of order $n+1$.
 - We can construct a reduced BDCLS $L = (l_{ij})$ of order $n+1$ from σ by assigning $l_{1j} = \sigma(j-1) + 1$ for all $2 \leq j \leq n$, which is sufficient information to uniquely determine L . Theorem 3.1.4 ensures that any reduced BDCLS of order $n+1$ is unipotent, since n is odd. Conversely, given a unipotent reduced BDCLS of order $n+1$, the permutation σ , defined by $l_{1j} = \sigma(j-1) + 1$ for all $2 \leq j \leq n$ and $\sigma(0) = 0$, is a canonical orthomorphism.
- Transversals containing the entry $(0, 0, 0)$ of the Cayley table of \mathbb{Z}_n .
 - In the Cayley table of \mathbb{Z}_n the diagonal consisting of the entries $(i, \sigma(i) - i, \sigma(i))$ for $i \in \mathbb{Z}_n$ is a transversal. Conversely, given a transversal of the Cayley table of \mathbb{Z}_n containing the entry $(0, 0, 0)$, the permutation σ , defined such that $\sigma(i)$ is the symbol in the transversal in row i , is a canonical orthomorphism.
- The canonical orthomorphism's difference equation $\partial\sigma$ and the fixed point $\sigma(0) = 0$.
- A placement of n non-attacking semiqueens on a toroidal $n \times n$ chess board (see [21, 271]). Semiqueens can move horizontally, vertically or along one diagonal but not the other diagonal. The board “wraps around” both horizontally and vertically.
 - Consider a transversal of the Cayley table of \mathbb{Z}_n . Any entry in a transversal prevents another entry in the same row, same column and of the same symbol. Since the symbols of the Cayley table of \mathbb{Z}_n are arranged cyclically the prevented entries are traced out by a semiqueen.

Cavenagh and Wanless [53] also noted that orthomorphisms are equivalent to so-called magic juggling sequences [261, p. 35].

3.2 Latin rectangles and partial orthomorphisms

This section follows the work of [305]. We introduce a congruence in Theorem 3.2.1 that motivates the subsequent study of the enumeration of partial orthomorphisms.

3.2.1 A congruence for the number of Latin rectangles

We are motivated by Theorem 1.1.5, which implies that $R_n \equiv 0 \pmod{p}$ for all primes $p \leq \lfloor n/2 \rfloor$, and Corollary 2.4.4, which shows that $R_p \equiv 1 \pmod{p}$ for prime p . The Latin squares case of the following theorem gives a formula for $R_n \pmod{p}$ for primes $p < n$.

Theorem 3.2.1. *Let p be a prime such that $n \geq k \geq p + 1$. Then*

$$R_{k,n} \equiv \chi(p, n-p) \frac{(n-p)!(n-p-1)!^2}{(n-k)!} R_{k-p, n-p} \pmod{p}.$$

Proof. When $n \geq 2p$, the theorem states $R_{k,n} \equiv 0 \pmod{p}$ which was proved in Theorems 2.2.1 and 2.2.2, so assume $n < 2p$.

We will use X to denote the symbol set and column indices of the $k \times n$ Latin rectangle L and $\mathcal{Y} \subseteq X$ to denote the row indices of L . We will assume that e is the minimum element of X and $e \in \mathcal{Y}$. A Latin rectangle $L = (l_{ij})$ is called reduced if $l_{ej} = j$ for all $j \in X$ and $l_{ie} = i$ for all $i \in \mathcal{Y}$.

Let $X = \{e\} \cup \mathbb{Z}_p \cup X$ where $X = \{x_1, x_2, \dots, x_{n-p-1}\}$ and $\mathcal{Y} = \{e\} \cup \mathbb{Z}_p \cup Y$ where $Y = \{x_1, x_2, \dots, x_{k-p-1}\}$, requiring $k \geq p + 1$. We wish to enumerate the reduced $k \times n$ Latin rectangles L modulo p .

Let α be the p -cycle $(0, 1, \dots, p-1)$ and G be the group of isomorphisms generated by $\theta := (\alpha, \alpha, \alpha)$. Since α fixes e , the group G acts on the set of reduced $k \times n$ Latin rectangles, partitioning it into orbits of cardinality either 1 or p , as p is prime. An orbit has cardinality 1 only if the Latin rectangle in that orbit admits the automorphism θ . Hence it is sufficient to enumerate only the reduced $k \times n$ Latin rectangles $L = (l_{ij})$ that admit the automorphism θ .

Let M be the submatrix formed by the rows $\{e\} \cup Y$ and columns $\{e\} \cup X$. Then M is a $(k-p) \times (n-p)$ subrectangle of L by Lemma 1.2.7. Therefore L is uniquely determined by M and the entries $(0, j, l_{0j})$ for $j \in X \setminus \{e\}$ and $(i, 0, l_{i0})$ for $i \in Y$.

We will now identify a $(p, n-p)$ -partial orthomorphism ν within L . Let $S = \{s \in \mathbb{Z}_p : l_{0s} \in \mathbb{Z}_p\}$. Then $\nu : S \rightarrow \mathbb{Z}_p$ defined by $\nu(s) = l_{0s}$ is a partial orthomorphism since θ is an automorphism of L . Furthermore, ν is a $(p, p - |S|)$ -partial orthomorphism because $\nu(s) \neq l_{0e} = 0$ and $\nu(s) \neq l_{es} = s$ for all $s \in S$. Since θ is an automorphism of L , the entries $(0, j, l_{0j})$ for $j \in X$ all have $l_{0j} \in \mathbb{Z}_p \setminus \{0\}$. Therefore $|S| = 2p - n > 0$ and so ν is a $(p, n-p)$ -partial orthomorphism.

We can construct any reduced $k \times n$ Latin rectangle $L = (l_{ij})$ with automorphism θ in the following way. Choose a $(p, n-p)$ -partial orthomorphism ν from the $\chi(p, n-p)$ available. There are $(n-p)!$ ways to choose the symbols l_{0j} for $j \in \mathbb{Z}_p$ such that $l_{0s} = \nu(s)$ for all s in the domain of ν and the remaining cells contain the symbols X . After these designations, row 0 can be completed in $(n-p-1)!$ ways so that $l_{0e} = 0$. The automorphism θ determines the remaining rows indexed by \mathbb{Z}_p from row 0. After these designations, column 0 can be completed in $(n-p-1)!/(n-k)!$ ways so that $l_{e0} = 0$. The automorphism θ determines the

remaining columns indexed by \mathbb{Z}_p from row 0. Regardless of the previous choices, there are $R_{k-p, n-p}$ choices for the subrectangle M so that L is a reduced $k \times n$ Latin rectangle.

As previously mentioned, the above choices uniquely determine L . Therefore there are exactly $\chi(p, n-p)(n-p)!(n-p-1)!^2 R_{k-p, n-p}/(n-k)!$ reduced $k \times n$ Latin rectangles that admit the automorphism θ . \square

The following corollary is a special case of Theorem 3.2.1 when $n = k = p + d$ for some prime p .

Corollary 3.2.2. *Let p be prime. Then $R_{p+d} \equiv d!(d-1)!^2 \chi(p, d) R_d \pmod{p}$.*

Corollary 3.2.2 implies that $R_{p+1} \equiv \chi(p, 1) \pmod{p}$ for primes p . Clark and Lewis [59] showed that $z_p \equiv -2 \pmod{p}$ when p is an odd prime. Hence

$$R_{p+1} \equiv \chi(p, 1) = z_p \equiv -2 \pmod{p}$$

when p is an odd prime, by Theorem 3.1.4. In Corollary 3.3.7 we will show that $R_{n+1} \equiv z_n \equiv 0 \pmod{n}$ for composite n .

Figure 3.3 lists some values of $\chi(p, d)$ when p is a small odd prime number. These were obtained by two independent computer enumerations, by Ian Wanless (private communication) and the author, except for $\chi(17, d)$ where $d \leq 6$ and $\chi(19, d)$ where $10 \leq d \leq 12$, which were only computed by Wanless. We did not compute $\chi(19, d)$ for $2 \leq d \leq 9$. Figure 3.4 lists the congruences for R_n that can be obtained from Figure 3.3 and Corollary 3.2.2. The limiting factors in extending Figure 3.4 are knowledge of $R_n \pmod{p}$ and $\chi(p, p-a) \pmod{p}$, when p is prime. The only known values of R_n are when $n \leq 11$, which are given in Figure 1.1.

Let p be a prime. We know that $R_n \equiv 0 \pmod{p}$ when $n \geq 2p$ by Theorem 1.1.5 and that $R_p \equiv 1 \pmod{p}$ by Corollary 2.4.4. We now also know the value of $R_n \pmod{p}$ when $p < n < 2p$ by Theorem 3.2.1. We currently do not know the value of $R_n \pmod{p}$ when $n < p$ except for $n \leq 11$, where we know R_n exactly. Our methodology cannot be extended to encompass the $p > n$ case since it is limited by the use of a group of isotopisms of cardinality that divides $n!$ ³.

We can use the following theorem to further check our computer enumerations of $\chi(n, d)$ in Figure 3.3.

Theorem 3.2.3. *Let $1 \leq d < n$. Then $d^2 / \gcd(n, d)$ divides $\chi(n, d)$.*

Proof. We will partition the set of (n, d) -partial orthomorphisms into parts of cardinalities that are divisible by $d^2 / \gcd(n, d)$. Suppose $\nu : S \rightarrow U$ is an arbitrary (n, d) -partial orthomorphism, where $U \subseteq \mathbb{Z}_n$ is the range of ν . For all $x, y \in \mathbb{Z}_n$ let $S_x = \{s + x : s \in S\}$ and $U_y = \{u + y : u \in U\}$. Define $\nu_{x,y} : S_x \rightarrow U_y$ to be the map defined by $\nu_{x,y}(s + x) \equiv \nu(s) + y \pmod{n}$ for each $s \in S$.

Call ν equivalent to $\nu_{x,y}$ if $\nu_{x,y}$ is an (n, d) -partial orthomorphism, thus defining an equivalence relation on the set of (n, d) -partial orthomorphisms. Let N denote the equivalence class containing ν . It is sufficient to show that $d^2 / \gcd(n, d)$ divides $|N|$.

To construct an (n, d) -partial orthomorphism that is equivalent to ν , we may choose any $y \in \mathbb{Z}_n \setminus \{-\nu(s) : s \in S\}$ then choose any $x \in \mathbb{Z}_n \setminus \{\nu(s) - s + y : s \in S\}$. Other choices for x and y would violate $\nu_{x,y}$ being an (n, d) -partial orthomorphism. This gives d^2 legal (n, d) -partial orthomorphisms, but they are not necessarily all distinct. However, for each $x \in \mathbb{Z}_n$ there can be at most one value of $y \in \mathbb{Z}_n$ such that $\nu = \nu_{x,y}$.

	$p = 3$	5	7	11	13	17	19
$d = 1$	1	3	19	3441	79259	94471089	4613520889
2	4	40	516	223940	7101048	14292413536	
3	1	54	1629	1971945	89669682	318490001352	
4		16	1360	5117280	341843440	2202786643008	
5		1	375	5189450	524957175	6346143586100	
6			36	2387448	380112048	8972410104288	
7			1	540470	142551780	6899440472008	
8				62400	29289024	3090449262976	
9				3645	3392685	845070847830	
10				100	222200	145573463200	80083309009000
11				1	7986	16101920120	12742629618906
12					144	1152470592	1361619013248
13					1	53126164	98471150232
14						1544480	4815882288
15						27000	157499100
16						256	3355392
17						1	44217
18							324

FIGURE 3.3: Some values of $\chi(p, d)$ for prime p in the range $3 \leq p \leq 19$.

Suppose that $\nu = \nu_{x,y} = \nu_{x',y'}$ for some $x, y, x', y' \in \mathbb{Z}_n$. Then $\nu = \nu_{ax+bx', ay+by'}$ for all $a, b \in \mathbb{Z}$. Using Euclid's Algorithm we may choose a, b such that $ax + bx' = \gcd(x, x')$. Therefore, there exists $x^*, y^* \in \mathbb{Z}_n$ such that $\nu = \nu_{x^*, y^*}$ and if $\nu = \nu_{x,y}$ for some $x, y \in \mathbb{Z}_n$ then $x = cx^*$ and $y = cy^*$ for some $c \in \mathbb{Z}_n$.

Let X be the subgroup of \mathbb{Z}_n generated by x^* . Then $|N| = d^2/|X|$. Lagrange's Theorem implies that $|X|$ divides n . We will now show that $|X|$ divides d . The group X acts on S via the map $s \mapsto s + x \pmod{n}$ for all $x \in X, s \in S$. Every orbit of S under X has size $|X|$ and therefore $|X|$ divides $n - d$. It follows that $|X|$ divides d . Therefore, $d^2/\gcd(n, d)$ divides $|N|$ and since ν was arbitrary, $d^2/\gcd(n, d)$ divides $\chi(n, d)$. \square

To illustrate Theorem 3.2.3, $\chi(6, 3) = 300$ is divisible by 3 (though not by 3^2). The $(6, 3)$ -partial orthomorphism ν defined by $\nu(0) = 1$, $\nu(2) = 5$ and $\nu(4) = 3$ is in the equivalence class $\{\sigma, \sigma_{2,4}, \sigma_{4,2}\}$.

3.2.2 Enumeration of partial orthomorphisms

Recall that $\omega(n, d)$ is the number of partial orthomorphisms of \mathbb{Z}_n of deficit d . Observe that $\omega(n, 0) = n\mathbb{Z}_n$, so assume $1 \leq d < n$. In the proof of Theorem 3.2.3, the set $C_\nu := \{\nu_{x,y} : x, y \in \mathbb{Z}_n\}$ has size $n^2/|X|$ and contains $d^2/|X|$ (n, d) -partial orthomorphisms. Since $1 \leq d < n$, every partial orthomorphism is contained in C_ν for some (n, d) -partial orthomorphism ν . Therefore, the C_ν partition the set of partial orthomorphisms of \mathbb{Z}_n . It follows that

$$\omega(n, d) = \frac{n^2}{d^2} \chi(n, d). \quad (3.2)$$

d	(mod 3)	(mod 5)	(mod 7)	(mod 11)	(mod 13)	(mod 17)	(mod 19)
$p-1$	$R_5 \equiv 2$	$R_9 \equiv 1$	$R_{13} \equiv 0$	$R_{21} \equiv 2$	$R_{25} \equiv -R_{12}$	$R_{33} \equiv -R_{16}$	$R_{37} \equiv -R_{18}$
$p-2$	$R_4 \equiv 1$	$R_8 \equiv 1$	$R_{12} \equiv 0$	$R_{20} \equiv 6$	$R_{24} \equiv 6$	$R_{32} \equiv R_{15}$	$R_{36} \equiv R_{17}$
$p-3$		$R_7 \equiv 0$	$R_{11} \equiv 3$	$R_{19} \equiv 7$	$R_{23} \equiv 6$	$R_{31} \equiv R_{14}$	$R_{35} \equiv 17R_{16}$
$p-4$		$R_6 \equiv 3$	$R_{10} \equiv 1$	$R_{18} \equiv 9$	$R_{22} \equiv 3$	$R_{30} \equiv 5R_{13}$	$R_{34} \equiv 16R_{15}$
$p-5$			$R_9 \equiv 3$	$R_{17} \equiv 10$	$R_{21} \equiv 8$	$R_{29} \equiv 3R_{12}$	$R_{33} \equiv 13R_{14}$
$p-6$			$R_8 \equiv 5$	$R_{16} \equiv 3$	$R_{20} \equiv 11$	$R_{28} \equiv 1$	$R_{32} \equiv 17R_{13}$
$p-7$				$R_{15} \equiv 6$	$R_{19} \equiv 8$	$R_{27} \equiv 8$	$R_{31} \equiv 0$
$p-8$				$R_{14} \equiv 5$	$R_{18} \equiv 5$	$R_{26} \equiv 2$	$R_{30} \equiv 2$
$p-9$				$R_{13} \equiv 4$	$R_{17} \equiv 7$	$R_{25} \equiv 7$	$R_{29} \equiv 7$
$p-10$				$R_{12} \equiv 9$	$R_{16} \equiv 4$	$R_{24} \equiv 15$	$R_{28} \equiv 5\chi$
$p-11$					$R_{15} \equiv 12$	$R_{23} \equiv 0$	$R_{27} \equiv 2\chi$
$p-12$					$R_{14} \equiv 11$	$R_{22} \equiv 11$	$R_{26} \equiv 8\chi$
$p-13$						$R_{21} \equiv 2$	$R_{25} \equiv 12\chi$
$p-14$						$R_{20} \equiv 3$	$R_{24} \equiv 2\chi$
$p-15$						$R_{19} \equiv 0$	$R_{23} \equiv 17\chi$
$p-16$						$R_{18} \equiv 15$	$R_{22} \equiv 5\chi$

FIGURE 3.4: Congruences implied by Figure 3.3 and Corollary 3.2.2, where $\chi = \chi(p, d)$.

Let $\omega_0(n, d)$ be the number of partial orthomorphisms σ of deficit d such that $\sigma(0) = 0$. Then

$$\omega_0(n, d) = \frac{(n-d)}{n^2} \omega(n, d) = \frac{(n-d)}{d^2} \chi(n, d). \quad (3.3)$$

While we use χ for the purposes of Theorem 3.2.1, for computer enumeration it is usually easiest to find ω_0 . However, for the remainder of this section we will discuss the properties of ω , and these properties can be transferred to χ and ω_0 by (3.3).

Given a partial orthomorphism σ on domain $S = \{s_1, s_2, \dots, s_a\}$ we can define a pair of vectors $\vec{s} = (s_1, s_2, \dots, s_a)$ and $\vec{u} = (u_1, u_2, \dots, u_a)$ such that $\sigma(s_i) = u_i$ for all $1 \leq i \leq a$. In fact σ defines $a!$ such pairs of vectors. For any $\vec{s}, \vec{u} \in \mathbb{Z}_n^a$, let $I(\vec{s}, \vec{u}) = 1$ if $s_i \mapsto u_i$ defines a partial orthomorphism and $I(\vec{s}, \vec{u}) = 0$ otherwise. Hence

$$a! \omega(n, n-a) = \sum_{\vec{s}, \vec{u} \in \mathbb{Z}_n^a} I(\vec{s}, \vec{u})$$

for all $a < n$. Of the n^{2a} pairs $(\vec{s}, \vec{u}) \in \mathbb{Z}_n^a \times \mathbb{Z}_n^a$ we have $I(\vec{s}, \vec{u}) = 0$ if and only if at least one of the following is true:

- (a) $u_i = u_j$ for some $1 \leq i < j \leq a$,
- (b) $s_i = s_j$ for some $1 \leq i < j \leq a$,
- (c) $u_i - s_i = u_j - s_j$ for some $1 \leq i < j \leq a$.

Let J be the set of $3a(a-1)/2$ equations of the form (a)–(c) above. For each $j \in J$ let E_j denote the set of all $(\vec{s}, \vec{u}) \in \mathbb{Z}_n^a \times \mathbb{Z}_n^a$ such that equation j is satisfied. Hence

$$a! \omega(n, n-a) = n^{2a} - \left| \bigcup_{j \in J} E_j \right|.$$

Applying Inclusion-Exclusion yields

$$a! \omega(n, n-a) = \sum_{\mathcal{E} \subseteq J} (-1)^{|\mathcal{E}|} \rho(\mathcal{E}, n), \quad (3.4)$$

where $\rho(\mathcal{E}, n) := |\cap_{j \in \mathcal{E}} E_j|$ and $\rho(\emptyset, n) := n^{2a}$. The subset \mathcal{E} corresponds to a system of linear congruences, which can be written in matrix form $XA^T = \mathbf{0}$ where

$$X = (s_1, s_2, \dots, s_a, u_1, u_2, \dots, u_a),$$

$A = A(\mathcal{E})$ is a $(-1, 0, +1)$ -matrix and $\mathbf{0}$ is the vector of $|\mathcal{E}|$ zeroes. The number of solutions of a system of linear congruences was given, for example, by Butson and Stewart [42]. In our case, the number of solutions for a given \mathcal{E} and n is

$$\rho(\mathcal{E}, n) = \gcd(e_1, n) \gcd(e_2, n) \cdots \gcd(e_r, n) n^{2a-r}, \quad (3.5)$$

where e_1, e_2, \dots, e_r are the invariant factors of A . In Figure 3.6 we will give an example of $\mathcal{E} \subset J$ with $\rho(\mathcal{E}, n) = n^2 \gcd(2, n)$ and the corresponding matrix $A(\mathcal{E})$. In Example 3.2.10 we will construct examples where ρ involves multiple gcd's.

Theorem 3.2.4. *For any a in the range $1 \leq a < n$ there exists $\mu \geq 1$ such that*

$$\omega(n, n-a) = \sum_{i=2}^{2a} \frac{(-1)^i}{a!} c_i n^i$$

for integer coefficients $c_i = c_i(a, n)$ that vary only with a and the value of $n \pmod{\mu}$.

Proof. It follows from (3.4) and (3.5) that $\omega(n, n-a) = \sum_{i=0}^{2a} \frac{(-1)^i}{a!} c_i n^i$ for integer coefficients $c_i = c_i(a, n)$ that vary only with a and the value of $n \pmod{\mu}$ for some μ depending on the invariant factors of $A(\mathcal{E})$ for $\mathcal{E} \subseteq J$.

For any $\mathcal{E} \subset J$, if (\vec{s}, \vec{u}) is a solution to the system of linear congruences $A(\mathcal{E})$ then so is $(\vec{s} + \mathbf{1}, \vec{u})$ and $(\vec{s}, \vec{u} + \mathbf{1})$, where $\mathbf{1}$ is the vector of a ones and addition is component-wise modulo n . Thus we can partition the solutions to $A(\mathcal{E})$ into equivalence classes of the form $\{(\vec{s} + k_1 \mathbf{1}, \vec{u} + k_2 \mathbf{1}) : k_1, k_2 \in \mathbb{Z}_n\}$. Therefore n^2 divides $\rho(\mathcal{E}, n)$ for all $\mathcal{E} \subset J$. This implies that $c_0 = c_1 = 0$. \square

Figure 3.5 gives the coefficients $c_i = c_i(a, n)$ of Theorem 3.2.4 for $1 \leq a \leq 6$. We discuss how these values were obtained in Section 3.2.3.

Corollary 3.2.5. *Let p be a prime and $1 \leq a < p$. Then*

$$R_{2p-a} \equiv \frac{(-1)^a c_2(a, p)}{a!(a-1)!^3} R_{p-a} \pmod{p}.$$

Proof. When $n = 2p - a$, (3.2) implies that $\chi(p, n-p) \equiv \frac{(n-p)^2}{p^2} \omega(p, n-p) \equiv (n-p)^2 c_2(a, p) \pmod{p}$ as in Theorem 3.2.4. Theorem 3.2.4 also ensures that $\omega(p, n-p)$ is divisible by p^2 . The result now follows from Theorem 3.2.1 and Wilson's Theorem. \square

Let p be a prime. Then it follows from Corollary 3.2.5, Figure 3.5 and (3.2) that

	$a = 1$	2	3	4	5	6
c_{2a}	1	1	1	1	1	1
c_{2a-1}		3	9	18	30	45
c_{2a-2}		2	30	135	395	915
c_{2a-3}			42	534	2970	11055
c_{2a-4}			20	1154	13862	87682
c_{2a-5}				1260	40740	475290
c_{2a-6}				$516 + 6 \gcd(2, n)$	$72580 + 30 \gcd(2, n)$	$1773420 + 90 \gcd(2, n)$
c_{2a-7}				$69840 + 360 \gcd(2, n)$	$4459740 + 2430 \gcd(2, n)$	
c_{2a-8}				$26112 + 960 \gcd(2, n)$	$7131232 + 24300 \gcd(2, n)$	
c_{2a-9}					$6360480 + 106200 \gcd(2, n)$	
c_{2a-10}					$2227680 + 168480 \gcd(2, n)$	$+1440 \gcd(3, n)$

FIGURE 3.5: The coefficients $c_i = c_i(a, n)$ in Theorem 3.2.4 for $1 \leq a \leq 6$.

- $R_{2p-1} \equiv -R_{p-1} \pmod{p}$ if $p \geq 2$,
- $R_{2p-2} \equiv R_{p-2} \pmod{p}$ if $p \geq 3$,
- $R_{2p-3} \equiv -\frac{5}{12}R_{p-3} \pmod{p}$ if $p \geq 5$,
- $R_{2p-4} \equiv \frac{29}{288}R_{p-4} \pmod{p}$ if $p \geq 5$,
- $R_{2p-5} \equiv -\frac{47}{2880}R_{p-5} \pmod{p}$ if $p \geq 7$,
- $R_{2p-6} \equiv \frac{37}{19200}R_{p-6} \pmod{p}$ if $p \geq 7$.

It is easy to find an exponential upper bound on the invariant factors of arbitrary $A(\mathcal{E})$, given that $|\det(M)| \leq \prod_j \sum_i |m_{ij}|$ for any square matrix $M = (m_{ij})$. We next show that the invariant factors can be exponentially large.

Example 3.2.6. For all $q \geq 0$ there exists a set of equations \mathcal{E}_q with $a = 3q + 1$ such that $\rho(\mathcal{E}_q, n) = n^2 \gcd(2^q, n)$.

Proof. Recall that we are allowed three types of equations in \mathcal{E}_q , they are: (a) $u_i = u_j$, (b) $s_i = s_j$ and (c) $u_i - s_i = u_j - s_j$ for some $1 \leq i < j \leq a$. We choose the equations of type (a) and (b) in \mathcal{E}_q so that \vec{s} and \vec{u} must have the form

$$\begin{array}{l} \vec{s} = (a_1, a_1, a_2, a_2, a_2, a_3, a_3, \dots, a_q, a_{q+1}, a_{q+1}) \\ \vec{u} = (b_1, b_2, b_2, b_1, b_3, b_3, b_2, \dots, b_{q+1}, b_{q+1}, b_q) \end{array}.$$

Now add to \mathcal{E}_q equations of type (c) such that $b_{i+1} - a_i = b_i - a_{i+1}$ for all $1 \leq i \leq q$ and $b_{i+1} - a_i = b_{i+2} - a_{i+2}$ for all $1 \leq i \leq q-1$ and $b_1 - a_1 = b_2 - a_2$. This completes the construction of \mathcal{E}_q .

For all $1 \leq i \leq q$ define $x_i = a_i - a_{i+1}$ and $y_i = b_i - b_{i+1}$. Then the equations of type (c) in \mathcal{E}_q are equivalent to (i) $x_i = -y_i$ for all $1 \leq i \leq q$, (ii) $x_i + x_{i+1} = y_{i+1}$ for all $1 \leq i \leq q-1$ and (iii) $x_1 = y_1$. From (i) and (ii) we deduce that $x_i = 2y_{i+1}$ for all $1 \leq i \leq q-1$. Since $x_1 = y_1$ and $x_1 = -y_1$ we have $2x_1 = 2y_1 = 0$. Therefore $2^q x_q = -2^{q-1} x_{q-1} = \dots = (-1)^{q-1} 2x_1 = 0$.

If we choose $x_q \in \mathbb{Z}_n$ such that $2^q x_q \equiv 0 \pmod{n}$ then we can determine the value of x_i and y_i for all $1 \leq i \leq q$. Therefore (\vec{s}, \vec{u}) is uniquely determined by the value of a_1, b_1 and x_q . In \mathbb{Z}_n there are n possible values for a_1 and b_1 and $\gcd(2^q, n)$ values of x_q satisfying $2^q x_q \equiv 0 \pmod{n}$. \square

Let μ_a be the smallest μ possible in Theorem 3.2.4 for a given value of a . Example 3.2.6 suggests that μ_a increases at least exponentially with a , although it is plausible that a dependence modulo 2^q might cancel in (3.4). In Example 3.2.10 we will give a further indication that μ_a is likely to grow quickly.

3.2.3 A graph theoretic approach

In this section we introduce a graph theoretic interpretation of the systems of linear congruences in Section 3.2.2. This will aid us in the computation of $\omega(n, n - a)$. We will work with simple graphs G , that is, undirected graphs without loops and parallel edges, on the vertex set $V(G)$ which will typically be $[a] := \{1, 2, \dots, a\}$. Let $E(G)$ be the edge set of G .

Throughout this section, by an *edge-colouring* δ of a graph G we will mean a map

$$\delta : E(G) \rightarrow \{\text{red, blue, green, black}\}.$$

By a *vertex-colouring* ϕ of the edge-coloured graph (G, δ) we will mean a map

$$\phi : V(G) \rightarrow \mathbb{Z}_n \times \mathbb{Z}_n$$

such that if we let $\phi(i) = (\phi_1(i), \phi_2(i))$ for every vertex i then for all edges ij in $E(G)$ we have:

- $\phi_1(i) = \phi_1(j)$ if $\delta(ij) = \text{red}$,
- $\phi_2(i) = \phi_2(j)$ if $\delta(ij) = \text{blue}$,
- $\phi_2(i) - \phi_1(i) = \phi_2(j) - \phi_1(j)$ if $\delta(ij) = \text{green}$ and
- $\phi(i) = \phi(j)$ if $\delta(ij) = \text{black}$.

We do not require δ or ϕ to be proper colourings. Let $\rho(G, \delta, n)$ be the number of vertex-colourings of (G, δ) .

Given $\mathcal{E} \subseteq J$, as in Section 3.2.2, let $(G, \delta)_{\mathcal{E}}$ be the edge-coloured graph on vertex set $[a]$ with edges defined in the following way:

- I: If $u_i = u_j$ is in \mathcal{E} then add a red edge between i and j .
- II: If $s_i = s_j$ is in \mathcal{E} then add a blue edge between i and j .
- III: If $u_i - s_i = u_j - s_j$ is in \mathcal{E} then add a green edge between i and j .
- IV: Replace any parallel edges resulting from I–III with a single black edge.

Then $\rho(\mathcal{E}, n) = \rho(G, \delta, n)$ where $(G, \delta) = (G, \delta)_{\mathcal{E}}$. In Figure 3.6 we give an example of a set of equations $\mathcal{E} \subset J$ with its corresponding matrix $A(\mathcal{E})$ and edge-coloured graph $(G, \delta)_{\mathcal{E}}$.

For any (G, δ) , let $J_{G, \delta} = \{\mathcal{E} \subseteq J : (G, \delta)_{\mathcal{E}} = (G, \delta)\}$ and let $b(\delta)$ be the number of black edges. A black edge arises if all three of I, II and III occur. It can also arise in 3 distinct ways

when precisely two of I, II and III occur. In the former case $|\mathcal{E}|$ is 1 larger than in the latter case. Hence, by (3.4),

$$\begin{aligned}
 a! \omega(n, n-a) &= \sum_{(G, \delta)} \sum_{\mathcal{E} \in J_{G, \delta}} (-1)^{|\mathcal{E}|} \rho(G, \delta, n) \\
 &= \sum_{(G, \delta)} \rho(G, \delta, n) \sum_{\mathcal{E} \in J_{G, \delta}} (-1)^{|\mathcal{E}|} \\
 &= \sum_{(G, \delta)} \rho(G, \delta, n) (-1)^{|E(G)|+b(\delta)} \sum_{x \geq 0} \binom{b(\delta)}{x} (-1)^x 3^{b(\delta)-x} \\
 &= \sum_{(G, \delta)} \rho(G, \delta, n) (-1)^{|E(G)|} (-2)^{b(\delta)} \tag{3.6}
 \end{aligned}$$

using the Binomial Theorem, where the dummy variable x counts the number of black edges where I, II and III all hold.

equations	s_1	s_2	s_3	s_4	u_1	u_2	u_3	u_4
$u_1 = u_2$	0	0	0	0	1	-1	0	0
$u_3 = u_4$	0	0	0	0	0	0	1	-1
$s_1 = s_3$	1	0	-1	0	0	0	0	0
$s_2 = s_4$	0	1	0	-1	0	0	0	0
$u_1 - s_1 = u_4 - s_4$	-1	0	0	1	1	0	0	-1
$u_2 - s_2 = u_3 - s_3$	0	-1	1	0	0	1	-1	0

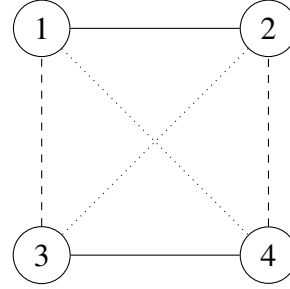


FIGURE 3.6: A set of equations $\mathcal{E} \subset J$, its corresponding matrix $A(\mathcal{E})$ and corresponding graph $(G, \delta)_{\mathcal{E}}$. Red edges are solid, blue edges are dashed and green edges are dotted.

For computational purposes, we split (3.6) as follows:

$$a! \omega(n, n-a) = \sum_{G \in I} \frac{a!}{|\text{Aut}(G)|} \sum_{\delta} (-1)^{|E(G)|} (-2)^{b(\delta)} \rho(G, \delta, n), \tag{3.7}$$

where I is a set containing one representative from each isomorphism class of (uncoloured) graphs on a vertices and $\text{Aut}(G)$ is the automorphism group of the graph G . In the second summation in (3.7) we sum over all edge-colourings δ of G of which there are $4^{|E(G)|}$, which requires a lengthy computation when $|E(G)|$ is large. However, when $|E(G)|$ is large there are comparatively few vertex-colourings. This means that (3.7) is particularly useful for computing the leading terms in $\omega(n, n-a)$, which is what we will do in Theorem 3.2.9.

For any graph G without isolated vertices, define

$$P_G(a) = n^{2(a-v)} \sum_{\delta} (-2)^{b(\delta)} \rho(G, \delta, n), \tag{3.8}$$

where v is the number of vertices of G and the sum is over all edge-colourings of G . Suppose G is the graph formed by removing every isolated vertex from a graph H with a vertices. Then $\rho(H, \delta, n) = n^{2(a-v)} \rho(G, \delta, n)$, so the contributions to (3.7) by H can be handled using $P_G(a)$. For all $e \geq 0$ and $v \geq 0$, let $\Gamma_{e,v}$ be a set containing one representative from each

isomorphism class of graphs on v vertices with e edges without isolated vertices. Then it follows from (3.7) and (3.8) that

$$a! \omega(n, n-a) = \sum_{v \geq 0} \sum_{e \geq 0} \sum_{G \in \Gamma_{e,v}} \frac{(-1)^e}{|\text{Aut}(G)|} a(a-1) \cdots (a-v+1) P_G(a). \quad (3.9)$$

We will now identify a necessary condition for a graph G to contribute to the coefficient of n^{2a-i} in $\omega(n, n-a)$. A *spanning forest* of G is a subgraph consisting of a spanning tree in each connected component of G .

Lemma 3.2.7. *The coefficient of n^{2a-i} in $P_G(a)$ can be non-zero only if G contains a spanning forest of between $\lceil i/2 \rceil$ and i edges inclusive. Moreover, for all $i \geq 0$, $c_{2a-i}(a, n)$ is a multivariate polynomial of degree at most $2i$ in a with variables $a, \gcd(2, n), \gcd(3, n), \dots, \gcd(c, n)$ for some $c \geq 1$.*

Proof. Each $(G, \delta) = (G, \delta)_{\mathcal{E}}$ for some $\mathcal{E} \in J_{G, \delta}$. Consequently $\rho(G, \delta, n)$ has the form

$$\gcd(e_1, n) \gcd(e_2, n) \cdots \gcd(e_r, n) n^{2a-r} = O(1) n^{2a-r}$$

for some integers e_1, e_2, \dots, e_r , corresponding to (3.5).

Let (F, δ_F) be a spanning forest of (G, δ) , where $\delta_F(ij) = \delta(ij)$ for all edges ij of F . Let f be the number of edges of F . Any vertex-colouring of (G, δ) is also a vertex-colouring of (F, δ_F) . Hence $\rho(G, \delta, n) \leq \rho(F, \delta_F, n) \leq n^{2a-f}$ for all n .

Let δ_{black} be the edge-colouring of G with all black edges. Any vertex-colouring of $(G, \delta_{\text{black}})$ is also a vertex-colouring of (G, δ) . Hence $\rho(G, \delta, n) \geq \rho(G, \delta_{\text{black}}, n) \geq n^{2a-2f}$ for all n . Thus $n^{2a-f} \geq \rho(G, \delta, n) \geq n^{2a-2f}$ for all n , implying $f \leq r \leq 2f$.

The second statement in the lemma now follows from (3.5), (3.8) and (3.9). \square

For Corollary 3.2.5, $c_2(a, p)$ can therefore be calculated by studying only the graphs containing a spanning forest of between $a-1$ and $2a-2$ edges inclusive. The converse of the first statement in Lemma 3.2.7 is false; a counter-example is given in Figure 3.7. The complete graph on 4 vertices does not contribute to the coefficient of n^{2a-4} due to cancellation.

Lemma 3.2.7 implies that $c_{2a-i}(a, n) = 0$ when $a \in \{0, 1, \dots, \lceil i/2 \rceil\}$ for all $i \geq 1$ and all n . Furthermore, in Theorem 3.2.9 we find that these are the only integer zeroes of $c_{2a-i}(a, n)$ when $2 \leq i \leq 4$.

Suppose a graph G has a non-zero coefficient of $a^{2i} n^{2a-i}$ in the summand in (3.9). Then G does not have any isolated vertices, G has at most i edges by Lemma 3.2.7 and G has at least $2i$ vertices by (3.9). So G is a one-factor on $2i$ vertices. For an edge-colouring δ of G to have a non-zero coefficient of n^{2a-i} in $P_G(a)$ in (3.8), it must not have a black edge. There are 3^i edge-colourings δ of G without black edges. In Lemma 3.2.7 we observed that $c_{2a-i}(a, n)$ has degree at most $2i$ in a . Therefore

$$c_{2a-i}(a, n) \sim \frac{3^i}{|\text{Aut}(G)|} a(a-1) \cdots (a-2i+1) \sim \frac{3^i a^{2i}}{i! 2^i},$$

for fixed i as $a \rightarrow \infty$ independent of n . This additionally implies that $c_{2a-i}(a, n)$ has a positive leading term.

Lemma 3.2.8. *Let G and H be graphs and let R be any graph formed by identifying a vertex of G and a vertex of H . Then $\frac{1}{n^{2a}} P_G(a) P_H(a) = P_{G \cup H}(a) = n^2 P_R(a)$.*

Proof. To begin, observe that $\rho(G \cup H, \delta, n) = \rho(G, \delta_G, n)\rho(H, \delta_H, n)$, where δ is an edge-colouring of $G \cup H$ and δ_G and δ_H are the edge-colourings on G and H induced by δ , respectively. Therefore (3.8) implies

$$\begin{aligned} P_{G \cup H}(a) &= n^{2(a-v)} \sum_{\delta_G} \sum_{\delta_H} (-2)^{b(\delta_G)+b(\delta_H)} \rho(G, \delta_G, n) \rho(H, \delta_H, n) \\ &= n^{2(a-v)} \left(\sum_{\delta_G} (-2)^{b(\delta_G)} \rho(G, \delta_G, n) \right) \left(\sum_{\delta_H} (-2)^{b(\delta_H)} \rho(H, \delta_H, n) \right) \\ &= \frac{1}{n^{2a}} P_G(a) P_H(a), \end{aligned} \quad (3.10)$$

where v is the number of vertices in $G \cup H$, δ is any edge-colouring of $G \cup H$ and δ_G and δ_H are any edge-colourings on G and H .

To prove that $P_{G \cup H}(a) = n^2 P_R(a)$, first let δ_G and δ_H be any edge-colourings of G and H , respectively. Let g be a vertex of G and h be a vertex of H . Let ϕ be a vertex-colouring of (H, δ_H) . For each $k_1, k_2 \in \mathbb{Z}_n$ the map $i \mapsto \phi(i) + (k_1, k_2)$ is also a vertex-colouring of (H, δ_H) . Thus we can partition the vertex-colourings of (H, δ_H) into n^2 parts of size $\frac{1}{n^2} \rho(H, \delta_H, n)$ according to the colour of h .

Given a vertex-colouring of (G, δ_G) , there are therefore $\frac{1}{n^2} \rho(H, \delta_H, n)$ vertex-colourings of (H, δ_H) such that g and h receive the same colour. Let δ_R be the edge-colouring of R induced by δ_G and δ_H . So

$$\rho(R, \delta_R, n) = \frac{1}{n^2} \rho(G, \delta_G, n) \rho(H, \delta_H, n). \quad (3.11)$$

By (3.8),

$$n^2 P_R(a) = n^{2(a-v)} \sum_{\delta_G} \sum_{\delta_H} (-2)^{b(\delta_G)+b(\delta_H)} \rho(G, \delta_G, n) \rho(H, \delta_H, n)$$

which is (3.10). \square

A graph is called *biconnected* if it is a connected graph and the deletion of any vertex leaves the graph connected. Lemmata 3.2.7 and 3.2.8 and (3.9) together imply that to find an equation for $c_{2a-i}(a, n)$ we only need:

- (a) A list of graph isomorphism class representatives G without isolated vertices, containing a spanning forest of between $\lceil i/2 \rceil$ and i edges inclusive,
- (b) $|\text{Aut}(G)|$ for the graphs listed in (a) and
- (c) $P_G(a)$ for the graphs listed in (a) that are biconnected.

Obtaining these items can be made easier with use of *nauty* [220], *GAP* [127] and *GRAPE* [295], for example.

We have now developed the theory for the enumeration of partial orthomorphisms that will enable us to find the leading terms in a formula for $\omega(n, n-a)$ in Theorem 3.2.9. Using (3.8) and (3.9) we computed all of the coefficients $c_i(a, n)$ for $1 \leq a \leq 5$ as given in Figure 3.5. These were independently verified by Ian Wanless (private communication) by computer enumeration and polynomial fitting. For $a = 6$, after using Theorem 3.2.9 we are left with six unknown coefficients. Ian Wanless (private communication) found $\chi(n, n-6)$ by computer

enumeration for $n \leq 51$ which provided more than enough data points to use polynomial fitting to obtain the coefficients for $a = 6$ in Figure 3.5. The excess data points provided a check of the result. The author verified these values by an independent computer enumeration for $n \leq 25$.

The following theorem gives the polynomial c_{2a-i} for $0 \leq i \leq 4$.

Theorem 3.2.9. $a! \omega(n, n-a) = n^{2a} - \frac{3}{2}a(a-1)n^{2a-1} + \frac{1}{8}a(a-1)(9a^2 - 13a - 2)n^{2a-2} - \frac{1}{16}a(a-1)(a-2)(9a^3 - 12a^2 - 5a - 8)n^{2a-3} + \frac{1}{1920}a(a-1)(a-2)(405a^5 - 1485a^4 + 825a^3 - 483a^2 + 2346a + 3304)n^{2a-4} + O(n^{2a-5})$ for fixed a as $n \rightarrow \infty$.

Proof. Figure 3.7 contains the graphs G , as identified by Lemma 3.2.7, such that $P_G(a)$ has a leading term at least n^{2a-3} . Therefore we can use (3.9) to obtain the first four coefficients. The data for the coefficient of n^{2a-4} can be found in Appendix A.5. \square

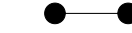
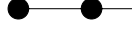









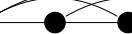
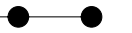

G	v	e	$ \text{Aut}(G) $	$P_G(a)$
	0	0	1	n^{2a}
	2	1	2	$3n^{2a-1} - 2n^{2a-2}$
	3	2	2	$9n^{2a-2} - 12n^{2a-3} + 4n^{2a-4}$
	3	3	6	$3n^{2a-2} + 6n^{2a-3} - 8n^{2a-4}$
	4	2	8	$9n^{2a-2} - 12n^{2a-3} + 4n^{2a-4}$
	4	3	2	$27n^{2a-3} - 54n^{2a-4} + 36n^{2a-5} - 8n^{2a-6}$
	4	3	6	$27n^{2a-3} - 54n^{2a-4} + 36n^{2a-5} + 8n^{2a-6}$
	4	4	2	$9n^{2a-3} + 12n^{2a-4} - 36n^{2a-5} + 16n^{2a-6}$
	4	4	8	$3n^{2a-3} + 54n^{2a-4} - 120n^{2a-5} + 64n^{2a-6}$
	4	5	4	$3n^{2a-3} + 18n^{2a-4} - 12n^{2a-5} - 8n^{2a-6}$
	4	6	24	$3n^{2a-3} + 36n^{2a-5} + (6 \gcd(2, n) - 44)n^{2a-6}$
	5	3	4	$27n^{2a-3} - 54n^{2a-4} + 36n^{2a-5} + 8n^{2a-6}$
	5	4	12	$9n^{2a-3} + 12n^{2a-4} - 36n^{2a-5} + 16n^{2a-6}$
	6	3	48	$27n^{2a-3} - 54n^{2a-4} + 36n^{2a-5} + 8n^{2a-6}$

FIGURE 3.7: The value of $P_G(a)$ for all $G \in \Gamma_{e,v}$ such that $P_G(a)$ has degree at least $2a - 3$ in n .

Another outcome of Lemma 3.2.8 is that it allows us to build explicit examples that realise the full generality of (3.5).

Example 3.2.10. Let (m_i) be a finite sequence of positive integers. Then there exists an edge-coloured graph (M^*, δ^*) such that $\rho(M^*, \delta^*, n) = n^2 \prod_i \gcd(m_i, n)$.

Proof. We begin by identifying, for each $m \geq 1$, an edge-coloured graph (G, δ) that has $\rho(G, \delta, n) = n^2 \gcd(m, n)$. If $m = 1$ we can take the graph consisting of one vertex, so assume $m \geq 2$.

Let the vertex set of G be $\{v_1, v_2, \dots, v_m\} \cup \{v'_1, v'_2, \dots, v'_m\}$. Thus G has $2m$ vertices. Join the vertices v_1, v_2, \dots, v_m by a red path. Join the vertices v'_1, v'_2, \dots, v'_m by a red path. For

each $1 \leq j \leq m$, join v_j to v'_j with a blue edge. Let γ be the m -cycle $(1, 2, \dots, m)$. For each $1 \leq j \leq m$, join v_j to $v'_{\gamma(j)}$ with a green edge. This completes our construction. We illustrate this construction in Figure 3.8 when $m = 5$.

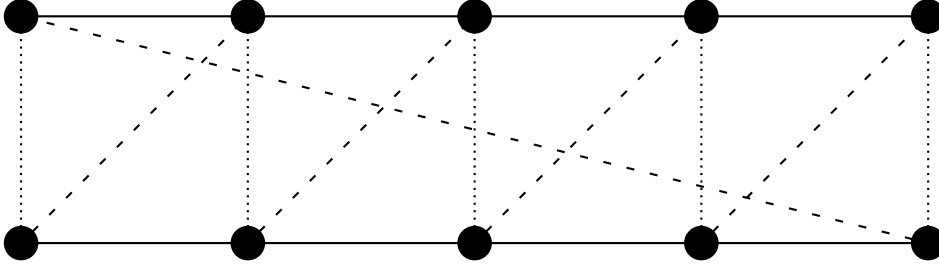


FIGURE 3.8: An edge-coloured graph (G, δ) with $\rho(G, \delta, n) = n^2 \gcd(5, n)$.

Now consider the number of vertex-colourings of (G, δ) . By the placement of the red and blue edges, for each $1 \leq j \leq m$, we can let (s_j, x) be the colour of vertex v_j and let (s_j, y) be the colour of vertex v'_j . The green edges imply that $x - s_j = y - s_{\gamma(j)}$ for all $1 \leq j \leq m$. Hence $\sum_{1 \leq j \leq m} x - s_j = \sum_{1 \leq j \leq m} y - s_{\gamma(j)} = \sum_{1 \leq j \leq m} y - s_j$ and so $mx \equiv my \pmod{n}$. Furthermore $s_1 - s_{\gamma(1)} = s_2 - s_{\gamma(2)} = \dots = s_m - s_{\gamma(m)} = x - y$. Therefore the values of x, y and s_1 determine the entire vertex-colouring. We can choose any value for x and s_1 in \mathbb{Z}_n and then we can choose $y \in \mathbb{Z}_n$ such that $mx \equiv my \pmod{n}$. Hence $\rho(G, \delta, n) = n^2 \gcd(m, n)$.

For each i , let (M_i, δ_i) be a graph with $\rho(M_i, \delta_i, n) = n^2 \gcd(m_i, n)$. Pick one vertex of each M_i and construct a new graph (M^*, δ^*) by identifying those vertices. Now (3.11) implies the stated result. \square

We will finish this section by identifying another property of the coefficients of the polynomials in Theorem 3.2.4.

Theorem 3.2.11. *For $0 \leq i \leq 5$, c_{2a-i} is a polynomial in a of degree $2i$ and $c_{2a-6} = 6\binom{a}{4} \gcd(2, n) + f(a)$ for some polynomial f of degree 12.*

Proof. Recall that $\rho(G, \delta, n)$ has the form given in (3.5) for any edge-coloured graph (G, δ) . Let (G^*, δ^*) be the graph in Figure 3.6 with the addition of some isolated vertices. Let a be the number of vertices in G^* . Then $\rho(G^*, \delta^*, n) = n^{2a-6} \gcd(2, n)$.

Assume that (G, δ) is an edge-coloured graph such that $\rho(G, \delta, n)$ is not a power of n but is divisible by n^{2a-r} where $r \leq 6$.

Case I: G is connected. Since r is at least the number of edges in the largest forest in G , Lemma 3.2.7 implies that G has no more than 7 vertices. We inspect the connected graphs G with no more than 7 vertices and find that (G, δ) must be isomorphic to (G^*, δ^*) without isolated vertices.

Case II: G is disconnected. Lemma 3.2.8 and Case I imply that G has a component isomorphic to G^* . In fact, since $r \leq 6$, (G, δ) is isomorphic to (G^*, δ^*) .

There are $6\binom{a}{4}$ graphs (G, δ) isomorphic to (G^*, δ^*) , and each of them satisfies $\rho(G, \delta, n) = n^{2a-6} \gcd(2, n)$. The result now follows from (3.6). \square

By combining the results of Figure 3.4, Theorem 1.1.5 and Theorem 2.7.2 we obtain, for example, that

- $R_{12} \equiv 50400 \pmod{55440}$,
- $R_{13} \equiv 342720 \pmod{720720}$,
- $R_{14} \equiv 428400 \pmod{720720}$,
- $R_{15} \equiv 8830080 \pmod{17297280}$,
- $R_{16} \equiv 7136640 \pmod{17297280}$,
- $R_{17} \equiv 95437440 \pmod{882161280}$.

3.3 Compound orthomorphisms

In this section we identify a special class of orthomorphisms which we will use to provide another congruence for R_n . We follow the work of [304].

Suppose d is a divisor of n . If σ is an orthomorphism such that $\sigma(i) \equiv \sigma(j) \pmod{d}$ whenever $i \equiv j \pmod{d}$ then we call σ a d -compound orthomorphism. All orthomorphisms of \mathbb{Z}_n are trivially 1-compound and n -compound. We call σ a *compound* orthomorphism if it is d -compound for some proper divisor d of n . If D is a subset of the divisors of n , we say σ is D -compound if σ is d -compound for all $d \in D$.

As we shall see, compound orthomorphisms are a natural and useful class of orthomorphism. A construction of van Rees [316] for “toroidal Latin queen squares” gives rise to a Latin square in which every row, column and broken diagonal (forward and backward) defines a compound orthomorphism. Evans [100, 112] has used 3-compound orthomorphisms in the construction of orthogonal orthomorphisms of \mathbb{Z}_{3p} for prime p . We will discuss orthogonal orthomorphisms in Section 3.3.5.

Let n be an odd number. If $c \in \mathbb{Z}_n$ such that $\gcd(c, n) = 1$ and $\gcd(c - 1, n) = 1$ we can define an orthomorphism $\eta_{c,n}$ by $\eta_{c,n}(i) \equiv ci \pmod{n}$ for all $i \in \mathbb{Z}_n$, which is called a *linear* orthomorphism. Recall that the translation $T_d[\sigma]$ of an orthomorphism σ is defined by $T_d[\sigma](i) = \sigma(i + d) - \sigma(d)$. Linear orthomorphisms $\eta_{c,n}$ satisfy $T_g[\eta_{c,n}] = \eta_{c,n}$ for all $T_g \in \mathcal{G}$ where \mathcal{G} is the group of translations. Clark and Lewis [59] showed that the number of linear orthomorphisms of \mathbb{Z}_n is given by

$$\prod_{p \in \mathbb{P}_n} p^{a-1}(p-2) \quad (3.12)$$

where \mathbb{P}_n is the set of prime divisors of n and $a = a(p, n)$ is the largest integer such that p^a divides n .

Suppose $n = dt$ is odd. Let μ be a canonical orthomorphism of \mathbb{Z}_d . For all $i \in \mathbb{Z}_d$, let σ_i be an orthomorphism of \mathbb{Z}_t and ensure σ_0 is canonical. Define the canonical d -compound orthomorphism $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ of \mathbb{Z}_n by

$$\kappa(i) \equiv \mu(i) + d\sigma_i(\lfloor i/d \rfloor) \pmod{n} \quad (3.13)$$

for all $i \in \mathbb{Z}_n$. When $d = 1$ we have $\kappa = \sigma_0$ and when $t = 1$ we have $\kappa = \mu$.

Formally, the ranges of μ and σ_i are \mathbb{Z}_d and \mathbb{Z}_t respectively, but we will implicitly equate them with $\{0, 1, \dots, d-1\} \subset \mathbb{Z}_n$ and $\{0, 1, \dots, t-1\} \subset \mathbb{Z}_n$ respectively by replacing each congruence class by its least non-negative representative. There are some examples of compound orthomorphisms of \mathbb{Z}_{27} in Figure 3.9.

We now argue that any κ defined by (3.13) is indeed an orthomorphism by showing $\kappa(i) - i \neq \kappa(j) - j$ whenever $i \neq j$. If $i \not\equiv j \pmod{d}$ then $\kappa(i) - i \equiv \mu(i) - i \not\equiv \mu(j) - j \equiv \kappa(j) - j \pmod{d}$ since μ is an orthomorphism of \mathbb{Z}_d . So assume $i \equiv j \pmod{d}$ and $i \neq j$. Without loss

of generality, let $i = dk_1 + c$ and $j = dk_2 + c$ where $k_1 = \lfloor i/d \rfloor$ and $k_2 = \lfloor j/d \rfloor$. Observe $k_1 \not\equiv k_2 \pmod{t}$. So $\kappa(i) - i \equiv \mu(c) + d\sigma_c(k_1) - dk_1 - c \pmod{n}$ and $\kappa(j) - j \equiv \mu(c) + d\sigma_c(k_2) - dk_2 - c \pmod{n}$. Therefore $\kappa(i) - i \not\equiv \kappa(j) - j \pmod{n}$ since $\sigma_c(k_1) - k_1 \not\equiv \sigma_c(k_2) - k_2 \pmod{t}$.

κ	$= \kappa_{3,9}[(0)(14287356), (0)(13645)(287), (0)(18)(256)(374); \eta_{2,3}]$
κ'	$= \kappa_{9,3}[\eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}; (0)(15382)(467)]$
κ''	$= \kappa_{3,9}[\eta_{2,9}, (01)(28)(37)(46)(5), (053268)(1)(47); \eta_{2,3}]$
	$= \kappa_{9,3}[\eta_{2,3}, \eta_{2,3}, (01)(2), \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, (01)(2), (02)(1), (02)(1); (0)(154278)(36)]$

FIGURE 3.9: Some compound orthomorphisms of \mathbb{Z}_{27} using the notation (3.13).

We will now identify some properties of compound orthomorphisms. The following property shows that (3.13) is sufficient to describe all canonical d -compound orthomorphisms.

Property 3.3.1. *Let $n = dt$. Every canonical d -compound orthomorphism κ of \mathbb{Z}_n is of the form (3.13). Hence there are exactly $t^{d-1}z_d z_t^d$ canonical d -compound orthomorphisms of \mathbb{Z}_n .*

Proof. We know $\kappa(i) \equiv \kappa(j) \pmod{d}$ if and only if $i \equiv j \pmod{d}$. Therefore we can define μ by $\mu(i) \equiv \kappa(i) \pmod{d}$ for $i \in \mathbb{Z}_d$.

Let $\langle d \rangle$ be the subgroup of \mathbb{Z}_n generated by $d \pmod{n}$. Define the isomorphism $I : \mathbb{Z}_t \rightarrow \langle d \rangle$ by $I(j) = dj$. For all $i \in \mathbb{Z}_d$ define $\tau_i : \langle d \rangle \rightarrow \langle d \rangle$ by $\tau_i(j) = \kappa(j+i) - \mu(i)$ for all $j \in \langle d \rangle$. Therefore we can define $\sigma_i : \mathbb{Z}_t \rightarrow \mathbb{Z}_t$ by $\sigma_i(j) = I^{-1}\tau_i I(j)$. The orthomorphism properties for μ and each σ_i are inherited from κ .

We can therefore construct every d -compound orthomorphism of \mathbb{Z}_n by a choice of (a) σ_0 from one of the z_d canonical orthomorphisms of \mathbb{Z}_d , (b) σ_0 from one of the z_t canonical orthomorphisms of \mathbb{Z}_t and (c) $\sigma_1, \sigma_2, \dots, \sigma_{d-1}$ from the tz_t orthomorphisms of \mathbb{Z}_t . \square

In Figure 3.10 we plot the known non-zero values of z_n and the number of 3-compound and 5-compound orthomorphisms of \mathbb{Z}_n .

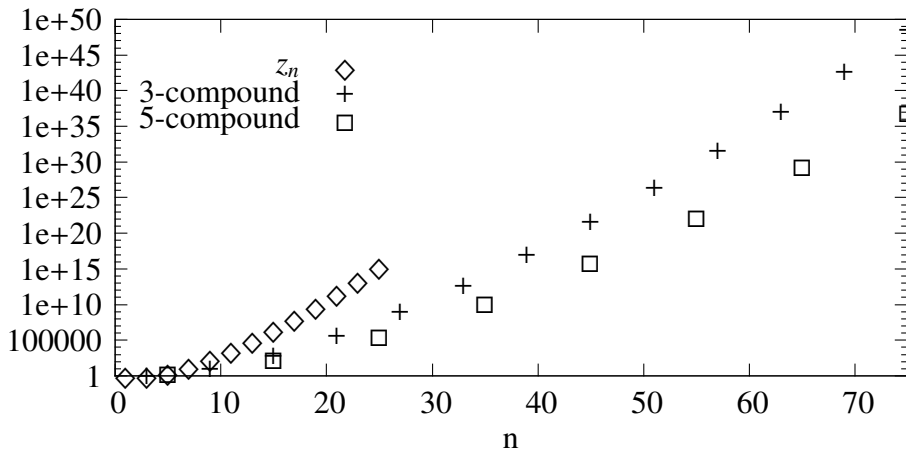


FIGURE 3.10: The value of z_n for odd $1 \leq n \leq 25$ and the number of canonical d -compound orthomorphisms of \mathbb{Z}_n for odd $n \leq 75$ such that d divides n and $d \in \{3, 5\}$, on a logarithmic scale.

Property 3.3.2. *If κ is a $\{d_1, d_2\}$ -compound orthomorphism of \mathbb{Z}_n then κ is an $\text{lcm}(d_1, d_2)$ -compound orthomorphism.*

Proof. Assume, seeking a contradiction, that $i, j \in \mathbb{Z}_n$ are such that $i \equiv j \pmod{\text{lcm}(d_1, d_2)}$ but $\kappa(i) \not\equiv \kappa(j) \pmod{\text{lcm}(d_1, d_2)}$. Then either $\kappa(i) \not\equiv \kappa(j) \pmod{d_1}$ or $\kappa(i) \not\equiv \kappa(j) \pmod{d_2}$. Since κ is $\{d_1, d_2\}$ -compound, either $i \not\equiv j \pmod{d_1}$ or $i \not\equiv j \pmod{d_2}$, giving a contradiction. \square

The converse of Property 3.3.2 is false; for example most orthomorphisms of \mathbb{Z}_{15} are not $\{3, 5\}$ -compound, but all are trivially 15-compound. Figure 3.9 lists three examples of orthomorphisms of \mathbb{Z}_{27} where (a) κ is 3-compound but not 9-compound, (b) κ' is 9-compound but not 3-compound and (c) κ'' is $\{3, 9\}$ -compound but not linear.

Property 3.3.3. *Let d be a divisor of n and let σ be an orthomorphism of \mathbb{Z}_n . If $T_d[\sigma] = \sigma$ then σ is d -compound.*

Proof. To begin, observe that

$$\begin{aligned} \sigma(i + (j + 1)d) - \sigma(i + jd) &= T_d[\sigma](i + jd) - T_d[\sigma](i + (j - 1)d) \\ &= \sigma(i + jd) - \sigma(i + (j - 1)d), \end{aligned}$$

for any $i, j \in \mathbb{Z}_n$, since $T_d[\sigma] = \sigma$. Therefore $\sigma(i + (j + 1)d) - \sigma(i + jd) = \sigma(i + d) - \sigma(i)$ for all $i, j \in \mathbb{Z}_n$. Hence

$$\frac{n}{d}(\sigma(i + d) - \sigma(i)) \equiv \sum_{j=0}^{n/d-1} (\sigma(i + (j + 1)d) - \sigma(i + jd)) \equiv 0 \pmod{n}.$$

Therefore d divides $\sigma(i + d) - \sigma(i)$ and also divides

$$\sum_{j=0}^{k-1} (\sigma(i + d) - \sigma(i)) \equiv \sum_{j=0}^{k-1} (\sigma(i + (j + 1)d) - \sigma(i + jd)) \equiv \sigma(i + kd) - \sigma(i) \pmod{n}$$

for all $k \geq 1$. Thus $\sigma(i + kd) \equiv \sigma(i) \pmod{d}$ for all $k \geq 1$, which implies that σ is d -compound. \square

The converse of Property 3.3.3 is false; for example, in Figure 3.9, $T_3[\kappa] \neq \kappa$ while κ is 3-compound.

Property 3.3.4. *Let σ be an orthomorphism of \mathbb{Z}_n such that $T_d[\sigma] = \sigma$. Then $T_{\gcd(d, n)}[\sigma] = \sigma$ and hence $T_{d'}[\sigma] = \sigma$ for all d' that are divisible by $\gcd(d, n)$.*

Proof. This follows since the group of translations \mathcal{G} is isomorphic to \mathbb{Z}_n . \square

Property 3.3.5. *A canonical orthomorphism σ of \mathbb{Z}_n is linear if and only if $T_1[\sigma] = \sigma$. Moreover, linear orthomorphisms $\eta_{c, n}$ satisfy $T_d[\eta_{c, n}] = \eta_{c, n}$ for all d .*

Proof. If $\sigma = \eta_{c, n}$ is linear, then $T_1[\eta_{c, n}](i) = \eta_{c, n}(i + 1) - \eta_{c, n}(1) = c \cdot (i + 1) - c = ci = \eta_{c, n}(i)$ for all i . Hence linear orthomorphisms satisfy $T_1[\sigma] = \sigma$. Property 3.3.4 implies that $T_d[\eta_{c, n}] = \eta_{c, n}$ for all d .

So now assume that $T_1[\sigma] = \sigma$ for some arbitrary orthomorphism σ of \mathbb{Z}_n . For all $i \in \mathbb{Z}_n$, $\sigma(i) = T_1[\sigma](i) = \sigma(i + 1) - \sigma(1)$. Therefore $\sigma(i + 1) - \sigma(i) = \sigma(1)$ for all i . Since σ is canonical, $\sigma(i) = \sigma(0) + \sum_{j=0}^{i-1} (\sigma(j + 1) - \sigma(j)) = \sigma(1)i$ for all i , implying $\sigma = \eta_{\sigma(1), n}$. \square

Therefore, Property 3.3.3 implies that linear orthomorphisms are d -compound for all divisors d of n , a notion we will explore in Section 3.3.3.

3.3.1 Evaluating $z_n \pmod{n}$

In this section we find the value of $z_n \pmod{n}$ for all n . The value of $z_n \pmod{n}$ for odd $n \leq 25$ is listed in Figure 3.2 on page 71. Clark and Lewis [59] proved that $z_n \equiv -2 \pmod{n}$ for prime n . Since their proof is brief, we have incorporated it into the proof of Theorem 3.3.6. The main objective of this section is therefore to show that $z_n \equiv 0 \pmod{n}$ when n is an odd composite number.

Theorem 3.3.6. *If n is prime, then $z_n \equiv -2 \pmod{n}$. If n is composite then $z_n \equiv 0 \pmod{n}$.*

Proof. When n is even $z_n = 0$ and the theorem holds, so assume that n is odd. First assume n is an odd prime number. Let σ be an arbitrary canonical orthomorphism of \mathbb{Z}_n . Since n is prime, $|\mathcal{G}(\sigma)| \in \{1, n\}$, where $\mathcal{G}(\sigma) = \{T_g[\sigma] : T_g \in \mathcal{G}\}$ is the orbit of σ . If $|\mathcal{G}(\sigma)| = 1$ then σ is a linear orthomorphism by Property 3.3.5. There are precisely $n - 2$ linear orthomorphisms of \mathbb{Z}_n by (3.12). Therefore $z_n \equiv -2 \pmod{n}$. This case was formerly proved in [59]. For the remainder of the proof, we assume that n is an odd composite number.

Claim: Let C be the set of canonical compound orthomorphisms of \mathbb{Z}_n . Then $z_n \equiv |C| \pmod{n}$.

The group of translations \mathcal{G} acts on the set of canonical orthomorphisms of \mathbb{Z}_n . Let σ denote an arbitrary canonical orthomorphism. By the Orbit-Stabiliser Theorem $n = |\mathcal{G}| = |\mathcal{G}(\sigma)||\mathcal{G}_\sigma|$ where $\mathcal{G}_\sigma = \{T_g \in \mathcal{G} : T_g[\sigma] = \sigma\}$ is the stabiliser of σ . Hence $|\mathcal{G}(\sigma)| = n$ unless there exists $T_d \in \mathcal{G}_\sigma$ such that $d \not\equiv 0 \pmod{n}$. Since $T_d \in \mathcal{G}_\sigma$ implies $T_{\gcd(d,n)} \in \mathcal{G}_\sigma$ by Property 3.3.4, we can assume $d = \gcd(d, n)$, that is, d divides n . If $d = 1$ then σ is a linear orthomorphism by Property 3.3.5 and so, since n is composite, σ is a compound orthomorphism by Properties 3.3.3 and 3.3.4. If $d > 1$ then Property 3.3.3 implies that σ is d -compound and $1 < d < n$. The claim follows since C is closed under the action of \mathcal{G} .

Let p be an arbitrary prime divisor of n and suppose $n = p^a t$ for some t indivisible by p . It is now sufficient to show that p^a divides $|C|$. The group of translations \mathcal{G} acts on C . Since we wish to enumerate modulo p^a , we may disregard the orbits that have cardinality divisible by p^a . Let $\kappa \in C$ such that $|\mathcal{G}(\kappa)|$ is indivisible by p^a . Then p divides $|\mathcal{G}_\kappa|$, by the Orbit-Stabiliser Theorem. By Sylow's First Theorem, there exists $T_g \in \mathcal{G}_\kappa$ of order p , that is, g satisfies $pg \equiv 0 \pmod{n}$. Equivalently, $p^{a-1}t$ divides g . Property 3.3.4 implies that $T_{\gcd(g,n)} \in \mathcal{G}_\kappa$, so we can assume that $g = p^{a-1}t$.

By Property 3.3.3, κ is g -compound. The group of translations \mathcal{G} acts on the set of canonical g -compound orthomorphisms of \mathbb{Z}_n , of which there are exactly $p^{g-1}z_g z_p^g$ by Property 3.3.1. Hence $|C| \equiv p^{g-1}z_g z_p^g \pmod{p^a}$. Since $g - 1 \geq 3^{a-1}t - 1 \geq a$ (as $a = 1$ implies $t \geq 3$) we find that p^a divides $|C|$. \square

In Corollary 3.2.2 we showed that $R_{n+1} \equiv z_n \pmod{n}$ if n is prime, and Theorem 1.1.5 implies that $R_{n+1} \equiv 0 \pmod{n}$ for all composite n . Corollary 3.3.7 now follows from Theorem 3.3.6.

Corollary 3.3.7. *If n is an odd prime then $R_{n+1} \equiv z_n \equiv -2 \pmod{n}$ and if n is composite then $R_{n+1} \equiv z_n \equiv 0 \pmod{n}$.*

3.3.2 Evaluating $z_n \pmod{3}$

The values of $z_n \pmod{3}$ for odd $n \leq 25$ are listed in Figure 3.2. It was established in Theorem 3.0.9 that z_n is divisible by 3 when $n \equiv 2 \pmod{3}$, which we will now extend.

Theorem 3.3.8. *Let n be an odd number. If $n \geq 5$ and $n \not\equiv 1 \pmod{3}$ then $z_n \equiv 0 \pmod{3}$. If $n \equiv 1 \pmod{3}$ then $z_n \equiv \zeta(n) \pmod{3}$, where $\zeta(n)$ is the number of partitions of $\{1, 2, \dots, n-1\}$ into parts of size 3 in which each part has sum divisible by n .*

Proof. Let A be the Latin square defined by

$$a_{ij} \equiv -i - j \pmod{n}. \quad (3.14)$$

Let T be the set of all transversals of A containing $(0, 0, 0)$.

The canonical orthomorphisms σ of \mathbb{Z}_n are in one-to-one correspondence with the transversals $\{(i, \sigma(i) - i, -\sigma(i)) : i \in \mathbb{Z}_n\}$ of A containing $(0, 0, 0)$ (see Section 3.1 or [324] for more details). Hence $z_n = |T|$. Let C_3 be the cyclic permutation group on three elements. Then C_3 acts on A by uniformly permuting the coordinates of each triplet. Consequently, C_3 has an induced action on T . The orbit of any $\psi \in T$, denoted $C_3(\psi)$, has cardinality either 1 or 3. Let $\mathcal{T} = \{\psi \in T : |C_3(\psi)| = 1\}$, so that $z_n = |T| \equiv |\mathcal{T}| \pmod{3}$.

Suppose $\psi \in \mathcal{T}$. If $(i, j, a_{ij}) \in \psi$ then $(a_{ij}, i, j), (j, a_{ij}, i) \in \psi$. Therefore $(i, j, a_{ij}) \in \psi$ implies that either $i = j = a_{ij}$ or $i \neq j \neq a_{ij} \neq i$, since ψ is a transversal. If $i = j = a_{ij}$ then $3i \equiv 0 \pmod{n}$ by (3.14). Let $X_\psi = \{i \in \mathbb{Z}_n : (i, i, i) \in \psi\}$. So $n = |\psi| \equiv |X_\psi| \pmod{3}$ and $X_\psi = \{0\}$ if 3 does not divide n .

Case I: $n \equiv 2 \pmod{3}$. Then $n = |\psi| \equiv |X_\psi| = 1 \pmod{3}$ giving a contradiction. Hence $\mathcal{T} = \emptyset$ and $z_n \equiv |\mathcal{T}| = 0 \pmod{3}$. This case was previously proved in [221].

Case II: $n \equiv 1 \pmod{3}$. Again $n = |\psi| \equiv |X_\psi| = 1 \pmod{3}$. By removing the ordering upon the triplets in $\psi \setminus \{(0, 0, 0)\}$ we construct a partition of $\{1, 2, \dots, n-1\}$ into parts of size 3 and sum congruent to 0 \pmod{n} . Reversing the process, any such partition can be used to generate $2^{(n-1)/3}$ transversals of A . As a result $z_n \equiv 2^{(n-1)/3} \zeta(n) \equiv \zeta(n) \pmod{3}$.

Case III: $n \equiv 0 \pmod{3}$. Follows from Theorem 3.3.6 since 3 divides n and $n \neq 3$. \square

Figure 3.11 shows the values of $\zeta(n)$ for some small values of $n \equiv 1 \pmod{6}$, computed by Ian Wanless (private communication). Every solution to Heffter's First Difference Problem can be used to construct one of the partitions counted by $\zeta(n)$. Hence [22] implies that $\zeta(n) \geq 2^{\lfloor (n-1)/12 \rfloor}$ for sufficiently large $n \equiv 1 \pmod{6}$. While ζ increases at least exponentially, we only require the value of $\zeta(n) \pmod{3}$ for Theorem 3.3.8. In the following theorem, we will show that $\zeta(n) \equiv 1 \pmod{3}$ for primes of the form $2 \cdot 3^k + 1$ (Sloane's A111974). A necessary and sufficient condition for the primality of $2 \cdot 3^k + 1$ was given by [331, 332] (see also [28]).

n	1	7	13	19	25	31	37	43	49	55
$\zeta(n)$	1	1	5	52	1055	31814	1403925	83999589	6567620752	649233882590
$(\text{mod } 3)$	1	1	2	1	2	2	0	0	1	2

FIGURE 3.11: Values of $\zeta(n)$ for some small values of $n \equiv 1 \pmod{6}$.

Theorem 3.3.9. *Let n be a prime of the form $2 \cdot 3^k + 1$. Then $z_n \equiv 1 \pmod{3}$.*

Proof. The theorem is true when $n = 3$, since $z_3 = 1$, so assume $k \geq 1$. By Theorem 3.3.8, it is sufficient to show that $\zeta(n) \equiv 1 \pmod{3}$. Let \mathcal{P} be the set of partitions counted by $\zeta(n)$. Let $\mathcal{R} = \cup_{P \in \mathcal{P}} P$.

The multiplicative group \mathbb{Z}_n^* of integers modulo n is cyclic because n is prime. Moreover, there exists a cyclic subgroup $G < \mathbb{Z}_n^*$ of order 3^k . The natural action of G partitions \mathcal{P} into orbits of cardinality in $\{1, 3, 3^2, \dots, 3^k\}$. Let \mathcal{P}^* be the set of all partitions in \mathcal{P} that are stabilised by G . Hence $\zeta(n) \equiv |\mathcal{P}^*| \pmod{3}$ and it is sufficient to show that $|\mathcal{P}^*| = 1$.

Observe that the orbits of G on \mathcal{R} have size 3^k or 3^{k-1} since each $p \in \mathcal{R}$ has cardinality 3. Each $P \in \mathcal{P}$ has precisely $2 \cdot 3^{k-1}$ parts. Therefore, if $P \in \mathcal{P}^*$ then the action of G partitions P into exactly two orbits of cardinality 3^{k-1} . The Orbit-Stabiliser Theorem implies that the stabiliser of each part $p \in P$ has order 3, and hence must be the unique subgroup $H \leq G$ of order 3. It follows that \mathcal{P}^* consists of the unique partition of $\mathbb{Z}_n \setminus \{0\}$ induced by the action of H . So $|\mathcal{P}^*| = 1$. \square

3.3.3 Polynomial and compatible orthomorphisms

A permutation σ of \mathbb{Z}_n is called a *polynomial permutation* if for some integer polynomial f we have $\sigma(i) \equiv f(i) \pmod{n}$ for all $i \in \mathbb{Z}$. We say σ is *described by* f . If σ is an orthomorphism and a polynomial permutation then σ is called a *polynomial orthomorphism*. Let π_n be the number of canonical polynomial orthomorphisms of \mathbb{Z}_n . If σ is a polynomial orthomorphism of \mathbb{Z}_n described by f and r is an integer polynomial such that $r(i) \equiv 0 \pmod{n}$ for all $i \in \mathbb{Z}$, then σ is also described by $f + r$. Linear orthomorphisms are simple examples of polynomial orthomorphisms.

Polynomial orthomorphisms of finite fields have been studied, for example, by Niederreiter and Robinson [247] and Wan [319] (see also [309]), who showed that, for any finite field \mathbb{F}_q where $q \geq 4$, every orthomorphism is described by a polynomial of degree at most $q - 3$. Evans [109] also discussed polynomial orthomorphisms of finite fields. In this section, we instead study polynomial orthomorphisms over the ring \mathbb{Z}_n .

Theorem 3.3.10. *There exists an orthomorphism of \mathbb{Z}_n that is not described by any integer polynomial if and only if n is an odd composite number.*

Proof. If $n = 1$ the theorem is true. If n is even then there are no orthomorphism of \mathbb{Z}_n and the theorem is vacuously true. If n is prime then \mathbb{Z}_n is a finite field and hence every orthomorphism of \mathbb{Z}_n is described by a polynomial.

Now suppose n is an odd composite number. Let d be a proper divisor of n and let σ be an orthomorphism of \mathbb{Z}_n such that $\sigma(0) = 0$ and $\sigma(d) = 1$. Grüttmüller [142] showed that σ exists. If f describes σ , then $f(0) \equiv 0 \not\equiv 1 \equiv f(d) \equiv f(0) \pmod{d}$, giving a contradiction. \square

An orthomorphism σ of \mathbb{Z}_n is called *compatible* if σ is d -compound for all divisors d of n . This definition follows Nöbauer [249]. Let λ_n denote the number of canonical compatible orthomorphisms of \mathbb{Z}_n . Clearly, every polynomial orthomorphism is compatible, therefore $\pi_n \leq \lambda_n$ for all n . However, it is not obvious whether or not every compatible orthomorphism is a polynomial orthomorphism – the argument in the proof of Theorem 3.3.10 cannot be applied to compatible orthomorphisms.

We will now show that every compatible orthomorphism of \mathbb{Z}_{21} is a polynomial orthomorphism. There are 5 linear orthomorphisms of \mathbb{Z}_{21} , described by $2i$, $5i$, $11i$, $17i$ and $20i$, and 14 other canonical polynomial orthomorphisms of \mathbb{Z}_{21} described by

$$f_a(i) = i^4 + (4a + 2)i^3 + (6a^2 + 6a + 5)i^2 + (4a^3 + 6a^2 + 10a - 6)i \quad (3.15)$$

and $i - f_a(i)$ for $0 \leq a \leq 6$. This is a complete list of the canonical compatible orthomorphisms of \mathbb{Z}_{21} . Hence $\pi_{21} = \lambda_{21} = 19$. This raises the question, for what other values of n does $\pi_n = \lambda_n$? That is, when is every compatible orthomorphism a polynomial orthomorphism? We will later answer this question with Theorem 3.3.15.

Property 3.3.11. *If κ is a canonical compatible orthomorphism of \mathbb{Z}_{dt} , then κ is of the form $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ as in (3.13) where $\sigma_0, \sigma_1, \dots, \sigma_{d-1}$ and μ are compatible orthomorphisms. Moreover, if κ is described by the polynomial f , then μ is described by f and σ_k is described by g_k where $g_k(i) = f(di + k)$ for all $0 \leq k \leq d - 1$.*

Proof. By assumption, κ is d -compound, so Property 3.3.1 implies that κ is of the form $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ as in (3.13). Suppose there exists a divisor t' of t such that $\sigma_k(i) \not\equiv \sigma_k(j) \pmod{t'}$ while $i \equiv j \pmod{t'}$ for some $i, j \in \mathbb{Z}_t$ and $k \in \mathbb{Z}_d$. Then (3.13) implies $\kappa(di + k) \not\equiv \kappa(dj + k) \pmod{dt'}$ while $di + k \equiv dj + k \pmod{dt'}$, giving a contradiction. Next, suppose there exists a divisor d' of d such that $\mu(i) \not\equiv \mu(j) \pmod{d'}$ while $i \equiv j \pmod{d'}$ for some $i, j \in \mathbb{Z}_d$. Then (3.13) implies $\kappa(i) \not\equiv \kappa(j) \pmod{d'}$, giving a contradiction. Therefore $\sigma_0, \sigma_1, \dots, \sigma_{d-1}$ and μ are all compatible.

Now suppose κ is described by the polynomial f . Then $\mu(i) \equiv f(i) \pmod{d}$ and $\sigma_k(i) \equiv f(di + k) \pmod{t}$ for all i and $0 \leq k \leq d - 1$. \square

Property 3.3.11 is a modified version of Property 3.3.1 for compatible and polynomial orthomorphisms. The converse of Property 3.3.11 is false for both compatible and polynomial orthomorphisms. For example, consider the orthomorphism defined by

$$\kappa = \kappa_{5,3}[\eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}, \eta_{2,3}; \eta_{2,5}].$$

Then $\kappa(0) = 0$ and $\kappa(3) = 1$ and therefore κ is not compatible or polynomial, while $\eta_{2,3}$ and $\eta_{2,5}$ are both polynomial and therefore compatible. However, Property 3.3.13 will show that the converse is true when dt is a prime power. We will now extend Property 3.3.11 in the case when $\gcd(d, t) = 1$.

Property 3.3.12. *Suppose $\gcd(d, t) = 1$ and let κ be a canonical compatible orthomorphism of \mathbb{Z}_{dt} . Then $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ as in (3.13) and is uniquely determined by σ_0 and μ . Moreover, if κ is a canonical polynomial orthomorphism then it is described by*

$$f_\kappa(i) = t^{\phi(d)} f_\mu(i) + d f_{\sigma_0}(d^{\phi(t)-1} i), \quad (3.16)$$

where ϕ is the Euler ϕ -function and f_μ and f_{σ_0} are integer polynomials that describe μ and σ_0 respectively.

Proof. Property 3.3.1 implies that $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ as in (3.13). Given μ and σ_0 we can define κ by $\kappa(i) \equiv \mu(i) \pmod{d}$ and $\kappa(i) \equiv \sigma_0(j) \pmod{t}$ for all $i \in \mathbb{Z}_{dt}$ and $j \equiv i \pmod{t}$. Using the Chinese Remainder Theorem, κ is uniquely determined. It is straightforward to show that κ defined in this way is indeed an orthomorphism.

If κ is a polynomial orthomorphism, Property 3.3.11 implies that μ and σ_0 are also polynomial orthomorphisms. Assume μ and σ_0 are described by f_μ and f_{σ_0} , respectively. It is straightforward to show that f_κ as given by (3.16) describes an orthomorphism. Since d and t are coprime, Euler's Totient Theorem implies that $t^{\phi(d)} \equiv 1 \pmod{d}$ and $d^{\phi(t)} \equiv 1 \pmod{t}$. It follows that $f_\kappa(i) \equiv \mu(i) \pmod{d}$ and $f_\kappa(di) \equiv d f_{\sigma_0}(d^{\phi(t)} i) \equiv d f_{\sigma_0}(i) \equiv d \sigma_0(i) \pmod{t}$, which implies that f_κ describes κ since d and t are coprime. \square

It follows from Properties 3.3.11 and 3.3.12 that λ_n and π_n are multiplicative functions, that is

$$\lambda_n = \prod_{p \in \mathbb{P}_n} \lambda_{p^a} \quad \text{and} \quad \pi_n = \prod_{p \in \mathbb{P}_n} \pi_{p^a} \quad (3.17)$$

where \mathbb{P}_n is the set of prime divisors of n and $a = a(p, n)$ is the largest integer such that p^a divides n .

Property 3.3.13. *If $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ as in (3.13) such that $\sigma_0, \sigma_1, \dots, \sigma_{d-1}$ and μ are all compatible orthomorphisms, then κ is d' -compound for all divisors d' of n such that either d divides d' or d' divides d .*

Proof. Immediate from (3.13). \square

We will now ready to give a formula for λ_{p^a} .

Theorem 3.3.14. *Let p be a prime and $a \geq 1$. Then*

$$\lambda_{p^a} = p^{(p^a-1)/(p-1)-a} z_p^{(p^a-1)/(p-1)}.$$

Proof. Properties 3.3.11 and 3.3.13 imply that every compatible orthomorphism of \mathbb{Z}_{p^a} is of the form $\kappa = \kappa_{p^{a-1},p}[\sigma_0, \sigma_1, \dots, \sigma_{p-1}; \mu]$ as in (3.13) where $\sigma_0, \sigma_1, \dots, \sigma_{p-1}$ and μ are all compatible. Therefore

$$\lambda_{p^a} = p^{p^{a-1}-1} \lambda_p^{p^{a-1}} \lambda_{p^{a-1}}$$

for all $a \geq 1$. Through repeated application we obtain

$$\lambda_{p^a} = p^{p^{a-1}-1} \lambda_p^{p^{a-1}} \lambda_{p^{a-1}} = p^{p^{a-1}-1+p^{a-2}-1} \lambda_p^{p^{a-1}+p^{a-2}} \lambda_{p^{a-2}} = \dots = p^{(p^a-1)/(p-1)-a} \lambda_p^{(p^a-1)/(p-1)}$$

using the identity $\sum_{i=0}^{a-1} p^i = (p^a - 1)/(p - 1)$. We then use $\lambda_p = z_p$. \square

Figure 3.12 plots some of the values of λ_n for odd n in the range $1 \leq n \leq 119$. It was computed from Theorem 3.3.14 and the data in Figure 3.2. Clearly λ_n behaves erratically. The value of λ_{121} has 53 digits and is literally off the chart.

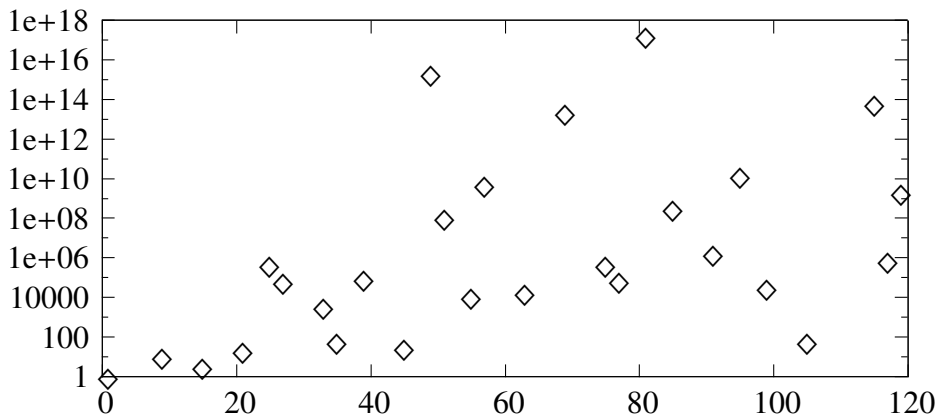


FIGURE 3.12: Some values of λ_n for n in the range $1 \leq n \leq 120$, on a logarithmic scale.

We are now ready to classify when $\pi_n = \lambda_n$.

Theorem 3.3.15. *When n is odd, $\pi_n = \lambda_n$ if and only if $n = 3^{a_3} 5^{a_5} p_1 p_2 \cdots p_r$ for $r \geq 0$, $a_3 \leq 3$, $a_5 \leq 2$ and distinct primes $p_i \geq 7$.*

Proof. Nöbauer [249] showed that all compatible permutations can be described by an integer polynomial if and only if $n = 2^{a_2} 3^{a_3} p_1 p_2 \cdots p_r$ for distinct primes $p_i \geq 5$ and $a_2 \leq 3$, $a_3 \leq 2$. Consequently, $\pi_n = \lambda_n$ if $n = 3^{a_3} 5^{a_5} p_1 p_2 \cdots p_r$ for distinct primes $p_i \geq 7$ and $a_3 \leq 2$ and $a_5 \leq 1$. Later we will show that $\pi_n = \lambda_n$ also when $a_3 \leq 3$ and $a_5 \leq 2$.

We will now construct canonical compatible orthomorphisms of \mathbb{Z}_{p^a} for prime $p \geq 7$ and $a \geq 2$ that are not polynomial orthomorphisms. To begin, observe that if f is any integer polynomial such that $f(0) = 0$ then

$$2f(p^{a-1}) \equiv f(2p^{a-1}) \pmod{p^a}. \quad (3.18)$$

Therefore, if there exists an orthomorphism σ_0 of \mathbb{Z}_p such that $\sigma_0(0) = 0$, $\sigma_0(1) = 2$ and $\sigma_0(2) = 1$ then $\kappa = \kappa_{p^{a-1}, p}[\sigma_0, \sigma_1, \dots, \sigma_{p^{a-1}-1}; \mu]$ cannot be a polynomial orthomorphism since it would not satisfy (3.18). Cavenagh, Härmäläinen and Nelson [51] showed that σ_0 exists for $p \geq 11$. When $p = 7$ we can instead use $\sigma_0 = (0)(153462)$ and again κ cannot be a polynomial orthomorphism because of (3.18). Given σ_0 , we may choose $\sigma_1, \sigma_2, \dots, \sigma_{p^{a-1}-1}$ to be any orthomorphisms of \mathbb{Z}_p and μ to be any canonical compatible orthomorphism of $\mathbb{Z}_{p^{a-1}}$, then Property 3.3.13 implies that κ is compatible. Therefore $\pi_{p^a} < \lambda_{p^a}$ for prime $p \geq 7$ and $a \geq 2$. Now we will handle the other odd primes, 3 and 5.

Claim: For $p \in \{3, 5\}$, every compatible orthomorphism of \mathbb{Z}_{p^a} is described by a polynomial if and only if there exists an integer polynomial r such that $r(i) \equiv p^{a-1} \pmod{p^a}$ if p^{a-1} divides i and $r(i) \equiv 0 \pmod{p^a}$ otherwise.

\Leftarrow Every orthomorphism σ of \mathbb{Z}_3 and \mathbb{Z}_5 satisfies $\sigma(i) \equiv \eta(i) + k$ where η is a linear orthomorphism and k is some integer constant. Therefore, using Property 3.3.11 it is straightforward to construct an arbitrary compatible orthomorphism of \mathbb{Z}_{p^a} as the sum of some affine transformations of r .

\Rightarrow Define $\eta'_{2,p}$ by $\eta'_{2,p}(i) \equiv 2i + 1 \pmod{p}$. Let f_1 be an integer polynomial that describes the orthomorphism $\kappa_{p^{a-1}, p}[\eta_{2,p}, \eta_{2,p}, \dots, \eta_{2,p}; \eta_{2,p^{a-1}}]$ and let f_2 be an integer polynomial that describes the orthomorphism $\kappa_{p^{a-1}, p}[\eta_{2,p}, \eta'_{2,p}, \eta_{2,p}, \eta_{2,p}, \dots, \eta_{2,p}; \eta_{2,p^{a-1}}]$. Property 3.3.13 implies that both f_1 and f_2 exist. Then r defined by $r(i) = f_2(i+1) - f_1(i+1)$ satisfies the claim.

Now we will identify the following cases when r , satisfying the claim, exists. When $n = 3^2$, we can take $r(i) = 6i^2 + 3$. When $n = 3^3$, we can take $r(i) = (i-1)(i-2)(i-3)(i-4)(i-5)(i-6)(i-7)(i-8)$. When $n = 5^2$, we can take $r(i) = 20i^4 + 5$. The claim therefore implies that $\pi_9 = \lambda_9$, $\pi_{27} = \lambda_{27}$ and $\pi_{25} = \lambda_{25}$. Next we will show that r , satisfying the claim, cannot exist for greater powers of 3 and 5.

When $n = 3^4$, let $r(i) = a_0 + a_1 i + i^2 g(i)$ for some integer polynomial g and integers a_0, a_1 . We require $r(0) \equiv 27 \pmod{81}$ so $a_0 \equiv 27 \pmod{81}$. We also require $r(9) \equiv 0 \pmod{81}$ implying $a_1 \equiv -3 \pmod{9}$ and $r(18) \equiv 0 \pmod{81}$ implying $a_1 \equiv 3 \pmod{9}$. Therefore r cannot be realised and $\pi_{81} < \lambda_{81}$.

When $n = 5^3$, let $r(i) = a_0 + a_1 i + a_2 i^2 + i^3 g(i)$ for some integer polynomial g and integers a_0, a_1, a_2 . We require $a_0 \equiv 25 \pmod{125}$. We also require $r(5) \equiv r(10) \equiv r(15) \equiv 0 \pmod{125}$, giving the three congruences $25 + 5a_1 + 25a_2 \equiv 0$, $25 + 10a_1 + 100a_2 \equiv 0$ and

$25 + 15a_1 + 225a_2 \equiv 0 \pmod{125}$, which cannot be simultaneously satisfied. Therefore r cannot be realised and $\pi_{125} < \lambda_{125}$.

Suppose μ is a canonical compatible orthomorphism of \mathbb{Z}_d and is not described by any integer polynomial. Then Property 3.3.11 implies that we can choose $\sigma_0, \sigma_1, \dots, \sigma_{d-1}$ such that $\kappa = \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ is a compatible orthomorphism of \mathbb{Z}_{dt} that cannot be described by any integer polynomial. Therefore if $\pi_d < \lambda_d$ then $\pi_{dt} < \lambda_{dt}$. In particular, $\pi_{p^a} < \lambda_{p^a}$ if $p = 3$ and $a \geq 4$ or $p = 5$ and $a \geq 3$.

To review, we have shown that every compatible orthomorphism of \mathbb{Z}_{p^a} , for prime $p \geq 3$, is described by an integer polynomial if and only if either (a) $p = 3$ and $a \in \{1, 2, 3\}$, (b) $p = 5$ and $a \in \{1, 2\}$ or (c) $p \geq 7$ and $a = 1$. The result now follows from (3.17). \square

We will now identify some more properties of polynomial orthomorphisms.

Property 3.3.16. *An integer polynomial f describes a polynomial orthomorphism of both \mathbb{Z}_d and \mathbb{Z}_t if and only if f describes a polynomial orthomorphism of $\mathbb{Z}_{\text{lcm}(d,t)}$.*

Proof. Assume f describes a polynomial orthomorphism of both \mathbb{Z}_d and \mathbb{Z}_t . If $i \not\equiv j \pmod{d}$ then:

- $f(i) \not\equiv f(j) \pmod{d}$ and hence $f(i) \not\equiv f(j) \pmod{\text{lcm}(d,t)}$ and
- $f(i) - i \not\equiv f(j) - j \pmod{d}$ and hence $f(i) - i \not\equiv f(j) - j \pmod{\text{lcm}(d,t)}$.

Similar statements hold $i \not\equiv j \pmod{t}$. Hence f describes a polynomial orthomorphism of $\mathbb{Z}_{\text{lcm}(d,t)}$.

Now assume f describes a polynomial orthomorphism σ of $\mathbb{Z}_{\text{lcm}(d,t)}$. Then σ is compatible, and in particular $\{d, t\}$ -compound. Therefore f also describes a polynomial orthomorphism of both \mathbb{Z}_d and \mathbb{Z}_t . \square

Property 3.3.17. *Let p be prime and $a \geq 2$. Then f describes a polynomial orthomorphism of \mathbb{Z}_{p^a} if and only if f describes a polynomial orthomorphism of \mathbb{Z}_p and $f'(i) \not\equiv 0 \text{ or } 1 \pmod{p}$ for all $i \in \mathbb{Z}$, where f' is the derivative of f .*

Proof. Nöbauer [248] showed that f describes a permutation of \mathbb{Z}_{p^a} if and only if f describes a permutation of \mathbb{Z}_p and $f'(i) \not\equiv 0 \pmod{p}$ for all $i \in \mathbb{Z}$. Consequently f and f^* , defined by $f^*(i) = f(i) - i$, simultaneously describe permutations of \mathbb{Z}_{p^a} (that is f describes a polynomial orthomorphism of \mathbb{Z}_{p^a}) if and only if (a) f describes a permutation of \mathbb{Z}_p , (b) f^* describes a permutation of \mathbb{Z}_p , (c) $f'(i) \not\equiv 0 \pmod{p}$ for all $i \in \mathbb{Z}$ and (d) $(f^*)'(i) = f'(i) - 1 \not\equiv 0 \pmod{p}$ for all $i \in \mathbb{Z}$. \square

For example, consider f defined by $f(i) = i^4 + 4i^3 - i^2 + i$. Then f describes a polynomial orthomorphism of \mathbb{Z}_3 and \mathbb{Z}_7 . Property 3.3.16 implies that f describes a polynomial orthomorphism of \mathbb{Z}_{21} . In fact f describes the same orthomorphism of \mathbb{Z}_{21} as f_4 in (3.15). However, $f'(0) = 1$ and therefore Properties 3.3.16 and 3.3.17 together imply that f does not describe a polynomial orthomorphism of \mathbb{Z}_n for any n that is divisible by the square of any prime.

For another example, consider f defined by $f(i) = pr(i) + ki$, where p is prime, $2 \leq k \leq p - 1$ and r is any integer polynomial. Then f describes a linear (and hence polynomial) orthomorphism of \mathbb{Z}_p and moreover $f'(i) \equiv k \pmod{p}$ for all i . Property 3.3.17 implies that f describes a polynomial orthomorphism of \mathbb{Z}_{p^a} for all a .

Properties 3.3.16 and 3.3.17 together imply the following corollary.

Property 3.3.18. *An integer polynomial f describes an orthomorphism of \mathbb{Z}_n if and only if for all prime divisors p of n , (a) f describes a polynomial orthomorphism of \mathbb{Z}_p and (b) if p^2 divides n , then $f'(i) \not\equiv 0, 1 \pmod{p}$ for all $i \in \mathbb{Z}$.*

3.3.4 Partial orthomorphism completion

We say that a partial orthomorphism $\nu : S \rightarrow \mathbb{Z}_n$ has *size* $a := |S|$. Suppose d is a proper divisor of n , such that for any $i, j \in S$, if $\nu(i) \not\equiv \nu(j) \pmod{d}$ then $i \not\equiv j \pmod{d}$, then ν is called a *partial d -compound orthomorphism* of \mathbb{Z}_n . If ν is a partial orthomorphism of \mathbb{Z}_n such that there exists an orthomorphism σ of \mathbb{Z}_n for which $\nu(i) = \sigma(i)$ for all $i \in S$, then we say ν admits a *completion*.

Let $\rho_{a,n}$ be the proportion of partial orthomorphisms of \mathbb{Z}_n of size a that admit a completion. Since $z_n = 0$ for even n , we will only discuss odd n . We list some values of $\rho_{a,n}$ in Figure 3.13 obtained by through a computer search and verified by Ian Wanless (private communication). For odd n :

- $\rho_{1,n} = \rho_{2,n} = \rho_{n-1,n} = \rho_{n,n} = 1$ using results of Grüttmüller [142] and Evans [109, p. 14].
- Grüttmüller² [143] asked if $\rho_{a,n} = 1$ for $n \geq 3a - 1$, having shown that:
 - (a) $\rho_{a,n} < 1$ when $3 \leq a \leq n - 2$ and $n \leq 3a - 2$ and
 - (b) $\rho_{a,n} = 1$ when $2 \leq a \leq 7$ and $3a - 1 \leq n \leq 21$ by a computer search.
- Cavenagh, Härmäläinen and Nelson [51] showed that $\rho_{3,n} = 1$ for prime $n \geq 11$.

Lemma 3.3.19. *If $2 \leq a \leq n - 2$ and $\rho_{a,n} = 1$ then $\rho_{a-1,n} = 1$.*

Proof. We already observed that the lemma is true when $a = 2$, so assume $3 \leq a \leq n - 2$. If $n \leq 3a - 2$ then $\rho_{a,n} < 1$, so the lemma is vacuously true. We can therefore assume $n > 3a - 2 > 2a - 1$. Let $\nu : S \rightarrow \mathbb{Z}_n$ be an arbitrary partial orthomorphism of \mathbb{Z}_n of size $a - 1$. Let U be the range of ν . Choose any $s \in \mathbb{Z}_n \setminus S$. It is sufficient to find $u \in \mathbb{Z}_n \setminus U$ such that $u - s \not\equiv \nu(i) - i$ for all $i \in S$, since then we may append $s \mapsto u$ to ν to create a partial orthomorphism of \mathbb{Z}_n of size a . This would then imply that ν admits a completion, since $\rho_{a,n} = 1$ by assumption. Since $\{\nu(i) - i : i \in S\}$ has cardinality $a - 1$, a suitable u exists if $|\mathbb{Z}_n \setminus U| = n - (a - 1) > a - 1$, which is true as $n > 2a - 1$. \square

Therefore, for odd $n \geq 5$ there exists an $a' \leq (n + 2)/3$ such that $\rho_{0,n} = \rho_{1,n} = \dots = \rho_{a',n} = 1$ and $\rho_{a'+1,n}, \rho_{a'+2,n}, \dots, \rho_{n-2,n} < 1$. The upper bound on a' comes from the result of Grüttmüller.

Theorem 3.3.20. *Suppose $\nu : S \rightarrow \mathbb{Z}_n$ is a partial d -compound orthomorphism of \mathbb{Z}_n of size a . For $i \in \mathbb{Z}_n$ let $S_i = \{s \in S : s \equiv i \pmod{d}\}$ and let $b = \max_i(|S_i|)$. If $\rho_{a,d} = \rho_{b,n/d} = 1$ then ν admits a completion.*

Proof. By Lemma 3.3.19 and (3.13) it is possible to construct a completion of ν . \square

²The proof of Theorem 2 in [143] gave a construction that was used to deduce that $\rho_{a,n} < 1$ whenever $n \leq 3a - 2$ and a is odd or $n \leq 3a - 3$ and a is even. This is correct except when $a = n - 1$, n is odd and $n \geq 3$.

	$n = 3$	5	7	9	11
$a = 1$	1	1	1	1	1
2	1	1	1	1	1
3	1	3/5	79/85	1	1
4		1	91/181	306/331	1
5		1	19/43	460/871	10453/11053
6			1	41/116	8292/14827
7			1	75/194	3264/10661
8				1	3409/14607
9				1	3441/11197
10					1
11					1

FIGURE 3.13: Some values of $\rho_{a,n}$.

In particular, we have already observed that if $b \leq 2$ in Theorem 3.3.20 then $\rho_{b,n/d} = 1$ if n/d is odd and $n/d \geq 3$.

Theorem 3.3.21. *Suppose n is the product of r pairwise-coprime odd factors f_1, f_2, \dots, f_r where $r > 3a - \frac{1}{2}(3 + \lceil 3a^{1/2} \rceil)$ and suppose $\rho_{a,n/f_1} = \rho_{a,n/f_2} = \dots = \rho_{a,n/f_r} = 1$. Then $\rho_{a,n} = 1$.*

Proof. Let ν be an arbitrary partial orthomorphism of \mathbb{Z}_n of size a . Let $R = \{1, 2, \dots, r\}$ and for any $X \subseteq R$ let $f_X = \prod_{x \in X} f_x$.

It is sufficient to find $X \subset R$, of cardinality less than r , such that for any distinct $i, j \in S$ we have $i \not\equiv j$, $\nu(i) \not\equiv \nu(j)$ and $\nu(i) - i \not\equiv \nu(j) - j \pmod{f_X}$. Given such an X , choose $d = n/f_c$ for some $c \in R \setminus X$ (which is non-empty since $|R| = r > |X|$). By Theorem 3.3.20, since $\rho_{a,n/f_c} = 1$, ν admits a completion to a d -compound orthomorphism of \mathbb{Z}_n .

Let P_1, P_2 and P_3 be the partitions of S induced by congruence modulo f_X on the sets $S = \{i : i \in S\}$, $\{\nu(i) : i \in S\}$ and $\{\nu(i) - i : i \in S\}$, respectively. Let $P = \{p_1 \cap p_2 \cap p_3 : p_1 \in P_1, p_2 \in P_2, p_3 \in P_3\}$, which is called the *meet* of P_1, P_2 and P_3 .

We begin with $X = \emptyset$ and $P = P_1 = P_2 = P_3 = \{S\}$. We then progressively add elements to X until $|P_1| = |P_2| = |P_3| = |P| = a$. If i and j are in the same part in P_1 then, since $i \not\equiv j \pmod{n}$, we can increase $|P_1|$ by increasing $|X|$ by one. Similar statements hold for $|P_2|$ and $|P_3|$ since then $\nu(i) \not\equiv \nu(j)$ and $\nu(i) - i \not\equiv \nu(j) - j \pmod{n}$, respectively. Moreover, if i and j are in the same part in P then we can increase $|P_1| + |P_2| + |P_3|$ by at least two by adding a single new element, say e , to X . This is because it is impossible for precisely two of the congruences $i \equiv j$, $\nu(i) \equiv \nu(j)$ and $\nu(i) - i \equiv \nu(j) - j$ to hold modulo f_e .

We work in two stages. Stage 1 is when $|P| < a$. We choose i and j in the same part of P and separate them by adding an element to X . Stage 1 ends when $|P| = a$. In Stage 2 we add elements to X that will increase at least one of $|P_1|$, $|P_2|$ or $|P_3|$. Suppose we add α elements to X in Stage 1 and β elements to X in Stage 2. Observe that $|P_1| + |P_2| + |P_3|$ increases by at least two for every element added to X in Stage 1 and by at least one thereafter. Initially, $|P_1| + |P_2| + |P_3| = 1 + 1 + 1 = 3$, while at the end of Stage 2, $|P_1| + |P_2| + |P_3| = a + a + a = 3a$. Hence $2\alpha + \beta \leq 3(a - 1)$. So $|X| = \alpha + \beta \leq \frac{3}{2}(a - 1) + \frac{1}{2}\beta$ after Stage 2.

Claim: At the end of Stage 1, $|P_1| \cdot |P_2| \cdot |P_3| \geq a^{3/2}$. Assume for some $i \in \{1, 2, 3\}$ that we have $|P_i| = \frac{1}{\epsilon} a^{1/2}$ for some $\epsilon > 1$ (otherwise the claim is trivial). Then P_i must contain a part Q of cardinality at least $a/|P_i| = \epsilon a^{1/2}$. Let j, k be such that $\{i, j, k\} = \{1, 2, 3\}$. If $q, q' \in Q$ and q

and q' are in the same part in P_j (resp. P_k), then q and q' are in the same part in P_k (resp. P_j), contradicting that $|P| = a$. Therefore $|P_j| \geq \epsilon a^{1/2}$ and $|P_k| \geq \epsilon a^{1/2}$. So $|P_1| \cdot |P_2| \cdot |P_3| \geq \epsilon a^{3/2}$ where $\epsilon > 1$, thus proving the claim.

Now the Arithmetic Mean-Geometric Mean Inequality implies that $|P_1| + |P_2| + |P_3| \geq 3(|P_1| \cdot |P_2| \cdot |P_3|)^{1/3} \geq 3a^{1/2}$ at the end of Stage 1. It follows that $\beta \leq 3a - \lceil 3a^{1/2} \rceil$ and $|X| \leq 3a - \frac{1}{2}(3 + \lceil 3a^{1/2} \rceil)$ at the end of Stage 2. Hence the theorem holds for $r > 3a - \frac{1}{2}(3 + \lceil 3a^{1/2} \rceil)$. \square

We now consider partial orthomorphisms of size 3. As discussed earlier, $\rho_{3,n} = 1$ for prime $n \notin \{2, 5, 7\}$ and odd n in the range $9 \leq n \leq 21$. It remains unresolved if $\rho_{3,n} = 1$ for all odd $n \geq 9$. However, by Theorem 3.3.21, it is sufficient to show that $\rho_{3,n} = \rho_{3,5n} = \rho_{3,7n} = 1$ for all composite $n \geq 25$ with $|\mathbb{P}_n| \leq 4$, where \mathbb{P}_n is the set of prime divisors of n . Furthermore, many partial orthomorphisms of size 3 can be shown to admit a completion using Theorem 3.3.20. Theorem 3.2.4 and Figure 3.5 imply that the number of partial orthomorphisms of \mathbb{Z}_n of size 3 is given by

$$\frac{1}{6}n^2(n-1)(n-2)(n^2-6n+10). \quad (3.19)$$

Theorem 3.3.22. *Suppose n is odd and has a divisor d such that d is prime or $d \leq 21$. Then $\rho_{3,n} > 1 - 9/d$.*

Proof. The theorem is trivially true when $d \leq 7$, so assume $d \geq 9$. If $d = n$, then n is prime or $n \leq 21$, so $\rho_{3,n} = 1$ by [51] and [143], so assume $d < n$.

Given a partial orthomorphism ν on domain $\{s_1, s_2, s_3\}$ we can define a pair of vectors $\vec{s} = (s_1, s_2, s_3)$ and $\vec{u} = (u_1, u_2, u_3)$ such that $\nu(s_i) = u_i$ for $1 \leq i \leq 3$. In fact ν defines 3! such pairs of vectors. Conversely, given two such vectors $\vec{s}, \vec{u} \in \mathbb{Z}_n^3$ sometimes $s_i \mapsto u_i$ defines a partial orthomorphism.

Let N be the set of all $(\vec{s}, \vec{u}) \in \mathbb{Z}_n^3 \times \mathbb{Z}_n^3$ for which $s_i \not\equiv s_j$, $u_i \not\equiv u_j$ and $u_i - s_i \not\equiv u_j - s_j \pmod{d}$, for all $1 \leq i < j \leq 3$. Hence

$$|N| \geq n^6 - 3 \binom{3}{2} \frac{n^6}{d}.$$

Each $(\vec{s}, \vec{u}) \in N$ defines a partial d -compound orthomorphism by $s_i \mapsto u_i$. Since $\rho_{1,d} = \rho_{1,n/d} = 1$, Theorem 3.3.20 implies that each partial orthomorphism $s_i \mapsto u_i$ admits a completion to a d -compound orthomorphism. Therefore there are at least $\frac{1}{6}|N| = \frac{1}{6}n^6(1 - 9/d)$ partial orthomorphisms of \mathbb{Z}_n of size 3 that admit a completion. The result now follows from (3.19), which implies that there are less than $n^6/6$ partial orthomorphisms of \mathbb{Z}_n of size 3 in total. \square

If (n_i) is a sequence of odd positive integers such that the greatest prime divisor $\text{gpd}(n_i) \rightarrow \infty$ as $i \rightarrow \infty$ then Theorem 3.3.22 implies $\rho_{3,n_i} \rightarrow 1$, that is, a partial orthomorphism of \mathbb{Z}_{n_i} of size 3 admits a completion asymptotically almost surely.

3.3.5 Orthogonal compound orthomorphisms

Two orthomorphisms ϕ and ϕ' of \mathbb{Z}_n are *orthogonal* if $i \mapsto \phi(i) - \phi'(i)$ is a permutation of \mathbb{Z}_n . Let ω_n be the cardinality of the largest set of mutually-orthogonal orthomorphisms of \mathbb{Z}_n . Evans [111, 112] proved that if $n > 3$ is odd and indivisible by 9 then $\omega_n \geq 2$.

Theorem 3.3.23. *Let $\phi := \kappa_{d,t}[\sigma_0, \sigma_1, \dots, \sigma_{d-1}; \mu]$ and $\phi' := \kappa_{d,t}[\sigma'_0, \sigma'_1, \dots, \sigma'_{d-1}; \mu']$ be two canonical d -compound orthomorphisms, as in (3.13). Then ϕ is orthogonal to ϕ' if and only if σ_i is orthogonal to σ'_i for all i and μ is orthogonal to μ' .*

Proof. Assume that ϕ is orthogonal to ϕ' . Suppose, seeking a contradiction, that there exists $0 \leq k \leq d-1$ and distinct $0 \leq i, j \leq t-1$ such that $\sigma_k(i) - \sigma'_k(i) \equiv \sigma_k(j) - \sigma'_k(j) \pmod{t}$. Then $\phi(id+k) - \phi'(id+k) \equiv \phi(jd+k) - \phi'(jd+k) \pmod{n}$, giving a contradiction. Hence σ_k is orthogonal to σ'_k . Instead suppose $\mu(i) - \mu'(i) \equiv \mu(j) - \mu'(j) \pmod{d}$ for some distinct $0 \leq i, j \leq d-1$. Then by (3.13), there are at least $2t$ distinct values of $0 \leq r \leq n-1$ such that $\phi(r) - \phi'(r) \equiv \mu(i) - \mu'(i) \pmod{d}$, giving a contradiction. Hence μ is orthogonal to μ' .

Now assume σ_k is orthogonal to σ'_k for all $0 \leq k \leq d-1$ and μ is orthogonal to μ' . Suppose $\phi(i) - \phi'(i) \equiv \phi(j) - \phi'(j) \pmod{n}$ for some distinct $0 \leq i, j \leq n-1$. Through the use of translations, we may assume that $j = 0$. Therefore, for some $1 \leq i \leq n-1$, $\phi(i) - \phi'(i) \equiv 0 \pmod{n}$, since ϕ and ϕ' are both canonical. Hence $\mu(i) \equiv \mu'(i) \pmod{d}$ and so $i \equiv 0 \pmod{d}$, since μ and μ' are orthogonal and both canonical. By (3.13), $d\sigma_0(i/d) - d\sigma'_0(i/d) \equiv 0 \pmod{n}$ where $0 \leq \sigma_0(i/d), \sigma'_0(i/d) \leq t-1$. Therefore $\sigma_0(i/d) = \sigma'_0(i/d)$. Since σ_0 and σ'_0 are orthogonal and both canonical, this only happens when $i/d \equiv 0 \pmod{t}$ and therefore $i \equiv 0 \pmod{n}$. \square

Corollary 3.3.24. *If $n = dt$, then the largest set of mutually-orthogonal d -compound orthomorphisms of \mathbb{Z}_n has cardinality $\min(\omega_d, \omega_t)$. Hence $\omega_n \geq \min(\omega_d, \omega_t)$.*

A set of mutually-orthogonal orthomorphisms of \mathbb{Z}_n can be used to construct a set of mutually-orthogonal Latin squares, as discussed by Evans [109, p. 7]. Corollary 3.3.24 is related to a result of MacNeish [213]: if N_n is the maximum size of a set of mutually-orthogonal Latin squares of order n and $n = dt$, then $N_n \geq \min(N_d, N_t)$.

CHAPTER 4

Autotopisms

This chapter focuses on autotopisms of Latin squares. We begin with the work in [307]. Throughout this thesis we have been seeking divisibility properties of R_n through the study of isotopisms and autotopisms of Latin squares. This raises the following question.

Question 4.0.25. *What is the largest divisor of R_n that can be found through the study of autotopisms alone?*

Since we are using a group of isotopisms, the best congruence for L_n we could conceivably find would be $L_n \pmod{n!^3}$. Since $R_n = n!(n-1)!L_n$ by (1.2), the best congruence for R_n we could conceivably find is $R_n \pmod{n!n}$. Let q be a fixed prime. In Corollary 4.1.2 we show that q^a divides R_n where $a = n/(q-1) - O(\log^2 n)$ as $n \rightarrow \infty$. For comparison, the largest a such that q^a divides $n!n$ is $a \leq \log_q n + \sum_{k \geq 1} \lfloor n/q^k \rfloor \leq n/(q-1) + \log_q n$.

Using a similar technique, we are able to bound the maximum number of subsquares in a Latin square in Section 4.2. Previous results on the maximum number of subsquares in a Latin square were given by Heinrich and Wallis [156] (see also [224]) for 2×2 subsquares, van Rees [317] for 3×3 subsquares and Browning, Vojtěchovský and Wanless [35] for general $k \times k$ subsquares, which we will improve when $k \geq 6$.

Afterwards we follow the work in [303]. In Section 4.3 we make further progress in classifying which isotopisms $\theta \in \mathcal{I}_n$ are the autotopism of some Latin square. We define $\Omega_n \subseteq \mathcal{I}_n$ to be the set of isotopisms θ for which there exists a Latin square L of order n with $\theta \in \text{Atop}(L)$. We improve upon several theorems by Falcón [113], which give conditions for $\theta \in \Omega_n$. For example, Theorems 4.3.8 and 4.3.11 give strong necessary conditions for when $\theta \in \Omega_n$. Corollary 4.3.9 gives a generalisation of Lemma 1.2.8.

In Section 4.3 we aim our focus at classifying which isomorphisms are automorphisms, which are of particular value in the study of quasigroups. This also has implications for Ω_n , for example, in Theorem 4.3.13 we show that $\theta = (\alpha, \beta, \gamma) \notin \Omega_n$ if $n \equiv 2 \pmod{4}$ and every cycle in α, β and γ has length congruent to 2 $\pmod{4}$ (fixed points are 1-cycles). This builds upon a condition given by McKay, Meynert and Myrvold [222, Lem. 4(ii)] and theoretically resolves several cases of when $\theta \notin \Omega_n$ that were identified by an exhaustive search by Falcón [113].

It is known that if $\theta = (\eta, \eta, \eta)$ such that η is an n -cycle for even n then $\theta \notin \Omega_n$ (this is equivalent to the non-existence of othomorphisms for even n – see Section 3). In Theo-

rem 4.3.16 this result is generalised; we show that $\theta \notin \Omega_n$ if $\theta = (\eta, \eta, \eta)$ such that η consists of an odd number of even cycles of the same length without fixed points. Moreover, Theorem 4.3.17 gives necessary and sufficient conditions for $\theta \in \Omega_n$ where $\theta = (\eta, \eta, \eta) \in \mathcal{I}_n$ such that η consists of cycles of the same length and possibly some fixed points. In Section 4.3.4 we give necessary and sufficient conditions for when $\theta \in \Omega_n$ where $\theta = (\eta, \eta, \eta) \in \mathcal{I}_n$ such that η consists of two cycles and possibly some fixed points. We also identify Ω_{12} , Ω_{13} and Ω_{14} in Appendix A.4.

4.1 How large can an autotopism group be?

Let L be a Latin square of order n . By a similar argument to (1.1) we can deduce that

$$\text{Red}(L) = \frac{n!n}{|\text{Atop}(L)|} \quad (4.1)$$

where $\text{Red}(L)$ is the number of reduced Latin squares isotopic to L . Let $\tau(n) = \gcd_L(\text{Red}(L))$ where the gcd is over all Latin squares L of order n . It immediately follows that $\tau(n)$ divides R_n . In the next section, we will find an asymptotic lower bound on the largest a such that q^a divides $\tau(n)$ as $n \rightarrow \infty$, for any fixed prime q . The values of $\tau(n)$ for $1 \leq n \leq 11$ are given in Figure 4.1 and were obtained from the data by McKay, Meynert and Myrvold [222] and Hulpke, Kaski and Östergård [164]. By using the proof template in Section 2.1 it is straightforward to show that $(\lceil n/2 \rceil - 1)!$ divides $\tau(n)$ for $n \geq 3$.

If we find a divisor d of $\tau(n)$ then d also divides R_n . To find divisors of $\tau(n)$ we will find a bound on the maximum size of the autotopism group of a Latin square L and then use (4.1). For small n , the divisor d will also be small and, in fact, d will divide $(\lceil n/2 \rceil - 1)!$ which we already know is a divisor of R_n by Theorem 1.1.5 on page 3. However, for large n , we will improve upon Theorem 1.1.5.

n	1	2	3	4	5	6	7	8	9	10	11
$\tau(n)$	1	1	1	1	2	4	6	6	24	96	240
					2	2^2	$2 \cdot 3$	$2 \cdot 3$	$2^3 \cdot 3$	$2^5 \cdot 3$	$2^4 \cdot 3 \cdot 5$

FIGURE 4.1: The values of $\tau(n)$ for $1 \leq n \leq 11$ along with its prime factorisation.

4.1.1 Divisors of R_n

For any $n \geq 1$ and prime q , we let $\text{pow}_q(n)$ be the largest integer such that $q^{\text{pow}_q(n)}$ divides n . In this section, we will find an upper bound on $|\text{Atop}(L)|$ and use it to give an asymptotic lower bound on $\text{pow}_q(R_n)$.

Theorem 4.1.1. *If L is a Latin square of order n , then*

$$|\text{Atop}(L)| \leq n^2 \prod_{t=1}^{\lfloor \log_2 n \rfloor} (n - 2^{t-1}).$$

Proof. Let $L = (l_{ij})$ be an arbitrary Latin square of order n and let $\mathcal{S} = \text{Atop}(L)$. We note that \mathcal{S} also acts on the entries of L , with $(\alpha, \beta, \gamma) \in \mathcal{S}$ mapping $(i, j, l_{ij}) \mapsto (\alpha(i), \beta(j), \gamma(l_{ij}))$ for $i, j \in \mathbb{Z}_n$. For any set E of entries of L , let \mathcal{S}_E be the pointwise stabiliser of E in \mathcal{S} , that is $\mathcal{S}_E = \{\zeta \in \mathcal{S} : \zeta(e) = e \text{ for all entries } e \in E\}$.

To begin, let e be an entry in the first row of L and $E_1 = \{e\}$. The Orbit-Stabiliser Theorem implies that $|\mathcal{S}| \leq n^2 |\mathcal{S}_{E_1}|$ since there are n^2 entries in L . In order to bound $|\mathcal{S}|$, we will find a sequence $(\mathcal{S}_{E_t})_{t=1}^\lambda$ of stabiliser subgroups of \mathcal{S} and bound $|\mathcal{S}_{E_t}|/|\mathcal{S}_{E_{t+1}}|$ at each step. Eventually, when $t = \lambda$, the sequence will reach the trivial group and we can stop.

Lemma 1.2.6 on page 17 states that for any set of entries E_t , there exists a unique smallest subsquare M_{E_t} of L that contains all of the entries in E_t . Therefore, Lemma 1.2.7 implies that every $\zeta \in \mathcal{S}_t$ stabilises every entry in M_{E_t} . Let m_t be the order of M_{E_t} for all $t \geq 1$.

To construct E_{t+1} from E_t , we add a single entry e' to E_t from the first row of L such that e' is outside of M_{E_t} . If no such entry exists, we must have $M_{E_t} = L$, so we can set $\lambda = t$ and stop. The orbit of e' under \mathcal{S}_{E_t} is of cardinality at most $n - m_t$ since the first row of L is stabilised by every $\zeta \in \mathcal{S}_{E_t}$. Therefore, the Orbit-Stabiliser Theorem implies that $|\mathcal{S}_{E_{t+1}}| \leq (n - m_t) |\mathcal{S}_{E_t}|$.

Lemma 1.2.4 implies that $m_{t+1} \geq 2m_t$ for each $t \geq 1$. Since $m_1 = 1$, we find that $m_t \geq 2^{t-1}$ for all $t \geq 1$. We are finished no later than when $2^{t-1} \geq n$, implying that $\lambda \leq \lfloor \log_2 n \rfloor + 1$. Hence

$$|\mathcal{S}| \leq n^2 |\mathcal{S}_{E_1}| \leq n^2 (n - 1) |\mathcal{S}_{E_2}| \leq n^2 (n - 1)(n - 2) |\mathcal{S}_{E_3}| \leq \cdots \leq n^2 \prod_{t=1}^{\lfloor \log_2 n \rfloor} (n - 2^{t-1}).$$

□

We can get a better feel for the accuracy of Theorem 4.1.1 by examining the autotopisms of elementary Abelian groups. Let q be a fixed prime and $n = q^a$ and let Z be the Cayley table of $(\mathbb{Z}_q)^a$. It is known [13, 23, 246, 280] that $|\text{Atop}(Z)| = n^2(n - 1)(n - q) \cdots (n - q^{a-1})$. Therefore, the bound in Theorem 4.1.1 is achieved when $n = 2^a$.

Corollary 4.1.2. *Let q be a fixed prime. Then $\text{pow}_q(R_n) \geq n/(q - 1) - O(\log^2 n)$ as $n \rightarrow \infty$.*

Proof. Let L be an arbitrary Latin square of order n . Theorem 4.1.1 implies that $|\text{Atop}(L)| \leq n^{2+\log_2 n}$. Hence $\text{pow}_q(|\text{Atop}(L)|) \leq \log_q(n^{2+\log_2 n}) = (2 + \log_2 n) \cdot \log_q n = O(\log^2 n)$. By (4.1),

$$\text{pow}_q(\text{Red}(L)) = \text{pow}_q(n!) + \text{pow}_q(n) - \text{pow}_q(|\text{Atop}(L)|).$$

The result now follows since $\text{pow}_q(n!) = \sum_{k \geq 1} \lfloor n/q^k \rfloor \geq n/(q - 1) - \log_q n$. □

4.2 The maximum number of subsquares of a Latin square

We will now use a similar technique to Section 4.1.1 to bound the number of $k \times k$ subsquares in a Latin square of order n , for arbitrary k and n .

“The number of subsquares in a Latin square is an important but mysterious guide to the properties of Latin squares.”

— VAN REES [317]

Let L be a Latin square of order n . Let $I_k(L)$ denote the number of subsquares of order k in L . Let $T_k(L) = \sum_{i=k}^{2k-1} I_i(L)$ and let $W(L) = \sum_{i=1}^n I_i(L)$.

Heinrich and Wallis [156, 224] showed that $\frac{1}{45}n^3 \leq \max I_2(L) \leq \frac{1}{4}n^3 - \frac{1}{4}n^2$ when $n \geq 4$. Van Rees [317] gave the bound $I_3(L) \leq \frac{1}{18}n^3 - \frac{1}{18}n^2$. McKay and Wanless [224] and Cavenagh, Greenhill and Wanless [49] showed that for any $\epsilon > 0$, with probability approaching 1 as $n \rightarrow \infty$, a random Latin square of order n contains at least $n^{3/2-\epsilon}$ and at most $\frac{9}{2}n^{5/2}$ intercalates, respectively. Browning, Vojtěchovský and Wanless [35] showed that

$$I_k(L) \leq \frac{n \binom{n}{h}}{k \binom{k}{h}} \quad (4.2)$$

where $h = \lceil (k+1)/2 \rceil$ and that $I_k(L) = O(n^{\sqrt{2k}+2})$ for fixed k as $n \rightarrow \infty$.

Figure 4.2 gives some values of $\max I_2(L)$ (Sloane's [290] A092237) and $\max I_3(L)$ for $1 \leq n \leq 9$. The value of $\max I_3(L)$ for $n = 8$ was reported by Ian Wanless (private communication).

n	1	2	3	4	5	6	7	8	9	10	11	12
$\max I_2(L)$	0	1	0	12	4	27	42	112	72	≥ 125	≥ 172	≥ 324
$\max I_3(L)$	0	0	1	0	0	4	7	4	36			

FIGURE 4.2: Some data on $I_2(L)$ and $I_3(L)$.

In Figure 4.3 we give:

- A Latin square of order 6 with 27 intercalates and 4 subsquares of order 3 and
- A Latin square of order 7 with 42 intercalates and 7 subsquares of order 3.

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

FIGURE 4.3: Some Latin squares with many subsquares.

We will now find an upper bound on $T_k(L)$ which we will later use to find an upper bound on $I_k(L)$ and $W(L)$.

Theorem 4.2.1. *Let L be a Latin square of order $n \geq 2$. Then*

$$T_k(L) \leq \frac{1}{2^{h(h-1)/2}} n^2 \prod_{i=0}^{\lceil \log_2 k \rceil - 1} (n - 2^i)$$

where $h = \lceil \log_2 k \rceil$. Hence $T_k(L) = O(n^{\lceil \log_2 k \rceil + 2})$ for fixed k as $n \rightarrow \infty$.

Proof. In this proof we present an algorithm that will return a set \mathcal{S} in which each $E \in \mathcal{S}$ gives rise to a subsquare M_E of order at least k . Furthermore, the set $\{M_E : E \in \mathcal{S}\}$ will contain every subsquare in L of order between k and $2k - 1$. We will then bound the size of $|\mathcal{S}|$ to obtain the stated result.

To begin, assign

$$\mathcal{S}_1 := \{\{e\} : e \text{ is an entry of } L\}.$$

The algorithm will construct a sequence of sets $(\mathcal{S}_t)_{t \geq 1}$. For each $t \geq 1$, each $E \in \mathcal{S}_t$ will be a set of entries of L , such that any two entries $e, e' \in E$ have the same symbol. Lemma 1.2.5 implies that, for each set of entries E , there exists a unique smallest subsquare M_E of L that contains all of the entries in E .

We will now describe how to construct \mathcal{S}_{t+1} from \mathcal{S}_t for all $t \geq 2$. In fact, we will first construct a set \mathcal{S}_{t+1}^* from \mathcal{S}_t and then construct \mathcal{S}_{t+1} from \mathcal{S}_{t+1}^* by filtering. For each $E \in \mathcal{S}_t$ we construct \mathcal{S}_{t+1}^* by either:

Case I: If M_E is a subsquare of order at least k , then put E in \mathcal{S}_{t+1}^* .

Case II: Otherwise put $E \cup \{e\}$ in \mathcal{S}_{t+1}^* for every entry e of L outside of M_E such that e contains the same symbol as the entries in E .

Afterwards we filter \mathcal{S}_{t+1}^* to give \mathcal{S}_{t+1} in the following way. If $E, E' \in \mathcal{S}_{t+1}^*$ give rise to M_E that is a subsquare of $M_{E'}$, then we delete E' from \mathcal{S}_{t+1}^* as $M_{E'}$ will be accounted for at a later step (or if $M_E = M_{E'}$ then it is already accounted for). This completes the description of the algorithm.

Eventually $\mathcal{S}_t = \mathcal{S}_{t+1} = \mathcal{S}_{t+2}$ and so on, which is where we stop and call this final set \mathcal{S} . In Case II, the order of $M_{E \cup \{e\}}$ is at least twice the order of M_E , by Lemma 1.2.4. Therefore, every $E \in \mathcal{S}_t$ gives rise to a subsquare M_E of order at least $\min(k, 2^{t-1})$. It follows that we reach $\mathcal{S} = \mathcal{S}_t$ no later than when $2^{t-1} \geq k$, which occurs when $t \geq \log_2 k + 1$.

Claim: $|\mathcal{S}_{t+1}| \leq \frac{1}{2^{t-1}} |\mathcal{S}_t| (n - 2^{t-1})$ for all $t \geq 2$.

In constructing \mathcal{S}_{t+1} from \mathcal{S}_t , the algorithm maximises $|\mathcal{S}_{t+1}|$ when every $E \in \mathcal{S}_t$ requires Case II of the algorithm. In this case, for each $E \in \mathcal{S}_t$, since the order of M_E is at least 2^{t-1} , we find that $|\mathcal{S}_{t+1}^*| \leq |\mathcal{S}_t| (n - 2^{t-1})$. To prove the claim, it is now sufficient to show, that $|\mathcal{S}_{t+1}| \leq \frac{1}{2^{t-1}} |\mathcal{S}_{t+1}^*|$.

Suppose, in constructing \mathcal{S}_{t+1} from \mathcal{S}_t , the algorithm adds $E \cup \{e\}$ to \mathcal{S}_{t+1}^* and $E \cup \{e'\}$ to \mathcal{S}_{t+1}^* . Then there are no proper subsquares of $M_{E \cup \{e\}}$ that contain M_E except M_E itself, otherwise $E \cup \{e\}$ would have been filtered out. Therefore, if e' is an entry of $M_{E \cup \{e\}}$ outside of M_E , then $M_{E \cup \{e'\}} = M_{E \cup \{e\}}$. In filtering \mathcal{S}_{t+1}^* to give \mathcal{S}_{t+1} , the algorithm would therefore have filtered out $E \cup \{e'\}$. Since M_E is a subsquare of order at least 2^{t-1} , there are at least 2^{t-1} symbols e' in $M_{E \cup \{e\}}$ such that e' is outside of M_E and e' and e have the same symbol, by Lemma 1.2.4. Hence $|\mathcal{S}_{t+1}| \leq \frac{1}{2^{t-1}} |\mathcal{S}_{t+1}^*|$, proving the claim.

We can use the above claim to give a bound for $|\mathcal{S}|$ since $|\mathcal{S}| = |\mathcal{S}_{\lceil \log_2 k \rceil + 1}|$ and $|\mathcal{S}_2| \leq n \binom{n}{2}$. It is therefore sufficient to prove the following claim.

Claim: Each subsquare M^* of L of order between k and $2k - 1$ is M_E for some $E \in \mathcal{S}$.

To prove the claim, we need to show that $E \in \mathcal{S}_s$ such that $M_E = M^*$ for some $s \geq 1$. The algorithm then retains $E \in \mathcal{S}_{s+1}, \mathcal{S}_{s+2}$, and so on, until the algorithm terminates, implying $E \in \mathcal{S}$.

Suppose $F \in \mathcal{S}_t$, for some $t \geq 1$, and M_F is a subsquare of M^* . Lemma 1.2.4 implies that M_F is a subsquare of M^* of order less than k or $M_F = M^*$. If $M_F = M^*$, then we can set

$E = F$ to prove the claim, so assume $M_F \neq M^*$. In going from step t to $t + 1$, the algorithm puts $F \cup \{e\}$ in \mathcal{S}_{t+1} for some entry e of M^* , that is outside of M_F . We know that $M_{F \cup \{e\}}$ must be a subsquare of M^* , since every entry of $F \cup \{e\}$ is in M^* , and the order of $M_{F \cup \{e\}}$ is strictly greater than the order of M_F . If $M_{F \cup \{e\}} \neq M^*$ then we repeat this process with F replaced by $F \cup \{e\}$. Since the order of M^* is finite, we cannot keep repeating indefinitely. Therefore, we eventually reach $E \in \mathcal{S}_s$ for some $s \geq t$, for which $M_E = M^*$. \square

For example, we find that $I_k(L) \leq T_2(L) \leq \frac{1}{2}n^2(n-1)$ for $k \in \{2, 3\}$. However, the results listed earlier imply that $I_2(L) \leq \frac{1}{4}n^2(n-1)$ and $I_3(L) \leq \frac{1}{18}n^2(n-1)$, so we have not made an improvement when $k \in \{2, 3\}$. As another example, $I_k(L) \leq T_4(L) \leq \frac{1}{8}n^2(n-1)(n-2)$ for $k \in \{4, 5, 6, 7\}$. In comparison, Browning, Vojtěchovský and Wanless [35] showed that

- $I_4(L) \leq \frac{1}{96}n^2(n-1)(n-2)$,
- $I_5(L) \leq \frac{1}{300}n^2(n-1)(n-2)$,
- $I_6(L) \leq \frac{1}{2160}n^2(n-1)(n-2)(n-3)$ and
- $I_7(L) \leq \frac{1}{29400}n^2(n-1)(n-2)(n-3)$.

Theorem 4.2.1 therefore gives an improvement on (4.2) when $k \in \{6, 7\}$ (and in fact, for all $k \geq 6$), for sufficiently large n .

We can use Theorem 4.2.1 to provide an asymptotic bound on $I_k(L)$ and $W(L)$. The following equation follows since $I_k(L) \leq T_j(L)$ when $j = \lfloor k/2 \rfloor + 1$.

$$I_k(L) = O\left(n^{\lceil \log_2(\lfloor k/2 \rfloor + 1) \rceil + 2}\right)$$

for fixed k as $n \rightarrow \infty$. The next equation follows from $W(L) \leq 1 + n^2 + \sum_{j=1}^{\lceil \log_2 n \rceil} T_{2^j}(L)$.

$$W(L) = O\left(n^{\lceil \log_2 n \rceil + 2}\right)$$

as $n \rightarrow \infty$.

Let p be a prime, $n = p^a$ and $k = p^r$. For comparison, we will now consider the number of subsquares of order k in elementary Abelian groups $(\mathbb{Z}_p)^a$. Let Z be a Cayley table of $(\mathbb{Z}_p)^a$. The number of subgroups of order p^r in $(\mathbb{Z}_p)^a$ is given by the Gaussian binomial coefficient $\begin{bmatrix} a \\ r \end{bmatrix} = \prod_{i=1}^r (p^{a-r+i} - 1)/(p^i - 1)$ when $a \geq r$ (see, for example, [296]). If C_1 and C_2 are any two cosets of $(\mathbb{Z}_p)^a$, then the rows of Z indexed by C_1 and columns of Z indexed by C_2 form a subsquare [71, pp. 44–45]. Therefore $I_k(Z) = \begin{bmatrix} a \\ r \end{bmatrix} p^{2(a-r)}$. For comparison, when $p = 2$ the bound in Theorem 4.2.1 gives

- $I_4(L) \leq \frac{1}{8}n^2(n-1)(n-2) = 12 \cdot I_4(Z)$ and
- $I_8(L) \leq \frac{1}{64}n^2(n-1)(n-2)(n-4) = 168 \cdot I_8(Z)$,

where L is any Latin square of order n .

4.3 Which isotopisms are autotopisms?

Graph automorphisms play a pivotal role in graph theory. Similarly, autotopisms and automorphisms are a fundamental tool in the study of Latin squares. If we take a permutation α of n vertices, then we can always construct a graph on those vertices that admits the automorphism α , for example, the complete graph. However, as we will now discuss, for some isotopisms $\theta \in \mathcal{I}_n$ there does not exist any Latin square L for which $\theta(L) = L$.

The following definitions are central to our discussion.

- For any $\theta \in \mathcal{I}_n$, let $\Delta(\theta)$ be the number of Latin squares L of order n for which $\theta \in \text{Atop}(L)$.
- Let Ω_n be the set of all isotopisms $\theta \in \mathcal{I}_n$ for which $\theta \in \text{Atop}(L)$ for some Latin square L of order n , i.e. $\Omega_n = \{\theta \in \mathcal{I}_n : \Delta(\theta) > 0\}$.
- Let $\Xi_n = \{\alpha \in S_n : (\alpha, \alpha, \alpha) \in \Omega_n\}$.

We investigate the following questions.

Question 4.3.1. *Given $\theta \in \mathcal{I}_n$, is $\theta \in \Omega_n$?*

Question 4.3.2. *Given $\alpha \in S_n$, is $\alpha \in \Xi_n$?*

For the sake of the readers' eyes, we will use $L(i, j) = l_{ij}$ for a Latin square $L = (l_{ij}) = (L(i, j))$.

4.3.1 The equivalence

We will now identify an equivalence relation amongst isotopisms that preserves the value of Δ .

For $\theta, \varphi \in \mathcal{I}_n$ we use the convention that $\theta\varphi(L) = \theta(\varphi(L))$ for all Latin squares L of order n . For $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ and $\lambda \in \{\varepsilon, (rc), (rs), (cs), (rcs), (rsc)\}$ (the parastrophy group, see Section 1.2.1), denote by θ^λ the element of \mathcal{I}_n obtained from θ by permuting its components according to λ . For example $\theta^{(rc)} = (\beta, \alpha, \gamma)$ and $\theta^{(cs)} = (\alpha, \gamma, \beta)$.

Lemma 4.3.3. *Let $\lambda \in \{\varepsilon, (rc), (rs), (cs), (rcs), (rsc)\}$. Let $\theta, \varphi \in \mathcal{I}_n$ and let L be a Latin square of order n . Then*

1. $\theta \in \text{Atop}(L)$ if and only if $\varphi\theta\varphi^{-1} \in \text{Atop}(\varphi(L))$ and
2. $\theta \in \text{Atop}(L)$ if and only if $\theta^\lambda \in \text{Atop}(L^\lambda)$.

Proof. The following statements are equivalent.

$$\theta(L) = L \iff \varphi\theta(L) = \varphi(L) \iff (\varphi\theta\varphi^{-1})\varphi(L) = \varphi(L).$$

Thus proving the first claim. The second claim follows since λ permutes the entries of $O(L)$ uniformly. \square

The *cycle structure* of a permutation $\delta \in S_n$ is the list of cycle lengths in non-increasing order. Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$. We define the *cycle structure* of θ to be the multiset of cycle structures of α, β and γ . Since two permutations in S_n are conjugate if and only if they have the same cycle structure [44, p. 25], we deduce from Lemma 4.3.3 that the value of $\Delta(\theta)$ depends only on the cycle structure of θ . We can also deduce that the autotopism groups $\text{Atop}(L)$ and $\text{Atop}(\varphi(L))$ are conjugate in \mathcal{I}_n , and hence are isomorphic.

4.3.2 Autotopisms of Latin squares

We will now review and extend some important conditions for membership of Ω_n . It is difficult to provide a comprehensive survey of results concerning autotopisms of Latin squares, since the results might be found under a variety of research topics, for instance the algebraic theory of quasigroups or the study of graph decompositions. However, we would like to point out some recent publications. Falcón [113] determined all autotopisms of Latin squares of order $n \leq 11$ and gave several results of a general nature. Falcón and Martín-Morales [114] gave the non-zero values of $\Delta(\theta)$ for all $\theta \in \mathcal{I}_n$ for $n \leq 7$. McKay, Meynert and Myrvold [222] derived an important necessary condition for $\theta \in \Omega_n$ (see Theorem 4.3.6) in the course of enumerating quasigroups and loops up to isomorphism for orders up to 10. Hulpke, Kaski and Östergård [164] gave a detailed account of the autoparatopisms of Latin squares of order 11. Kerby and Smith [185] identified a relationship between Ξ_n and symmetric group characters.

The following lemmata are easy to observe. We include them for future reference.

Lemma 4.3.4. *If L is a Latin square and $\theta \in \text{Atop}(L)$ then $\theta^r \in \text{Atop}(L)$ for every $r \geq 1$. Consequently, $\theta \in \Omega_n$ implies $\theta^r \in \Omega_n$ for every $r \geq 1$ and $\alpha \in \Xi_n$ implies $\alpha^r \in \Xi_n$ for every $r \geq 1$.*

The *direct product* of two Latin squares L and L' of orders n and n' , respectively, is a Latin square $K = L \times L'$ of order nn' with entries $K((i, i'), (j, j')) = (L(i, j), L'(i', j'))$. The *direct product* of two permutations δ of \mathbb{Z}_n and δ' of $\mathbb{Z}_{n'}$ is defined by $(\delta \times \delta')(i, i') = (\delta(i), \delta'(i'))$.

Lemma 4.3.5. *Let L and L' be Latin squares such that $\theta = (\alpha, \beta, \gamma) \in \text{Atop}(L)$ and $\theta' = (\alpha', \beta', \gamma') \in \text{Atop}(L')$. Then $\theta \times \theta' \in \text{Atop}(L \times L')$ where $\theta \times \theta' = (\alpha \times \alpha', \beta \times \beta', \gamma \times \gamma')$.*

Let $c(\delta)$ denote the cycle structure of any $\delta \in S_n$. For $r \geq 1$, let $c^r(\delta)$ denote the list formed by sorting the concatenation of r copies of $c(\delta)$.

We will only need Lemma 4.3.5 in the special case of when $\theta' = (\varepsilon, \varepsilon, \varepsilon)$ is the trivial autotopism. If the order of L' is n' , then the cycle structure of $(\alpha, \beta, \gamma) \times (\varepsilon, \varepsilon, \varepsilon)$ is $\{c^{n'}(\alpha), c^{n'}(\beta), c^{n'}(\gamma)\}$. Note that it is possible to have $\theta \times (\varepsilon, \varepsilon, \varepsilon) \in \Omega_{nn'}$ while $\theta \notin \Omega_n$. For example, in Theorem 4.3.17 we will find that $(\alpha, \alpha, \alpha) \notin \Omega_n$ if n is even and α is an n -cycle, but if $n' = 2$ then $(\alpha, \alpha, \alpha) \times (\varepsilon, \varepsilon, \varepsilon) \in \Omega_{nn'}$.

Conditions

We begin our list of conditions for membership of Ω_n with the following theorem by McKay, Meynert and Myrvold [222].

Theorem 4.3.6. *Let L be a Latin square of order n and let (α, β, γ) be a non-trivial autotopism of L . Then either*

- (a) α, β and γ have the same cycle structure with at least 1 and at most $\lfloor n/2 \rfloor$ fixed points, or
- (b) one of α, β or γ has at least 1 fixed point and the other two have the same cycle structure with no fixed points, or
- (c) α, β and γ have no fixed points.

It is clear that a non-trivial autotopism must have at least two non-trivial components. Lemma 4.3.3 implies that the following theorem is sufficient to characterise all non-trivial autotopisms with one trivial component.

Theorem 4.3.7. *Let $\theta = (\alpha, \beta, \varepsilon) \in \mathcal{I}_n$. Then $\theta \in \Omega_n$ if and only if both α and β consist of n/d d -cycles for some divisor d of n .*

Proof. The necessity was proved in [201, Lem. 1.1] and rediscovered in [113, 126]. The converse follows from Lemma 4.3.5 since the Cayley table of \mathbb{Z}_n admits the autotopism

$$((0, 1, \dots, n-1), (n-1, n-2, \dots, 0), \varepsilon)^{n/d}$$

for every divisor d of n . □

There is a fundamental error in Lemma 1.2 of [201] causing the subsequent results to be unreliable; for example it implies $\Delta((\alpha, \alpha, \varepsilon)) = 252720/19$ when $n = 6$ and $\alpha = (012)(345)$, which is not even an integer.

The evaluation of $\Delta(\theta)$ when $\theta = (\alpha, \alpha, \varepsilon)$ was also studied by Ganfornina [126] (also known as Falcón). For instance, he gave an explicit formula for $\Delta(\theta)$ when α consists of n/d cycles of length $d \in \{1, 2, 3\}$. When $n = 6$ and $\alpha = (012)(345)$, we find that $\Delta((\alpha, \alpha, \varepsilon)) = 6! \cdot 3!^2 = 25920$, both through a computer enumeration and by using Ganfornina's formula.

We will now give our first new necessary condition for membership of Ω_n .

Theorem 4.3.8. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be an autotopism of a Latin square L . If i belongs to an a -cycle of α and j belongs to a b -cycle of β , then $L(i, j)$ belongs to a c -cycle of γ , where $\text{lcm}(a, b) = \text{lcm}(b, c) = \text{lcm}(a, c) = \text{lcm}(a, b, c)$.*

Proof. The orbit of the entry $(i, j, L(i, j))$ of L under $\langle \theta \rangle$, the group generated by θ , has cardinality $\text{lcm}(a, b)$. Therefore $\theta^{\text{lcm}(a, b)} = (\varepsilon, \varepsilon, \varepsilon)$ and so c must divide $\text{lcm}(a, b)$. Hence $\text{lcm}(a, b) = \text{lcm}(a, b, c)$. The result follows since $\theta^\lambda \in \text{Atop}(L^\lambda)$ for all λ by Lemma 4.3.3. □

Theorem 4.3.8 is useful for proving $\theta \notin \Omega_n$. For example, if α has an a -cycle and β has a b -cycle, but γ does not have a c -cycle where $\text{lcm}(a, b) = \text{lcm}(b, c) = \text{lcm}(a, c) = \text{lcm}(a, b, c)$, then $(\alpha, \beta, \gamma) \notin \Omega_n$.

We will now identify a corollary that identifies an important class of subsquares of Latin squares with non-trivial autotopisms. First, we will need to introduce some notation. Recall that we use $\mathbb{N} = \{1, 2, \dots\}$ and let $S \subseteq \mathbb{N}$ be such that (a) $\text{lcm}(a, b) \in S$ whenever $a, b \in S$ and (b) $\text{lcm}(a, x) \notin S$ whenever $a \in S$ and $x \in \mathbb{N} \setminus S$. We call S a *strongly lcm-closed set*. The finite strongly lcm-closed sets are the sets $\{d \in \mathbb{N} : d \text{ divides } n\}$ for some $n \in \mathbb{N}$. However, there are also infinite strongly lcm-closed sets, such as $\{a \in \mathbb{N} : a \not\equiv 0 \pmod{p}\}$ and $\{p^a : a \geq 0\}$ for any prime p .

Let $L = (L(i, j))$ be a Latin square with $\theta = (\alpha, \beta, \gamma) \in \text{Atop}(L)$. Suppose M is a subsquare of L formed by the rows $R \subseteq \mathbb{Z}_n$ and columns $C \subseteq \mathbb{Z}_n$. Let $S = \{L(i, j) : i \in R \text{ and } j \in C\}$, so $|R| = |C| = |S|$. Suppose R , C and S are closed under the action of $\langle \alpha \rangle$, $\langle \beta \rangle$ and $\langle \gamma \rangle$, respectively. By restricting the domains of α , β and γ to R , C and S , respectively, we see that M admits an autotopism, which we will denote θ_M . We acknowledge the possibility that R , C and S may not be the same sets, but this issue can be resolved by establishing bijections with $\{0, 1, \dots, |R| - 1\}$.

Corollary 4.3.9. *Let S be a strongly lcm-closed set. Let L be a Latin square with $\theta = (\alpha, \beta, \gamma) \in \text{Atop}(L)$. Let M be the submatrix of L formed by every row whose index belongs to an a -cycle of α and every column whose index belongs to a b -cycle in β , over all $a, b \in S$. Then either M is a subsquare of L that admits the autotopism θ_M or M is empty.*

Proof. Assume M is non-empty and $M \neq L$. Suppose an arbitrary symbol in M belongs to a c -cycle of γ . For some $a, b \in S$, this symbol occurs in a row that belongs to an a -cycle of α and a column that belongs to a b -cycle of β . Theorem 4.3.8 implies that $\text{lcm}(a, b) = \text{lcm}(b, c) = \text{lcm}(a, c) = \text{lcm}(a, b, c)$. Hence $\text{lcm}(a, c) = \text{lcm}(a, b) \in S$ since S is a strongly lcm-closed set and moreover, $c \in S$. Therefore, every symbol in M belongs to a c -cycle of γ , for some $c \in S$.

Pick an entry $(i, j, L(i, j))$ in a row that belongs to an r -cycle of α such that $r \notin S$ and a column that belongs to a b -cycle of β with $b \in S$. Suppose $L(i, j)$ belongs to an x -cycle of γ . Theorem 4.3.8 implies that $\text{lcm}(b, x) = \text{lcm}(b, r)$, but $\text{lcm}(b, r) \notin S$ since $r \notin S$. Hence $x \notin S$. We can argue similarly with rows and columns switched. Hence every symbol outside of M , but sharing a row or column with M , belongs to an x -cycle of γ for some $x \notin S$. Hence M is a subsquare of L .

That θ_M is an autotopism of M follows from the earlier discussion. \square

In particular, when $S = \{1\}$, Corollary 4.3.9 identifies the (possibly empty) subsquare formed by the fixed rows and columns of θ . The following corollary is a special case of Corollary 4.3.9.

Corollary 4.3.10. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$. Suppose L is a Latin square of order n with $\theta \in \text{Atop}(L)$. If γ contains an c -cycle, then*

$$\sum_{b|c} bs_b(\alpha) = \sum_{b|c} bs_b(\beta).$$

For example,

$$\theta = ((123456)(789), (123)(456)(78)(9), (123456)(789)) \in \mathcal{I}_9$$

satisfies $\sum_{b|3} bs_b(\alpha) = 3 < 7 = \sum_{b|3} bs_b(\beta)$. Corollary 4.3.10 therefore implies that $\theta \notin \Omega_n$.

The next necessary condition for membership of Ω_n identifies when we can find enough room in a Latin square L to place all n copies of each symbol satisfying Theorem 4.3.8 such that $\theta \in \text{Atop}(L)$. The permanent of an $n \times n$ square matrix was defined in Section 1.2.4. In particular, if X is an $n \times n$ matrix with entries in $\{0, 1\} \subseteq \mathbb{Z}$, then $\text{PER}(X)$ counts the number of $n \times n$ permutation matrices that embed into X .

Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ and suppose $s \in \mathbb{Z}_n$ belongs to a c -cycle in γ . We define $X_s = X_s(i, j)$ to be the $(0, 1)$ -matrix with $X_s(i, j) = 1$ if i belongs to an a -cycle of α and j belongs to a b -cycle of β such that $\text{lcm}(a, b) = \text{lcm}(b, c) = \text{lcm}(a, c) = \text{lcm}(a, b, c)$, and $X_s(i, j) = 0$ otherwise. Informally, the 0's in X_s mark the positions where Theorem 4.3.8 says a symbol s cannot be placed in a Latin square L of order n with $\theta \in \text{Atop}(L)$.

If $\theta \in \text{Atop}(L)$ for some Latin square L of order n , then the copies of the symbol s in L identify a permutation matrix embedded in X_s . Hence we have just proved the following theorem.

Theorem 4.3.11. *Let $\theta \in \mathcal{I}_n$. If $\theta \in \Omega_n$ then $\text{PER}(X_s) > 0$ for all $s \in \mathbb{Z}_n$.*

To illustrate, let $\theta = (\alpha, \alpha, \alpha) \in \mathcal{I}_{23}$ be such that $(6, 3, 3, 3, 2, 2, 2, 2)$ is the cycle structure of α . Consider X_s for some s that belongs to a 2-cycle in γ . Note that $X_s(i, j) = 0$ whenever i belongs to an a -cycle in α and j belongs to an b -cycle in β where $(a, b) \in \{(2, 3), (2, 6), (3, 2), (3, 3), (6, 2)\}$. For instance, $X_s(i, j) = 0$ if $(a, b) = (3, 3)$ since $\text{lcm}(3, 3) < \text{lcm}(2, 3)$. It is now not too difficult to see that $\text{PER}(X_s) = 0$. Hence, Theorem 4.3.11 implies that $\theta \notin \Omega_n$.

We now consider the following theorem, which was proved by McKay, Meynert and Myrvold [222, Lem. 4], although they did not state it in the following form.

Theorem 4.3.12. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$. Suppose that $n \equiv 2 \pmod{4}$ and every cycle in α, β and γ has length 2. Then $\theta \notin \Omega_n$.*

We will later generalise Theorem 4.3.12 by Theorem 4.3.17, where we identify the class of automorphisms in Ξ_n that have every non-trivial cycle length equal. In the following theorem, we observe that sometimes θ' is of the form in Theorem 4.3.12, while θ is not.

Theorem 4.3.13. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$. Suppose that $n \equiv 2 \pmod{4}$ and every cycle in α, β and γ has length congruent to 2 modulo 4. Then $\theta \notin \Omega_n$.*

Proof. Let $\{d_1, d_2, \dots, d_k\}$ be the set of cycle lengths in α, β and γ . Then the order of θ in \mathcal{I}_n is $\text{Ord}(\theta) = \text{lcm}_{1 \leq i \leq k} d_i \equiv 2 \pmod{4}$. Hence $\text{Ord}(\theta)/2$ is odd. Since every cycle in α, β and γ is of even length, every cycle in $\alpha^{\text{Ord}(\theta)/2}, \beta^{\text{Ord}(\theta)/2}$ and $\gamma^{\text{Ord}(\theta)/2}$ is of length 2. The result now follows from Lemma 4.3.4 and Theorem 4.3.12. \square

Falc3n [113] identified six non-equivalent isotopisms θ (in the sense of Lemma 4.3.3), for which he proved computationally that $\theta \notin \Omega_n$ but no theoretical reason was known. Five of these cases are resolved theoretically by Theorem 4.3.13. The remaining has the same cycle structure as

$$\theta = ((1, 2, 3, 4)(5, 6), (1, 2, 3, 4)(5, 6), (1, 2, 3, 4)(5)(6)) \in \mathcal{I}_6. \quad (4.3)$$

If one attempts to construct a Latin square L with this $\theta \in \text{Atop}(L)$, then an unusual clash arises. It arises again when $n = 14$ in the isotopism $\theta' = (\alpha, \alpha, \gamma)$ where

$$\begin{aligned} \alpha &= (1, 2, 3, 4, 5, 6, 7, 8)(9, 10, 11, 12)(13, 14) \text{ and} \\ \gamma &= (1, 2, 3, 4, 5, 6, 7, 8)(9, 10, 11, 12)(13)(14). \end{aligned}$$

If one attempts to construct a Latin square L with this $\theta' \in \text{Atop}(L)$, then Corollary 4.3.9 implies that the rows and columns indexed by 9, 10, \dots , 14 form a subsquare M of L , which admits the autotopism θ_M with the same cycle structure as in (4.3).

4.3.3 Simple permutations and contours

The notion of cycle structure of an isotopism θ is crucial in characterising Ω_n . Since two isotopisms with the same cycle structure have the same Δ value, we can pick whichever is easiest to work with. We also use of the total order $0 < 1 < \dots < n - 1$ on \mathbb{Z}_n .

Each $\alpha \in S_n$ can be decomposed into disjoint cycles α_i . Let d_i be the length of α_i . We can assume $d_1 \geq d_2 \geq \dots$. Each cycle α_i can be written as $(t_i, \alpha(t_i), \alpha^2(t_i), \dots, \alpha^{d_i-1}(t_i))$. We will take t_i to be the minimum of $\{t_i, \alpha(t_i), \dots, \alpha^{d_i-1}(t_i)\}$, and call t_i the *leading entry* of α_i . We say α is written in *canonical form* when it is written in this manner.

For $\alpha \in S_n$ define α^{simp} to be the unique permutation with the same cycle structure as α such that each α_i is the cycle $(t_i, t_i+1, \dots, t_i+d_i-1)$ and the leading entry $t_i < t_j$ whenever $i < j$ and $d_i = d_j$. We will refer to α^{simp} as a *simple* permutation. When simple permutations are written in canonical form they read $1, 2, \dots, n$, with some parentheses. We say $\theta = (\alpha, \beta, \gamma)$ is *simple* if α, β and γ are simple and define $\theta^{\text{simp}} = (\alpha^{\text{simp}}, \beta^{\text{simp}}, \gamma^{\text{simp}})$. By Lemma 4.3.3, $\theta \in \Omega_n$ if and only if $\theta^{\text{simp}} \in \Omega_n$.

For example, the permutation of \mathbb{Z}_8 given in two-row format by

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 2 & 0 & 1 & 4 & 7 & 6 \end{pmatrix}$$

has the canonical form $(1, 5, 4)(0, 3)(6, 7)(2)$ with cycle lengths $d_1 = 3, d_2 = 2, d_3 = 2$ and $d_4 = 1$ and leading entries $t_1 = 1, t_2 = 0, t_3 = 6$ and $t_4 = 2$. The permutation $\alpha^{\text{simp}} = (0, 1, 2)(3, 4)(5, 6)(7)$ is written in canonical form, which has leading entries $t_1 = 0, t_2 = 3, t_3 = 5$ and $t_4 = 7$.

Suppose we have the autotopism $\theta = (\alpha, \beta, \gamma)$ where $\alpha = (0, 1)(2)(3), \beta = (2, 3)(0)(1)$ and $\gamma = (0, 1)(2)(3)$. We observe that θ^{simp} is an autotopism (and in fact an automorphism) of the Latin square

$$L = \begin{array}{|c|c|c|c|} \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline 0 & 1 & 2 & 3 \\ \hline 1 & 0 & 3 & 2 \\ \hline \end{array}.$$

We can therefore deduce that $\theta \in \Omega_n$. Observe that the placement of the horizontal and vertical lines uniquely determine α^{simp} and β^{simp} . In fact, L can be reconstructed from knowledge of

2	.	0	.
3	.	.	0
0	.	2	3
.	0	3	2

and $\gamma = (0, 1)(2)(3)$. We call a diagram a *contour* of θ if we can construct from it a Latin square L with $\theta \in \text{Atop}(L)$. Importantly, a contour of $\theta = (\alpha, \beta, \gamma)$ gives knowledge of

- (a) α, β and γ and
- (b) a representative from each orbit of $O(L)$ under $\langle \theta \rangle$, the group generated by θ .

For our purpose, we will only need to consider simple isotopisms. In this case, $\alpha^{\text{simp}}, \beta^{\text{simp}}$ and γ^{simp} are determined by their cycle structures. Typically, our contours display only leading entries of γ^{simp} .

Suppose $\theta = (\alpha, \beta, \gamma)$ is an autotopism of a Latin square L . If x and y are the leading entries in non-trivial cycles of α and β , respectively, and if $L(x, y) = z$, we will typically see the following in L .

	y	$\beta(y)$	$\beta^2(y)$	\dots
x	z			
$\alpha(x)$		$\gamma(z)$		
$\alpha^2(x)$			$\gamma^2(z)$	
\vdots				\ddots

This depicts part of the orbit of the entry $(x, y, z) \in O(L)$ under the action of $\langle \theta \rangle$. However, the orbit of x under $\langle \alpha \rangle$ may not be of the same cardinality as the orbit of y under $\langle \beta \rangle$. For example, if x is in a 2-cycle in α and y is in a 6-cycle in β , the orbit of (x, y, z) looks like the following.

	y	$\beta(y)$	$\beta^2(y)$	$\beta^3(y)$	$\beta^4(y)$	$\beta^5(y)$
x	z		$\gamma^2(z)$		$\gamma^4(z)$	
$\alpha(x)$		$\gamma(z)$		$\gamma^3(z)$		$\gamma^5(z)$

In this case, we additionally require that $\gamma^6(z) = z$ and $\gamma^2(z) \neq z$ and $\gamma^4(z) \neq z$; an observation that was made generally in Theorem 4.3.8.

Later in this chapter, we will claim to have found a contour for various isomorphisms. We will use the following lemma, Lemma 4.3.14, to prove that our purported contour is indeed a contour.

Let $\theta^{\text{simp}} = (\alpha^{\text{simp}}, \beta^{\text{simp}}, \gamma^{\text{simp}}) \in \mathcal{I}_n$ and suppose L is a Latin square of order n with $\theta^{\text{simp}} \in \text{Atop}(L)$. Let α_i and β_j be any two cycles in α^{simp} and β^{simp} , respectively. Let M be the submatrix of L formed by the intersection of the rows of L whose indices belong to α_i and the columns of L whose indices belong to β_j . The submatrix M will be called an $a \times b$ block of L , where a is the length of α_i and b is the length of β_j . We will similarly define the term “block” of a partial $n \times n$ matrix C (for example, a contour) whose rows and columns indices are \mathbb{Z}_n . A cell orbit of the $a \times b$ block B defined by α_i and β_j refers to the set of cells $\{(\alpha_i^r(k_1), \beta_j^r(k_2)) : r \in \mathbb{Z}\}$ where (k_1, k_2) is any cell within B .

We will need one more convention before we continue further. Our rows, columns and symbols all belong to the ring \mathbb{Z}_n . However, in the next lemma for example, we will want to discuss row indices (or column indices) modulo r for some r that does not necessarily divide n . In this case, we replace each index $i \in \mathbb{Z}_n$ by its least non-negative representative.

Lemma 4.3.14. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be a simple isotopism. Let Γ be the set of all leading entries of γ . Let C be a partial matrix of order n . Suppose:*

- (a) *C is a partial Latin square, i.e. every symbol in C is in $\Gamma \subseteq \mathbb{Z}_n$ and any symbol occurs at most once in each row and each column.*
- (b) *Every $a \times b$ block B of C contains precisely $\gcd(a, b)$ symbols from Γ , all in distinct cell orbits of B .*
- (c) *If $z \in \Gamma$ is a symbol in an $a \times b$ block, then z belongs to a c -cycle of γ such that $\text{lcm}(a, b) = \text{lcm}(b, c) = \text{lcm}(a, b, c)$.*
- (d) *If $z \in \Gamma$ belongs to a c -cycle of γ , then:*
 - (i) *If two copies of z are in distinct rows i and i' in C then either i and i' belong to distinct cycles of α or $i \not\equiv i' \pmod{\gcd(a, c)}$.*
 - (ii) *If two copies of z are in distinct columns j and j' in C then either j and j' belong to distinct cycles of β or $j \not\equiv j' \pmod{\gcd(b, c)}$.*

Then C uniquely determines a Latin square with autotopism θ .

Proof. We take C and apply $\langle \theta \rangle$, the group generated by θ , to construct L , which we claim is a Latin square. Specifically, if (i, j, z) is an entry of C then $(\alpha^r(i), \beta^r(j), \gamma^r(z))$ is also an entry of L for all $r \geq 1$.

There are precisely $\gcd(a, b)$ cell orbits of an $a \times b$ block. Therefore, condition (b) guarantees that every cell of L contains at least one entry. Condition (c) guarantees that every cell within L contains at most one entry (see Theorem 4.3.8). Therefore, we conclude that every cell of L contains a unique entry.

It is now sufficient to show that any given row or column contains only distinct symbols. Firstly, observe that if two copies of the same symbol occur in the same row, then two copies of a symbol in Γ occur in some row. A similar statement is also true for columns. Therefore, we need only show that every row and every column does not contain two copies of some $z \in \Gamma$.

Suppose (i, j, z) is an entry of C in a block B and z belongs to a c -cycle of γ . The entry $(\alpha^r(i), \beta^r(j), \gamma^r(z))$ contains the symbol z whenever c divides r . Therefore, B contains exactly $\text{lcm}(a, b)/c$ copies of z in entries along the cell orbit $\{(\alpha^r(i), \beta^r(j)) : r \in \mathbb{Z}\}$. In fact

- B contains a copy of z in row i' whenever $i \equiv i' \pmod{\gcd(a, c)}$ and
- B contains a copy of z in column j' whenever $j \equiv j' \pmod{\gcd(b, c)}$.

Hence conditions (d)(i) and (d)(ii) are necessary. Since we have assumed that C is a partial Latin square, there were no clashes initially. To ensure no clashes are generated by $\langle \theta \rangle$ from C , conditions (d)(i) and (d)(ii) are sufficient. \square

4.3.4 Automorphisms of Latin squares

In this section we will consider whether $\theta \in \Omega_n$ when $\theta = (\alpha, \alpha, \alpha)$ is an isomorphism, that is, whether $\alpha \in \Xi_n$. Recall that automorphisms play an important role in the study of quasigroups, which were discussed in Section 1.2.2. In fact, Lemma 4.3.3 allows us to deduce that $\Delta(\theta) = \Delta((\alpha, \alpha, \alpha))$ whenever each component of θ has the same cycle structure as α . This includes cases where θ is not an isomorphism, but has the same cycle structure as an isomorphism.

Automorphisms with all non-trivial cycles of the same length

We start with the following result, which was given by Wanless [323] (see also [41]).

Theorem 4.3.15. *If $\alpha \in S_n$ is a d -cycle, where $2 \leq d \leq n$, then $\alpha \in \Xi_n$ if and only if either $d = n$ is odd or $\lceil n/2 \rceil \leq d < n$.*

The work throughout Section 4.3.4 will expand upon Theorem 4.3.15. For example, Theorem 4.3.17 is a generalisation of Theorem 4.3.15.

Theorem 4.3.16. *Suppose that $\alpha \in S_n$ consists of m non-trivial cycles without fixed points, and each cycle has the same length d . If m is odd and d is even, then $\alpha \notin \Xi_n$, otherwise $\alpha \in \Xi_n$.*

Proof. Case I: d is odd (m may be even or odd). Theorem 4.3.15 states that $(0, 1, \dots, d-1) \in \Xi_d$. We now use a direct product (i.e. Lemma 4.3.5) to show that $\alpha \in \Xi_n$.

Case II: both d and m are even. It is sufficient to show that $\alpha \in \Xi_n$ when $m = 2$, since the rest of this case then follows from Lemma 4.3.5. When $m = 2$, we construct the desired Latin square from the following contour C . If $d \geq 2$, let

$$\begin{aligned} C(d/2 - i, i - 1) &= 0 && \text{for } 1 \leq i \leq d/2, \\ C(d/2 - i - 1, i - 1) &= d && \text{for } 1 \leq i \leq d/2 - 1, \\ C(d - 1, d/2 - 1) &= d. \end{aligned}$$

Let $\beta = (0, 1, \dots, 2d - 1)$. We construct the remainder of C by applying the isotopisms $(\alpha^{d/2}, \beta^d, \varepsilon)$ and $(\beta^d, \alpha^{d/2}, \varepsilon)$. We display the constructed contours for $d = 2, 4, 6$ and 8 in Figure 4.4. Finally, we appeal to Lemma 4.3.14 to show that C is indeed a contour.

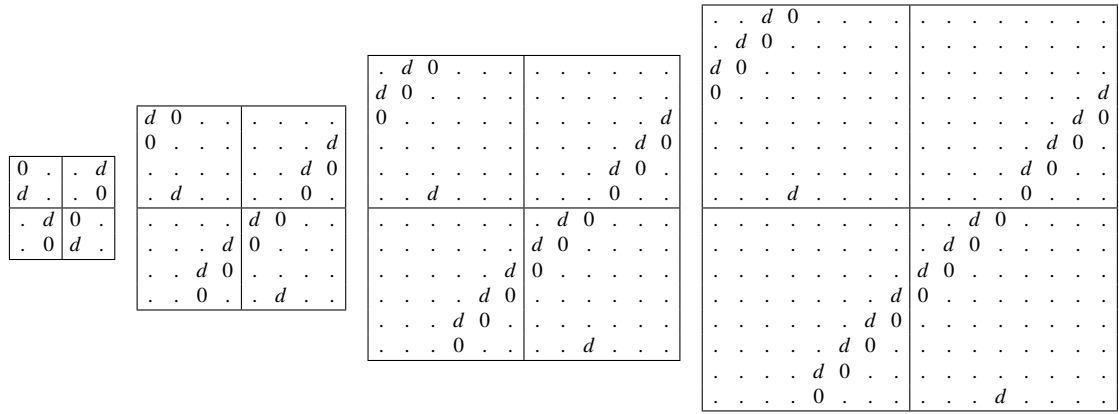


FIGURE 4.4: Contours from the proof of Theorem 4.3.16.

Case III: d is even and m is odd. We have $n = md$. By Lemma 4.3.3, we can assume $\alpha = \alpha^{\text{simp}}$, that is

$$\alpha = (0, 1, \dots, d-1)(d, d+1, \dots, 2d-1) \cdots ((m-1)d, (m-1)d+1, \dots, md-1).$$

Let $L = (L(i, j))$ be a Latin square of order n such that $(\alpha, \alpha, \alpha) \in \text{Aut}(L)$. We replace each symbol in L by its least non-negative representative. For any row i we have

$$\sum_{j=0}^{n-1} L(i, j) = \frac{n(n-1)}{2} \quad \text{and so} \quad \sum_{r=0}^{m-1} \sum_{j=0}^{n-1} L(dr, j) = m \frac{n(n-1)}{2}. \quad (4.4)$$

Similarly, for any column j we have

$$\sum_{i=0}^{n-1} L(i, j) = \frac{n(n-1)}{2}. \quad (4.5)$$

Consider the the first row and column of the $d \times d$ block of L with its “top-left corner” indexed by (dr, ds) , for arbitrary $0 \leq r, s \leq m-1$. Then

$$\begin{aligned}
 \sum_{t=1}^{d-1} L(dr+t, ds) &= \sum_{t=1}^{d-1} L(dr+d-t, ds) && \text{change of variables} \\
 &= \sum_{t=1}^{d-1} L(\alpha^{-t}(dr), \alpha^{-t}(ds+t)) \\
 &= \sum_{t=1}^{d-1} \alpha^t(L(dr, ds+t)) && \text{by (1.3)} \\
 &\equiv \sum_{t=1}^{d-1} (L(dr, ds+t) + t) \pmod{d} && (4.6)
 \end{aligned}$$

Thus

$$\begin{aligned}
 m \frac{n(n-1)}{2} &= \sum_{r=0}^{m-1} \sum_{s=0}^{m-1} \left(\sum_{t=0}^{d-1} L(dr+t, ds) \right) && \text{by (4.5)} \\
 &\equiv \sum_{r=0}^{m-1} \sum_{s=0}^{m-1} \left(\sum_{t=0}^{d-1} (L(dr, ds+t) + t) \right) \pmod{d} && \text{by (4.6)} \\
 &= m^2 \sum_{t=0}^{d-1} t + \sum_{r=0}^{m-1} \sum_{j=0}^{n-1} L(dr, j) && \text{change of variables} \\
 &= m^2 \frac{d(d-1)}{2} + m \frac{n(n-1)}{2}. && \text{by (4.4)}
 \end{aligned}$$

We conclude that $m^2 d(d-1)/2 \equiv 0 \pmod{d}$, but this contradicts our assumption that d is even and m is odd. \square

Theorem 4.3.16 generalises a result (the $m = 1$ case of Theorem 4.3.16), which was proved by Euler [97] in the context of orthomorphisms of \mathbb{Z}_n . We extend Theorem 4.3.16 to include the case of when α has fixed points in the following theorem, thus generalising Theorem 4.3.15.

Theorem 4.3.17. *Suppose that $\alpha \in S_n$ has precisely m non-trivial cycles of length d . If α has no fixed points, then $\alpha \in \Xi_n$ if and only if m is even or d is odd. If α has at least one fixed point, then $\alpha \in \Xi_n$ if and only if $n \leq 2md$.*

Proof. The theorem is true if α does not have a fixed point, by Theorem 4.3.16. So assume α has at least one fixed point, i.e. $n > md$. If $n > 2md$ then $\alpha \notin \Xi_n$ by Theorem 4.3.6. If $md < n \leq 2md$, Theorem 4.3.15 guarantees the existence of a Latin square of order n with automorphism $\omega = (0, 1, \dots, md-1)(md)(md+1) \cdots (n-1)$ and so $\omega^m \in \Xi_n$ by Lemma 4.3.4. Since ω^m has the same cycle structure as α , Lemma 4.3.3 implies $\alpha \in \Xi_n$. \square

Automorphisms with two non-trivial cycles

In this subsection we classify when $\alpha \in \Xi_n$ for $\alpha \in S_n$ that consist of precisely two non-trivial cycles.

Theorem 4.3.18. *Suppose $\alpha \in S_n$ consists of a d_1 -cycle, a d_2 -cycle and d_∞ fixed points.*

- *If $d_1 = d_2$ then $\alpha \in \Xi_n$ if and only if $0 \leq d_\infty \leq 2d_1$.*
- *If $d_1 > d_2$ then $\alpha \in \Xi_n$ if and only if (a) d_2 divides d_1 , (b) $d_1 \geq \lceil n/2 \rceil$, (c) $d_2 \geq d_\infty$ and (d) if d_2 is even then $d_\infty > 0$.*

Proof. The $d_1 = d_2$ case is resolved by Theorem 4.3.17, so assume $d_1 > d_2$. By Lemma 4.3.3 we can assume $\alpha = \alpha^{\text{simp}}$. We depict the structure of a Latin square L with $(\alpha, \alpha, \alpha) \in \text{Aut}(L)$ in Figure 4.5. Let $D_1 = \{0, 1, \dots, d_1 - 1\}$, $D_2 = \{d_1, d_1 + 1, \dots, d_1 + d_2 - 1\}$ and $D_\infty = \{d_1 + d_2, d_1 + d_2 + 1, \dots, n - 1\}$, so $d_i = |D_i|$ for $i \in \{1, 2, \infty\}$. Hence L is partitioned into nine submatrices M_{ij} , where $i, j \in \{1, 2, \infty\}$, such that the rows of M_{ij} are indexed by D_i and the columns of M_{ij} are indexed by D_j . We write $k : m_k$ in some M_{ij} if every element of D_k appears in M_{ij} precisely m_k times.

L	D_1	D_2	D_∞
D_1	1 : $d_1 - d_2 - d_\infty$ 2 : d_1 ∞ : d_1	1 : d_2	1 : d_∞
D_2	1 : d_2	2 : $d_2 - d_\infty$ ∞ : d_2	2 : d_∞
D_∞	1 : d_∞	2 : d_∞	∞ : d_∞

FIGURE 4.5: Diagram of L with $d_1 > d_2$ the only non-trivial cycle lengths.

Corollary 4.3.9 and Theorem 4.3.8 imply that $M_{\infty\infty}$ (shaded dark gray in Figure 4.5) is a subsquare that has the symbol set D_∞ . Observe that $\{r \in \mathbb{N} : r \text{ divides } d_2\}$ is a strongly lcm-closed set that does not contain d_1 . Therefore Corollary 4.3.9 also implies that the submatrix K formed by M_{22} , $M_{2\infty}$, $M_{\infty 2}$ and $M_{\infty\infty}$ (comprising of the shaded regions in Figure 4.5) is also a subsquare. Theorem 4.3.8 implies that K has the symbol set $D_2 \cup D_\infty$. Since $M_{\infty\infty}$ and K are both subsquares, we can deduce that L indeed has the structure depicted in Figure 4.5.

The necessity of the conditions (a)–(d) can be observed in Figure 4.5 in the following way.

- Applying Theorem 4.3.8 to any entry in M_{12} gives $\text{lcm}(d_1, d_2) = \text{lcm}(d_1, d_1) = d_1$, so d_2 must divide d_1 .
- Since K is a subsquare, Lemma 1.2.4 on page 17 implies that $n - d_1 = d_2 + d_\infty \leq \lfloor n/2 \rfloor$. Thus $d_1 \geq n - \lfloor n/2 \rfloor = \lceil n/2 \rceil$.
- We have $d_2 \geq d_\infty$ otherwise $M_{2\infty}$ is impossible.
- If $d_\infty = 0$ then Corollary 4.3.9 implies that $K = M_{22}$ is a $d_2 \times d_2$ subsquare with an automorphism consisting of a single cycle of length d_2 . So d_2 must be odd by Theorem 4.3.15.

For the rest of the proof assume that conditions (a)–(d) hold. Our task is to find a Latin square L such that $(\alpha, \alpha) \in \text{Aut}(L)$.

Case I: d_1 is odd, d_2 is odd and $d_\infty = 0$. We define a contour $C = C(i, j)$, satisfying the conditions of Lemma 4.3.14, in the following way.

$$\begin{aligned}
 C(d_1 - i, i - 1) &= d_1 && \text{for } 1 \leq i \leq d_2, \\
 C(d_1 - d_2 - i, d_2 + i - 1) &= 0 && \text{for } 1 \leq i \leq d_1 - d_2, \\
 C(d_1 - i, d_1 + i - 1) &= 0 && \text{for } 1 \leq i \leq d_2, \\
 C(d_1 + d_2 - i, i - 1) &= 0 && \text{for } 1 \leq i \leq d_2, \\
 C(d_1 + d_2 - i, d_1 + i - 1) &= d_1 && \text{for } 1 \leq i \leq d_2.
 \end{aligned}$$

This contour is illustrated in Figure 4.6(a) for $d_1 = 9$ and $d_2 = 3$.

Case II: d_1 is even, d_2 is odd, and $d_\infty = 0$. We define a contour $C = C(i, j)$, satisfying the conditions of Lemma 4.3.14, in the following way.

$$\begin{aligned}
 C(i - 1, d_1 - i) &= 0 && \text{for } 1 \leq i \leq d_1/2, \\
 C(d_1/2, d_1) &= 0, \\
 C(d_1/2 + i, d_1/2 - i) &= 0 && \text{for } 1 \leq i \leq d_1/2 - d_2, \\
 C(d_1 - d_2 + i, d_1 + d_2 - i) &= 0 && \text{for } 1 \leq i \leq d_2 - 1, \\
 C(d_1 - d_2 + i, d_2 - i) &= d_1 && \text{for } 1 \leq i \leq d_2 - 1, \\
 C(0, 0) &= d_1, \\
 C(d_1 + i - 1, d_2 - i) &= 0 && \text{for } 1 \leq i \leq d_2, \\
 C(d_1 + i - 1, d_1 + d_2 - i) &= d_1 && \text{for } 1 \leq i \leq d_2.
 \end{aligned}$$

This is illustrated in Figure 4.6(b) for $d_1 = 12$ and $d_2 = 3$.

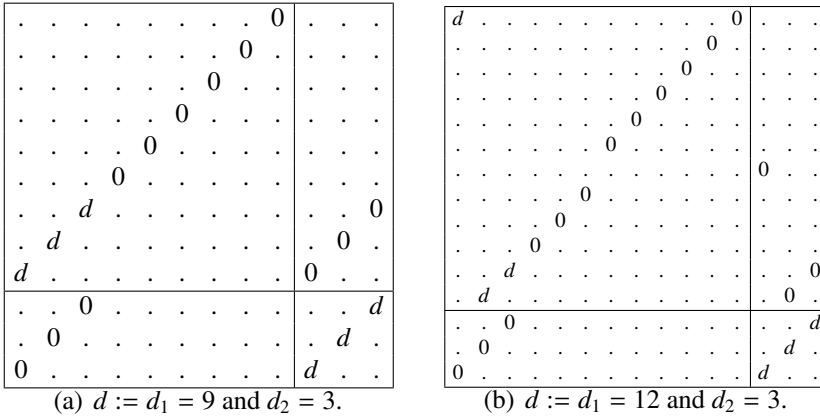


FIGURE 4.6: Some contours C .

For the remainder of this proof we will not continue to define C inside the subsquare K because K can be found independently of the rest of L . With the assumptions of the theorem, Theorem 4.3.15 implies that K exists.

Case III: d_1 is even, d_2 is even and $d_\infty = 1$. We cannot have $d_\infty = 0$ by condition (d). We define a contour $C = C(i, j)$, which we claim satisfies the conditions of Lemma 4.3.14, in the

following way.

$$\begin{aligned}
C(i-1, d_1-i) &= 0 && \text{for } 1 \leq i \leq d_1/2 - d_2, \\
C(d_1/2 - d_2 + i - 1, d_1/2 + d_2 - i) &= d_1 && \text{for } 1 \leq i \leq d_2, \\
C(d_1/2 + i, d_1/2 - i) &= 0 && \text{for } 1 \leq i \leq d_1/2 - 1, \\
C(0, 0) &= d_1 + d_2, \\
C(d_1/2 - d_2 + i - 1, d_1 + d_2 - i) &= 0 && \text{for } 1 \leq i \leq d_2/2, \\
C(d_1/2 - d_2/2, d_1 + d_2) &= 0, \\
C(d_1/2 - d_2/2 + i, d_1 + d_2/2 - i) &= 0 && \text{for } 1 \leq i \leq d_2/2, \\
C(d_1, 0) &= 0,
\end{aligned}$$

and if $d_1/d_2 \equiv 1 \pmod{2}$ then

$$\begin{aligned}
C(d_1 + i, d_1/2 + d_2/2 - i) &= 0 && \text{for } 1 \leq i \leq d_2/2 - 1, \\
C(d_1 + d_2/2 + i - 1, d_1/2 + d_2 - i) &= 0 && \text{for } 1 \leq i \leq d_2/2, \\
C(d_1 + d_2, d_1/2) &= 0,
\end{aligned}$$

otherwise

$$\begin{aligned}
C(d_1 + i, d_1/2 + d_2 - i) &= 0 && \text{for } 1 \leq i \leq d_2/2 - 1, \\
C(d_1 + d_2/2 + i - 1, d_1/2 + d_2/2 - i) &= 0 && \text{for } 1 \leq i \leq d_2/2, \\
C(d_1 + d_2, d_1/2 + d_2/2) &= 0.
\end{aligned}$$

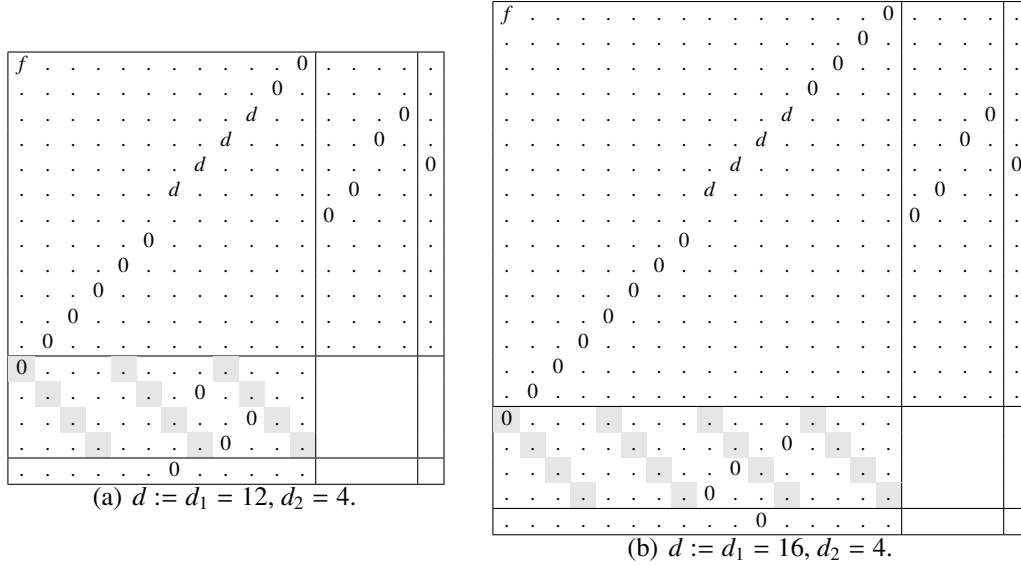
These contours are illustrated in Figure 4.7 for $(d_1, d_2) \in \{(12, 4), (16, 4)\}$. We let $f = d_1 + d_2$ and shade the cell orbit containing $(d_1, 0)$. Two cells (i, j) and (i', j') are on the same cell orbit of M_{21} if and only if $i - j \equiv i' - j' \pmod{d_2}$, since d_2 divides d_1 .

When d_1/d_2 is odd, d_2 does not divide $d_1/2$ and hence $d_1/2 \equiv d_2/2 \pmod{d_2}$. Therefore the set of values of $i - j \pmod{d_2}$ for the entries $(i, j, 0)$ in M_{21} is

$$\{0\} \cup \{2i : 1 \leq i \leq d_2/2 - 1\} \cup \{2i - 1 : 1 \leq i \leq d_2/2\} = \{0, 1, \dots, d_2 - 1\}. \quad (4.7)$$

When d_1/d_2 is even, we instead find $d_1/2 \equiv 0 \pmod{d_2}$ and the set of values of $i - j \pmod{d_2}$ for the entries $(i, j, 0)$ in M_{21} is also given by (4.7). In either case, each cell orbit of M_{21} contains a unique 0. Hence C satisfies the conditions of Lemma 4.3.14.

Case IV: addition of a fixed point. Suppose that we have a contour C for the parameters d_1, d_2, d_∞ with $d_\infty < d_2$. Let $n = d_1 + d_2 + d_\infty$. We will construct a contour for parameters $d_1, d_2, d_\infty + 1$ by adding a fixed point t in the following way. Pick a row i and column j of C in the block M_{11} such that $C(i, j) = 0$. Set $C(i, j) = t$. Set $C(i, n+1) = 0, C(n+1, i) = 0$. Since $d_\infty + 1 \leq d_2$ the subsquare K still can be completed by Theorem 4.3.15. Again C satisfies the conditions of Lemma 4.3.14. \square

FIGURE 4.7: Some more contours C .

4.3.5 Autotopisms of small Latin squares

Falcón [113] identified Ω_n for $n \leq 11$. We tabulate the isotopisms in Ω_{12} , Ω_{13} and Ω_{14} in Appendix A.4. Appealing to Lemma 4.3.3, we only list the cycle structures of autotopisms and write cycle structures in an abbreviated form. For example $4^2 \cdot 2^2 \cdot 1^2$ is an abbreviation for the cycle structure $(4, 4, 2, 2, 1, 1)$.

The first column of Figures A.7, A.8 and A.9 gives the cycle structure of α . If α, β and γ all have the same cycle structure (which we indicate by \sim), we give no additional information about β and γ . In other cases we list all possible cycle structures of β and γ in the second column. If $\beta \sim \gamma$, we only give the cycle structure of β and otherwise we list the cycles structures of β and γ as an ordered pair in parentheses.

Every isotopism $\theta \in \mathcal{I}_n$ for $n \leq 14$ can either be shown to have $\theta \notin \Omega_n$ using the information in this chapter, or has $\theta \in \Omega_n$. Chris Mears provided some assistance in finding Latin squares with a given autotopism.

CHAPTER 5

Future research

To review, in this thesis we have found several congruences satisfied by $R_{k,n}$ and have found links between $R_{k,n}$ and numbers of other combinatorial objects, such as orthomorphisms and partial orthomorphisms of \mathbb{Z}_n . Latin square autotopisms played a key role in finding congruences for $R_{k,n}$, which we also studied in detail.

The purpose of this concluding chapter is to list some open problems and future research ideas related to topics that arose within this thesis.

Divisors

The main motivation for this thesis was Figure 2.1 on page 39 which shows that $R_{k,n}$ tends to have many small divisors. We have made some progress towards finding theoretical reasons for these divisors, however the theory developed leaves some open questions. For example, Figures 2.4, 2.7, 2.9 and 3.2 and Appendices A.2 and A.3 all display a surprisingly large power of 2 divisor.

Question 5.0.19. *Why does such a large power of 2 divide $R_{k,n}$?*

The following two questions are motivated by Figure A.6 where we plot the largest integer a such that p^a divides $R_{k,n}$ for $k \in \{4, 5\}$ and $p \in \{2, 3\}$.

Question 5.0.20. *Is there a significant difference in the largest power of 2 dividing R_n and the largest power of p dividing R_n , for other primes p , as $n \rightarrow \infty$?*

Question 5.0.21. *How do the prime power divisors p^a of $R_{k,n}$ behave asymptotically for a fixed $k > p$ as $n \rightarrow \infty$ or as both $k \rightarrow \infty$ and $n \rightarrow \infty$?*

Also, Figure 1.6 motivates the following question.

Question 5.0.22. *Is the number of isomorphism classes of quasigroups of order n always odd?*

We were unable to resolve the following question in Section 2.4.

Question 5.0.23. *What is $R_{k,n} \pmod k$ for prime $k \geq 7$?*

We have modified the template in Section 2.1 to find (a) some divisors of the number of graph decompositions in Section 2.6, (b) divisors of some sets of Latin rectangles and Latin hypercuboids in Section 2.5 and (c) some congruences for the number of even and odd Latin squares in Section 2.7. Some of the results of Section 3.3 on compound orthomorphisms were, in some sense, obtained by using the template.

Question 5.0.24. *What other combinatorial numbers can we use this template to find divisors of?*

Judging from the data in Figure 1.14 on page 23, it appears the converse of Theorem 2.7.8 might also be true. Specifically, Figure 1.14 implies that $R_n^{\text{EVEN}} \not\equiv R_n^{\text{ODD}} \pmod n$ for $n \in \{2, 3, 5, 7\}$. Drisko [84] showed that $U_n^{\text{EVEN}} \not\equiv U_n^{\text{ODD}} \pmod n$ for all prime n .

Question 5.0.25. *Is it true that $R_n^{\text{EVEN}} \not\equiv R_n^{\text{ODD}} \pmod n$ if n is prime?*

Orthomorphisms

In Section 3.3.4 we make progress on the problem of partial orthomorphism completion. However, the question in general remains largely open.

Question 5.0.26. *Which partial orthomorphisms admit a completion? When is $\rho_{a,n} = 1$?*

The results presented in Section 3.3.4 consider when partial orthomorphisms complete to a d -compound orthomorphism of \mathbb{Z}_n . Cavenagh, Härmäläinen and Nelson [51] found conditions for the completion of a partial orthomorphism to a “quadratic orthomorphism.” This raises the following question.

Question 5.0.27. *What other classes of orthomorphism can we use to find conditions for the completion of a partial orthomorphisms of \mathbb{Z}_n ?*

The following was conjectured by Snevily [293]. It was shown true for odd n by Dasgupta, Karolyi, Serra and Szegedy [69].

Conjecture 5.0.28. *If $S, U \subseteq \mathbb{Z}_n$ with $|S| = |U| = a$, then there exists a partial orthomorphism $\nu : S \rightarrow U$ of \mathbb{Z}_n if and only if S and U are not both cosets of \mathbb{Z}_n of even order a .*

If L is a Latin square with $(\alpha, \alpha, \alpha) \in \text{Atop}(L)$ where $\alpha = (0, 1, \dots, n-1)$ and L' is a Latin square with $(\alpha, \alpha, \varepsilon) \in \text{Atop}(L')$, then L and L' must be orthogonal.

Question 5.0.29. *For which isotopisms θ and φ does the existence of two Latin squares L and L' , with $\theta \in \text{Atop}(L)$ and $\varphi \in \text{Atop}(L')$, imply that L and L' are orthogonal?*

Figure 2.10 gives a Steiner Latin square that is also a diagonally cyclic Latin square (DCLS).

Question 5.0.30. *What are the properties of the orthomorphisms that arise from Steiner Latin squares that are also DCLSs?*

Numbers

Doyle [81] gave a formula for the number of $k \times n$ Latin rectangles. There are 2^{k-1} variables in his formula that sum to n . However, many of the summands are 0, so we could simplify the sum considerably if we knew which ones.

Question 5.0.31. *Which of the summands in (1.16) are 0?*

Doyle halved the number of variables required by counting normalised Latin rectangles.

Question 5.0.32. *Can we modify Doyle's formula to instead count reduced Latin rectangles?*

Upon inspection of Doyle's formula, this appears to be a very difficult request.

Dougherty and Szczepanski [80] conjectured a generalisation of the Alon-Tarsi Conjecture (Conjecture 1.2.9 on page 21). We prove a special case of their conjecture in Corollary 2.5.12 on page 57. We also showed that $R_{4_s} \equiv 1 \pmod{3}$ for all $s \geq 1$. The first few values of the sequence $(R_{5_s} \pmod{3})_{s \geq 2}$ are $(2, 1, 1, 2, \dots)$, obtained from Figure 2.4.

Question 5.0.33. *Is $R_{5_s} \not\equiv 0 \pmod{3}$ for all $s \in \mathbb{N}$?*

Also observe that $(R_{5_s} \pmod{5})_{2 \leq s \leq 5} = (1, 1, 1, 1)$ as in Figure 2.4 on page 47.

Question 5.0.34. *Is $R_{p_s} \equiv 1 \pmod{p}$ for all primes p and $s \geq 1$?*

This relates to Corollary 2.4.4, which resolves the question in the affirmative when $s = 2$.

In Figure 1.3 we reproduce some estimates of R_n . For example, Kuznetsov [200] reports that the estimate for R_{12} was obtained in 159.3 seconds to an accuracy of 1%. It may be that the exact value of R_{12} is unknown for some time and that these estimates will be all we have to work with. Therefore it would be interesting to see these estimates improved in the future.

Notice that

- $R_{6_2}^{\text{EVEN}} = 5856$ and $R_{6_2}^{\text{ODD}} = 3552$ as given in Figure A.1 and
- $R_{6_3}^{\text{EVEN}} = 92793745368$ and $R_{6_3}^{\text{ODD}} = 3116150784$ as given in Section 2.5.1.

The increasing difference between these values leads to the following question.

Question 5.0.35. *Can we find estimates for $R_{\vec{n}_s}^{\text{EVEN}}$ and $R_{\vec{n}_s}^{\text{ODD}}$ to provide evidence to support Conjecture 2.5.3?*

Subsquares

In Section 4.2 we found a bound on the maximum number of $k \times k$ subsquares in a Latin square of order n .

Question 5.0.36. *Which Latin squares have the most subsquares?*

It seems reasonable to suspect that Cayley tables of elementary Abelian groups of order p^a have the most subsquares of order p^r , where p is a fixed prime, r is a fixed positive integer and $a \rightarrow \infty$. In fact, it is known [156] that of all Latin squares of order 2^a , the Cayley table of $(\mathbb{Z}_2)^a$ achieves the maximum number of 2×2 subsquares for all $a \geq 1$.

Question 5.0.37. *For which n, m, k does there exist a Latin square of order n containing exactly m subsquares of order k ?*

Latin squares without proper subsquares were studied by [91, 133, 214]. Wanless [320] identified some classes of Latin squares that have exactly one proper subsquare.

Ian Wanless (private communication) reported that for $n = 8$, there exists a Latin square of order n with exactly m subsquares of order k only in the following cases.

- $k = 2$ and $m \in \{0, 1, \dots, 52\} \cup \{56, 60, 64, 68, 72, 80, 88, 112\}$.
- $k = 3$ and $m \in \{0, 1, 2, 3, 4\}$.
- $k = 4$ and $m \in \{0, 4, 12, 28\}$.

Conjecture 5.0.38. *Let $m \geq 0$ and $k \geq 2$. For sufficiently large n , there exists a Latin square of order n with exactly m subsquares of order k .*

Autotopisms

In Section 4.1.1 we found an asymptotic divisor for R_n derived from bounding the maximum cardinality of the autotopism group of a Latin square of order n .

Question 5.0.39. *Which Latin squares have the largest autotopism group?*

It also seems reasonable to suspect that Cayley tables of groups have this property. In fact, Theorem 4.1.1 shows that the maximum for $n = 2^a$ is achieved by the Cayley table of $(\mathbb{Z}_2)^a$. However, this question was posed at the British Combinatorial Conference 2009, to which Bailey [43] promptly identified several classes of Latin squares of order n that have autotopism groups of order greater than any group table of order n .

Starting from Section 4.3 we extend the current knowledge of which $\theta \in \mathcal{I}_n$ have $\Delta(\theta) > 0$, where $\Delta(\theta)$ is the number of Latin squares of order n with $\theta \in \text{Atop}(L)$. We could ask a related question about reduced Latin squares. Let $\Delta_R(\theta)$ be the number of reduced Latin squares L of order n with $\theta \in \text{Atop}(L)$.

Question 5.0.40. *For which $\theta \in \mathcal{I}_n$ is $\Delta(\theta) > 0$? For which $\theta \in \mathcal{I}_n$ is $\Delta_R(\theta) > 0$?*

Question 5.0.41. *Can we find $\Delta(\theta)$ or $\Delta_R(\theta)$ exactly for some infinite classes of $\theta \in \mathcal{I}_n$?*

Question 5.0.42. *Can we find congruences satisfied by $\Delta(\theta)$?*

These questions also generalises to Latin rectangles and Latin hypercuboids. Progress on this topic has been made by Ahmad [1], Laywine [201], Bailey [13], Wanless [323], McKay, Meynert and Myrvold [222], Falcón Ganfornina [113, 126] (see also [114]) and Bryant, Buchanan and Wanless [41].

Question 5.0.43. *Let $o_n = \max\{\text{Ord}(\theta) : \theta \in \Omega_n\}$. We found that $o_n = n$ for $n \leq 26$ by a computer search. Does $o_n = n$ for $n \geq 27$?*

Suppose L is a Latin square with $\theta \in \text{Atop}(L)$. It would be interesting to find conditions for which $\varphi \in \Omega_n$ are also in $\text{Atop}(L)$.

Question 5.0.44. *For which pairs $\theta, \varphi \in \Omega_n$ does there exist a Latin square L such that both $\theta, \varphi \in \text{Atop}(L)$?*

McKay and Wanless [225] showed that the proportion of Latin squares with non-trivial autotopism group tends quickly to zero. This motivates the following conjecture.

Conjecture 5.0.45. *For $n > 0$ let $P(n)$ be the probability that a randomly chosen $\alpha \in S_n$ is a component of some isotopism $\theta = (\alpha, \beta, \gamma)$ with $\Delta(\theta) > 0$. Then $\lim_{n \rightarrow \infty} P(n) = 0$.*

Motivated by the results of Falcón [113], we have verified computationally that the following problem holds for all primes $p \leq 23$.

Question 5.0.46. *If $\theta = (\alpha, \beta, \gamma) \in \Omega_p$ for some prime $p \leq 23$, then either θ is equivalent to $(\delta, \delta, \varepsilon)$ where δ is a p -cycle, or α, β and γ all have the same cycle structure. Is this also true for primes $p \geq 29$?*

We have no particular reason to suspect that Question 5.0.46 is true for all primes, however, we have not yet found a counter-example.

\vec{d}	the dimensions of a Latin \vec{d} -hypercuboid
α	usually a permutation, sometimes used as the row permutation of an isotopism
$\vec{\alpha}_s$	$\vec{\alpha}_s$ is the isomorphism $(\alpha, \alpha, \dots, \alpha)$ of length s
$\text{Apar}(L)$	the autoparatopism group of L
$\text{Atop}(L)$	the autotopism group of L
$\text{Aut}(H)$	the automorphism group of the graph H
$\text{Aut}(L)$	the automorphism group of L
β	usually a permutation, often used as the column permutation of an isotopism
C	a set of Latin rectangles, $\mathcal{A} \subseteq C$ / a contour
ce	the property “is a column-even Latin square”
$\chi(n, d)$	the number of partial orthomorphisms $\nu : S \rightarrow \mathbb{Z}_n$ of \mathbb{Z}_n with deficit d such that $\nu(i) \notin \{0, i\}$ for all $i \in S$
$c_k(n)$	the number of decompositions of the complete graph on n vertices into k -cycles
co	the property “is a column-odd Latin square”
\mathcal{E}	a set of equations described in Section 3.2.2
$E = E(G)$	the edge set of a graph G
ε	the identity permutation
ϵ	$\epsilon(\alpha)$ is the sign of the permutation α , $\epsilon(L)$ is the sign of the Latin square L , etc.
EVEN	the property “is an even Latin hypercube” or “is an even Latin square”
F	used to denote a set fixed by some permutation
F^*	used to denote a set permuted by some permutation, the complement of F
G	a group / a graph
γ	often used as the symbol permutation of an isotopism
$G(L)$	the orbit of L under the action of a group G of isotopisms
$\text{gpd}(n)$	the greatest prime divisor of n
H	a group / a graph
(i, j, l_{ij})	an entry of a Latin rectangle $L = (l_{ij})$
\mathcal{I}_n	the group of all isotopisms, $\mathcal{I}_n = S_n \times S_n \times S_n$
$K_{k,n}$	the number of $k \times n$ normalised Latin rectangles / the complete bipartite graph
$k \times n$	usually the dimensions of Latin rectangles
K_n	the number of normalised Latin squares of order n / the complete graph on n vertices

L	a Latin square, Latin rectangle or Latin hypercuboid
λ_n	the number of canonical compatible orthomorphisms of \mathbb{Z}_n
Λ_n^s	the set of $(0, 1)$ -matrices with exactly s non-zero entries in each row and column
$L_{k,n}$	the number of $k \times n$ Latin rectangles
L_n	the number of Latin squares of order n
M	a matrix, often a subsquare or subrectangle of a Latin rectangle
m	sometimes $m = \lfloor n/2 \rfloor$
$[n]$	$\{1, 2, \dots, n\}$
\mathbb{N}	$\{1, 2, \dots\}$
\vec{n}_s	$\vec{n}_s = (n, n, \dots, n)$ of length s
ν	a partial orthomorphism
O	the orthogonal array of a Latin square, or Latin hypercuboid
ODD	the property “is an odd Latin hypercube” or “is an odd Latin square”
Ω_n	the set of isotopisms of order n that are autotopisms of some Latin square
$\omega(n, d)$	the number of partial orthomorphisms of \mathbb{Z}_n with deficit d
$\text{PER}(M)$	the permanent of a matrix M
π_n	the number of canonical polynomial orthomorphisms of \mathbb{Z}_n
RE	the property “is a row-even Latin square”
$\rho(\mathcal{E}, n)$	the number of solutions modulo n to a system of linear congruences defined by \mathcal{E}
$R_{k,n}$	the number of reduced $k \times n$ Latin rectangles
R_n	the number of reduced Latin squares of order n
RO	the property “is a row-odd Latin square”
$S_2(\cdot, \cdot)$	the Stirling number of the second kind
SE	the property “is a symbol-even Latin square”
σ	a permutation / an orthomorphism
SO	the property “is a symbol-odd Latin square”
θ	an isotopism $\theta \in \mathcal{I}_n$
$\vec{\theta}$	the isotopism $\vec{\theta} = (\theta_0, \theta_1, \dots, \theta_s)$
\vec{u}	an arbitrary cell of a Latin \vec{a} -hypercuboid
$V = V(H)$	the vertex set of a graph H
Ξ_n	the set of isomorphisms of order n that are autotopisms of some Latin square
\mathbb{Z}_n	the ring of integers modulo n
z_n	the number of canonical orthomorphisms of \mathbb{Z}_n

BIBLIOGRAPHY

- [1] S. AHMAD, *Cycle structure of automorphisms of finite cyclic groups*, J. Combin. Theory, 6 (1969), pp. 370–374.
- [2] A. A. ALBERT, *Quasigroups II*, Trans. Amer. Math. Soc., 55 (1944), pp. 401–419.
- [3] N. ALON, *On the number of subgraphs of prescribed type of graphs with a given number of edges*, Israel J. Math., 38 (1981), pp. 116–130.
- [4] N. ALON, J. SPENCER, AND P. TETALI, *Covering with Latin transversals*, Discrete Appl. Math., 57 (1995), pp. 1–10.
- [5] N. ALON AND M. TARSI, *Colorings and orientations of graphs*, Combinatorica, 12 (1992), pp. 125–134.
- [6] B. ALSPACH, *Research problem 3*, Discrete Math., 36 (1981), p. 333.
- [7] R. ALTER, *How many Latin squares are there?*, Amer. Math. Monthly, 82 (1975), pp. 632–634.
- [8] L. D. ANDERSEN AND A. J. W. HILTON, *Generalized Latin rectangles*, in Graph Theory and Combinatorics, vol. 34, Pitman, 1979, pp. 1–17.
- [9] —, *Generalized Latin rectangles. I. Construction and decomposition*, Discrete Math., 31 (1980), pp. 125–152.
- [10] —, *Generalized Latin rectangles. II. Embedding*, Discrete Math., 31 (1980), pp. 235–260.
- [11] V. L. ARLAZAROV, A. M. BARAEV, J. U. GOL’FAND, AND I. A. FARADŽEV, *Construction with the aid of a computer of all Latin squares of order 8*, Algorithmic Investigations in Combinatoric, (1978), pp. 129–141. In Russian.
- [12] K. B. ATHREYA, C. R. PRANESACHAR, AND N. M. SINGHI, *On the number of Latin rectangles and chromatic polynomial of $L(K_{r,s})$* , European J. Combin., 1 (1980), pp. 9–17.
- [13] R. A. BAILEY, *Latin squares with highly transitive automorphism groups*, J. Aust. Math. Soc., 33 (1982), pp. 18–22.
- [14] —, *Orthogonal partitions in designed experiments*, Des. Codes Cryptogr., 8 (1996), pp. 45–77.

- [15] R. A. BAILEY AND P. J. CAMERON, *Latin squares: Equivalents and equivalence*, (2003). Encyclopedia of Design Theory. <http://designtheory.org/library/encyc/latinsq/g/topics/lsee.pdf>.
- [16] S. E. BAMMEL AND J. ROTHSTEIN, *The number of 9×9 Latin squares*, Discrete Math., 11 (1975), pp. 93–95.
- [17] D. BEDFORD, *Construction of orthogonal Latin squares using left neofields*, Discrete Math., 115 (1993), pp. 17–38.
- [18] —, *Orthomorphisms and near orthomorphisms of groups and orthogonal Latin squares: A survey*, Bull. Inst. Combin. Appl., 15 (1995), pp. 13–33.
- [19] —, *Addendum to: “Orthomorphisms and near orthomorphisms of groups and orthogonal Latin squares: A survey”*, Bull. Inst. Combin. Appl., 18 (1996), p. 86.
- [20] G. B. BELJAVSKAJA AND S. MURATHUDJAEV, *About admissibility of n -ary quasigroups*, in Colloq. Math. Soc. János Bolyai, vol. I, North-Holland, 1978, pp. 101–119.
- [21] J. BELL AND B. STEVENS, *A survey of known results and research areas for n -queens*, Discrete Math., 309 (2009), pp. 1–31.
- [22] G. K. BENNETT, M. J. GRANNELL, AND T. S. GRIGGS, *Exponential lower bounds for the numbers of Skolem-type sequences*, Ars Combin., 73 (2004), pp. 101–106.
- [23] G. BIRKHOFF AND P. HALL, *On the order of groups of automorphisms*, Trans. Amer. Math. Soc., 39 (1936), pp. 496–499.
- [24] K. P. BOGART AND J. Q. LONGYEAR, *Counting 3 by n Latin rectangles*, Proc. Amer. Math. Soc., 54 (1976), pp. 463–467.
- [25] G. BOL, *Gewebe und Gruppen*, Math. Ann., 114 (1937), pp. 414–431.
- [26] J. BOSÁK, *Latinské štvorce*, Mladá Fronta, 1976.
- [27] R. C. BOSE AND B. MANVEL, *Introduction to Combinatorial Theory*, Wiley, 1984.
- [28] W. BOSMA, *Cubic reciprocity and explicit primality tests for $h \cdot 3^k \pm 1$* , in High Primes and Misdemeanours, 2004, pp. 77–89.
- [29] L. J. BRANT AND G. L. MULLEN, *A note on isomorphism classes of reduced Latin squares of order 7*, Util. Math., 27 (1985), pp. 261–263.
- [30] —, *Some results on enumeration and isotopic classification of frequency squares*, Util. Math., 29 (1986), pp. 231–244.
- [31] L. M. BRÈGMAN, *Certain properties of nonnegative matrices and their permanents*, Soviet Math. Dokl., 14 (1973), pp. 945–949.
- [32] R. BRIER AND D. BRYANT, *Perpendicular rectangular Latin arrays*, Graphs Combin., 25 (2009), pp. 15–25.
- [33] J. W. BROWN, *Enumeration of Latin Squares and Isomorphism Detection in Finite Planes*, PhD thesis, University of Los Angeles, 1966.
- [34] —, *Enumeration of Latin squares with application to order 8*, J. Combin. Theory, 5 (1968), pp. 177–184.
- [35] J. BROWNING, P. VOJTĚCHOVSKÝ, AND I. M. WANLESS, *Overlapping Latin subsquares and full products*. Submitted.

- [36] R. A. BRUALDI AND H. J. RYSER, *Combinatorial Matrix Theory*, Cambridge University Press, 1991.
- [37] R. H. BRUCK, *Finite nets. I. Numerical invariants*, Canadian J. Math., 3 (1951), pp. 94–107.
- [38] —, *Finite nets. II. Uniqueness and imbedding*, Pacific J. Math., 13 (1963), pp. 421–457.
- [39] B. F. BRYANT AND H. SCHNEIDER, *Principal loop-isotopes of quasigroups*, Canad. J. Math., 18 (1966), pp. 120–125.
- [40] D. BRYANT, *Cycle decompositions of complete graphs*, in *Surveys in Combinatorics*, vol. 346, Cambridge University Press, 2007, pp. 67–97.
- [41] D. BRYANT, M. BUCHANAN, AND I. M. WANLESS, *The spectrum for quasigroups with cyclic automorphisms and additional symmetries*, Discrete Math., 304 (2009), pp. 821–833.
- [42] A. T. BUTSON AND B. M. STEWART, *Systems of linear congruences*, Canad. J. Math., 7 (1955), pp. 358–368.
- [43] P. J. CAMERON, *Problems from BCC22*, Discrete Math. To appear.
- [44] —, *Permutation Groups*, Cambridge University Press, 1999.
- [45] H. CAO, J. DINITZ, D. KREHER, D. STINSON, AND R. WEI, *On orthogonal generalized equitable rectangles*, Des. Codes Cryptogr., 51 (2009), pp. 225–230.
- [46] L. CARLITZ, *Congruences connected with three-line Latin rectangles*, Proc. Amer. Math. Soc., 4 (1953), pp. 9–11.
- [47] N. J. CAVENAGH, *Avoidable partial Latin squares of order $4m + 1$* , Ars Combin. To appear.
- [48] —, *The theory and application of Latin bitrades: A survey*, Math. Slovaca, 58 (2008), pp. 691–718.
- [49] N. J. CAVENAGH, C. GREENHILL, AND I. M. WANLESS, *The cycle structure of two rows in a random Latin square*, Random Structures Algorithms, 33, pp. 286–309.
- [50] N. J. CAVENAGH, C. HÄMÄLÄINEN, J. G. LEFEVRE, AND D. S. STONES, *Multi-Latin squares*. Submitted.
- [51] N. J. CAVENAGH, C. HÄMÄLÄINEN, AND A. M. NELSON, *On completing three cyclically generated transversals to a Latin square*, Finite Fields Appl., 15 (2009), pp. 294–303.
- [52] N. J. CAVENAGH AND L.-D. ÖHMAN, *Partial Latin squares are avoidable*. Submitted.
- [53] N. J. CAVENAGH AND I. M. WANLESS, *On the number of transversals in Cayley tables of cyclic groups*, Discrete Appl. Math. To appear.
- [54] A. CAYLEY, *On Latin squares*, Messenger of Math., 19 (1890), pp. 135–137. See [55], vol. 13, no. 903, pp. 55–57.
- [55] —, *The Collected Mathematical Papers of Arthur Cayley*, Cambridge University Press, 1897.
- [56] A. G. CHETWYND AND S. J. RHODES, *Avoiding partial Latin squares and intricacy*, Discrete Math., 177 (1997), pp. 17–32.
- [57] T. Y. CHOW, *On the Dinitz Conjecture and related conjectures*, Discrete Math., 145 (1995), pp. 73–82.

- [58] B. CIPRA, *If you're stumped, try something harder*, Science, 259 (1993), p. 1404.
- [59] D. CLARK AND J. T. LEWIS, *Transversals of cyclic Latin squares*, Congr. Numer., 128 (1997), pp. 113–120.
- [60] C. J. COLBOURN, *The complexity of completing partial Latin squares*, Discrete Appl. Math., 8 (1984), pp. 25–30.
- [61] C. J. COLBOURN, J. H. DINITZ, ET AL., *The CRC Handbook of Combinatorial Designs*, CRC Press, 1996.
- [62] C. J. COLBOURN AND A. ROSA, *Triple systems*, Oxford University Press, 1999.
- [63] F. N. COLE, L. D. CUMMINGS, AND H. S. WHITE, *The complete enumeration of triad systems in 15 elements*, Proc. Natl. Acad. Sci. USA, 3 (1917), pp. 197–199.
- [64] L. COMTET, *Advanced Combinatorics: The Art of Finite and Infinite Expansions*, Reidel, 1974.
- [65] C. COOPER, *A lower bound for the number of good permutations*, Data Recording, Storage and Processing, Nat. Acad. Sci. Ukraine, 2.3 (2000), pp. 15–25.
- [66] C. COOPER, R. GILCHRIST, I. N. KOVALENKO, AND D. NOVAKOVIC, *Estimation of the number of “good” permutations, with applications to cryptography*, Cybernet. Systems Anal., 35 (2000), pp. 688–693.
- [67] C. COOPER AND I. N. KOVALENKO, *An upper bound on the number of complete mappings*, Theory Probab. Math. Statist., 53 (1995), pp. 77–83.
- [68] J. CUTLER AND L.-D. ÖHMAN, *Latin squares with forbidden entries*, Electron. J. Combin., 13 (2006). R47, 9 pp.
- [69] S. DASGUPTA, G. KÁROLYI, O. SERRA, AND B. SZEGEDY, *Transversals of additive Latin squares*, Israel J. Math., 126 (2001), pp. 17–28.
- [70] A. DE GENNARO, *How many Latin rectangles are there?*, (2007). arXiv:0711.0527v1 [math.CO], 20 pp.
- [71] J. DENÉS AND A. D. KEEDWELL, *Latin Squares and their Applications*, Academic Press, 1974.
- [72] —, *Latin squares and 1-factorizations of complete graphs. I. Connections between the enumeration of Latin squares and rectangles and r -factorizations of labelled graphs*, Ars Combin., 25 (1988), pp. 109–126.
- [73] —, *Latin squares and one-factorizations of complete graphs. II. Enumerating one-factorizations of the complete directed graph K_n^* using MacMahon’s double partition idea*, Util. Math., 34 (1988), pp. 73–83.
- [74] —, *Latin Squares: New Developments in the Theory and Applications*, North-Holland, 1991.
- [75] J. DENÉS AND G. L. MULLEN, *Enumeration formulas for Latin and frequency squares*, Discrete Math., 111 (1993), pp. 157–163.
- [76] C. L. DENG AND C. K. LIM, *A result on generalized Latin rectangles*, Discrete Math., 72 (1988), pp. 71–80.
- [77] L. E. DICKSON AND F. H. SAFFORD, *Solutions of problems: Group theory: 8*, Amer. Math. Monthly, 13 (1906), pp. 150–151.

- [78] J. H. DINITZ, D. K. GARNICK, AND B. D. MCKAY, *There are 526, 915, 620 nonisomorphic one-factorizations of K_{12}* , J. Combin. Des., 2 (1994), pp. 273–285.
- [79] J. H. DINITZ AND D. R. STINSON, *Contemporary Design Theory: A Collection of Surveys*, Wiley, 1992.
- [80] S. T. DOUGHERTY AND T. A. SZCZEPANSKI, *Latin k -hypercubes*, Australas. J. Combin., 40 (2008), pp. 145–160.
- [81] P. G. DOYLE, *The number of Latin rectangles*, (2007). arXiv:math/0703896v1 [math.CO], 15 pp.
- [82] A. A. DRISKO, *Loops, Latin Squares and the Alon-Tarsi Conjecture*, PhD thesis, University of California, 1995.
- [83] —, *On the number of even and odd Latin squares of order $p + 1$* , Adv. Math., 128 (1997), pp. 20–35.
- [84] —, *Proof of the Alon-Tarsi Conjecture for $n = 2^r p$* , Electron. J. Combin., 5 (1998). R28, 5 pp.
- [85] —, *Transversals in row-Latin rectangles*, J. Combin. Theory Ser. A, 84 (1998), pp. 181–195.
- [86] L. DUAN, *An upper bound for the number of normalized Latin square*, Chinese Quart. J. Math., 21 (2006), pp. 585–589.
- [87] H. E. DUDENEY, *Amusements in Mathematics*, Nelson, 1917.
- [88] A. L. DULMAGE, *E650*, Amer. Math. Monthly, 52 (1945), p. 458.
- [89] A. L. DULMAGE AND G. E. McMASTER, *A formula for counting three-line Latin rectangles*, Congr. Numer., 14 (1975), pp. 279–289.
- [90] G. P. EGORICHEV, *The solution of the van der Waerden problem for permanents*, Adv. Math., 42 (1981), pp. 299–305.
- [91] J. R. ELLIOTT AND P. B. GIBBONS, *The construction of subsquare free Latin squares by simulated annealing*, Australas. J. Combin., 5 (1992), pp. 209–228.
- [92] P. ERDŐS, D. R. HICKERSON, D. A. NORTON, AND S. K. STEIN, *Has every Latin square of order n a partial Latin transversal of size $n - 1$?*, Amer. Math. Monthly, 95 (1988), pp. 428–430.
- [93] P. ERDŐS AND I. KAPLANSKY, *The asymptotic number of Latin rectangles*, Amer. J. Math., 68 (1946), pp. 230–236.
- [94] P. ERDŐS, A. L. RUBIN, AND H. TAYLOR, *Choosability in graphs*, Congr. Numer., 26 (1980), pp. 125–157.
- [95] P. ERDŐS AND J. SPENCER, *Lopsided Lovász Local Lemma and Latin transversals*, Discrete Appl. Math., 30 (1991), pp. 151–154.
- [96] M. J. ERICKSON, *Introduction to Combinatorics*, Wiley, 1996.
- [97] L. EULER, *Recherches sur une nouvelle espèce de quarrés magiques*, Verh. Zeeuwsch. Gennot. Weten. Vliiss., 9 (1782), pp. 85–239. Eneström E530, Opera Omnia OI7, pp. 291–392.

- [98] —, *Solutio quaestionis curiosae ex doctrina combinationum*, Mémoires de l'Académie des Sciences de St. Pétersbourg, 3 (1811), pp. 57–64. E738, OI7, pp. 435–440.
- [99] —, *De quadratis magicis*, Commentationes Arithmeticae, 2 (1849), pp. 593–602. E795, OI7, pp. 441–457.
- [100] A. B. EVANS, *Orthomorphism graphs of $GF(q)^+ \times GF(3)^+$* . Preprint.
- [101] —, *Generating orthomorphisms of $GF(q)^+$* , Discrete Math., 63 (1987), pp. 21–26.
- [102] —, *Orthomorphisms of \mathbb{Z}_p* , Discrete Math., 64 (1987), pp. 147–156.
- [103] —, *Orthomorphism graphs of \mathbb{Z}_p* , Ars Combin., 25 (1988), pp. 141–152.
- [104] —, *Orthomorphism graphs of groups*, J. Geom., 35 (1989), pp. 66–74.
- [105] —, *Orthomorphisms of $GF(q)^+$* , Ars Combin., 27 (1989), pp. 121–131.
- [106] —, *Orthomorphisms of groups*, Ann. New York Acad. Sci., 555 (1989), pp. 187–191.
- [107] —, *Maximal sets of mutually orthogonal Latin squares. I*, European J. Combin., 12 (1991), pp. 477–482.
- [108] —, *Maximal sets of mutually orthogonal Latin squares. II*, European J. Combin., 13 (1992), pp. 345–350.
- [109] —, *Orthomorphism Graphs of Groups*, Springer, 1992.
- [110] —, *Cyclotomy and orthomorphisms: A survey*, Congr. Numer., 101 (1994), pp. 97–107.
- [111] —, *On orthogonal orthomorphisms of cyclic and non-Abelian groups*, Discrete Math., 243 (2002), pp. 229–233.
- [112] —, *On orthogonal orthomorphisms of cyclic and non-Abelian groups. II*, J. Combin. Des., 15 (2007), pp. 195–209.
- [113] R. M. FALCÓN, *Cycle structures of autotopisms of the Latin squares of order up to 11*, Ars Combin., (2009). To appear.
- [114] R. M. FALCÓN AND J. MARTÍN-MORALES, *Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7* , J. Symbolic Comput., 42 (2007), pp. 1142–1154.
- [115] D. I. FALIKMAN, *A proof of van der Waerden's conjecture on the permanent of a doubly stochastic matrix*, Math. Notes, 29 (1981), pp. 475–479.
- [116] C. FAN, A. GUPTA, AND J. LIU, *Latin cubes and parallel array access*, in Parallel Processing Symposium, 1994, pp. 128–132.
- [117] W. T. FEDERER, *Statistics and Society*, CRC Press, 1991.
- [118] D. J. FINNEY, *Some enumerations for the 6×6 Latin squares*, Util. Math., 21 (1982), pp. 137–153.
- [119] R. A. FISHER AND F. YATES, *The 6×6 Latin squares*, Proc. Cambridge Philos. Soc., 30 (1934), pp. 492–507.
- [120] M. F. FRANKLIN, *Cyclic generation of orthogonal Latin squares*, Ars Combin., 17 (1984), pp. 129–139.

- [121] —, *Cyclic generation of self-orthogonal Latin squares*, Util. Math., 25 (1984), pp. 135–146.
- [122] M. FROLOV, *Sur les permutations carrés*, J. de Math. spéc., 4 (1890), pp. 8–11 and 25–30.
- [123] H.-L. FU, *On Latin $(n \times n \times (n - 2))$ -parallelepipeds*, Tamkang J. Math., 17 (1986), pp. 107–111.
- [124] Z.-L. FU, *The number of Latin rectangles*, Math. Practice Theory, (1992), pp. 40–41. In Chinese.
- [125] F. GALVIN, *The list chromatic index of a bipartite multigraph*, J. Combin. Theory Ser. B, 63 (1995), pp. 153–158.
- [126] R. M. F. GANFORNINA, *Latin squares associated to principal autotopisms of long cycles. Application in cryptography*, in Proceedings of Transgressive Computing, 2006, pp. 213–230.
- [127] THE GAP GROUP, *GAP – Groups, algorithms, programming – A system for computational discrete algebra*. <http://www.gap-system.org/>.
- [128] P. GARCIA, *Major Percy Alexander MacMahon*, PhD thesis, Open University, 2006.
- [129] E. N. GELLING AND R. E. ODEH, *On 1-factorizations of the complete graph and the relationship to round robin schedules*, Util. Math., (1974), pp. 213–221.
- [130] I. M. GESSEL, *Counting three-line Latin rectangles*, in Proceedings of the Colloque de Combinatoire Énumérative, Springer, 1986.
- [131] —, *Counting Latin rectangles*, Bull. Amer. Math. Soc., 16 (1987), pp. 79–83.
- [132] S. G. GHURYE, *A characteristic of species of 7×7 Latin squares*, Ann. Eugenics, 14 (1948), p. 133.
- [133] P. B. GIBBONS AND E. MENDELSON, *The existence of a subsquare free Latin square of side 12*, SIAM J. Algebraic Discrete Methods, 8 (1987), pp. 93–99.
- [134] D. G. GLYNN, *On Rota's Basis Conjecture and Latin squares*. Submitted.
- [135] C. D. GODSIL AND B. D. MCKAY, *Asymptotic enumeration of Latin rectangles*, Bull. Amer. Math. Soc. (N.S.), 10 (1984), pp. 91–92.
- [136] —, *Asymptotic enumeration of Latin rectangles*, J. Combin. Theory Ser. B, 48 (1990), pp. 19–44.
- [137] I. P. GOULDEN AND D. M. JACKSON, *Combinatorial Enumeration*, Wiley, 1983.
- [138] T. GRANLUND ET AL., *GNU multiple precision arithmetic library*. <http://gmplib.org/>.
- [139] T. A. GREEN, *Asymptotic Enumeration of Latin Rectangles and Associated Waiting Times*, PhD thesis, Stanford University, 1984.
- [140] —, *Asymptotic enumeration of generalized Latin rectangles*, J. Combin. Theory Ser. A, 51 (1989), pp. 149–160.
- [141] —, *Erratum: "Asymptotic enumeration of generalized Latin rectangles"*, J. Combin. Theory Ser. A, 52 (1989), p. 322.
- [142] M. GRÜTTMÜLLER, *Completing partial Latin squares with two cyclically generated prescribed diagonals*, J. Combin. Theory Ser. A, 103 (2003), pp. 349–362.

- [143] —, *Completing partial Latin squares with prescribed diagonals*, Discrete Appl. Math., 138 (2004), pp. 89–97.
- [144] H. GUPTA, *On permutation cubes and Latin cubes*, Indian J. Pure Appl. Math., 5 (1974), pp. 1003–1021.
- [145] L. HABSIEGER AND J. C. M. JANSSEN, *The difference in even and odd Latin rectangles for small cases*, Ann. Sci. Math. Québec, 19 (1995), pp. 69–77.
- [146] R. HÄGGKVIST, *A note on Latin squares with restricted support*, Discrete Math., 75 (1989), pp. 253–254.
- [147] —, *Towards a solution of the Dinitz problem?*, Discrete Math., 75 (1989), pp. 247–251.
- [148] M. HALL, JR, *An existence theorem for Latin squares*, Bull. Amer. Math. Soc., 51 (1945), pp. 387–388.
- [149] —, *Distinct representatives of subsets*, Bull. Amer. Math. Soc., 54 (1948), pp. 922–926.
- [150] M. HALL, JR AND J. D. SWIFT, *Determination of Steiner triple systems of order 15*, Math. Tables Aids Comput., 9 (1955), pp. 146–152.
- [151] P. HALL, *On representatives of subsets*, J. London Math. Soc., 10 (1935), pp. 26–30.
- [152] J. R. HAMILTON AND G. L. MULLEN, *How many $i - j$ reduced Latin rectangles are there?*, Amer. Math. Monthly, 87 (1980), pp. 392–394.
- [153] K. HARE, *Perfect $\langle k, r \rangle$ -Latin squares*, Ars Combin., 63 (2002), pp. 311–318.
- [154] A. HEDAYAT AND E. SEIDEN, *F-square and orthogonal F-squares design: A generalization of Latin square and orthogonal Latin squares design.*, Ann. Math. Statist., 41 (1970), pp. 2035–2044.
- [155] K. HEINRICH, *Prolongation in m-dimensional permutation cubes*, in Algebraic and Geometric Combinatorics, vol. 65, North-Holland, 1982, pp. 229–238.
- [156] K. HEINRICH AND W. D. WALLIS, *The maximum number of intercalates in a Latin square*, in Lecture Notes in Math., vol. 884, Springer, 1981, pp. 221–233.
- [157] A. HEINZE AND M. KLIN, *Links between Latin squares, nets, graphs and groups: Work inspired by a paper of A. Barlotti and K. Strambach*, Electron. Notes Discrete Math., 23 (2005), pp. 13–21.
- [158] A. J. W. HILTON, *School timetables*, Ann. Discrete Math., 11 (1981), pp. 177–188.
- [159] P. HORÁK, *Latin parallelepipeds and cubes*, J. Combin. Theory Ser. A, 33 (1982), pp. 213–214.
- [160] J. HSIANG, D. F. HSU, AND Y.-P. SHIEH, *On the hardness of counting problems of complete mappings*, Discrete Math., 277 (2004).
- [161] J. HSIANG, Y.-P. SHIEH, AND Y.-C. CHEN, *The cyclic complete mappings counting problems*, in Problems and Problem Sets for ATP Workshop, 2002.
- [162] D. F. HSU, *Cyclic Neofields and Combinatorial Designs*, Springer, 1980.
- [163] R. HUANG AND G.-C. ROTA, *On the relations of various conjectures on Latin squares and straightening coefficients*, Discrete Math., 128 (1994), pp. 225–236.

- [164] A. HULPKE, P. KASKI, AND P. R. J. ÖSTERGÅRD, *The number of Latin squares of order 11*, arXiv:0909.3402v1 [math.CO].
- [165] E. C. IHRIG AND B. M. IHRIG, *The recognition of symmetric Latin squares*, J. Combin. Des., 16 (2008), pp. 291–300.
- [166] A. IRANMANESH AND A. R. ASHRAFI, *Generalized Latin square*, J. Appl. Math. Comput., 22 (2006), pp. 285–293.
- [167] T. ITO, *Method, equipment, program and storage media for producing tables*, Japanese Patent Office, JP2004-272104A (2004). In Japanese.
- [168] S. M. JACOB, *The enumeration of the Latin rectangle of depth three by means of a formula of reduction, with other theorems relating to non-clashing substitutions and Latin squares*, Proc. London Math. Soc. (2), 31 (1930), pp. 329–354.
- [169] M. JACOBSON AND P. MATTHEWS, *Generating uniformly distributed Latin squares*, J. Combin. Des., 4 (1996), pp. 405–437.
- [170] J. C. M. JANSSEN, *The Dinitz problem solved for rectangles*, Bull. Amer. Math. Soc. (N.S.), 29 (1993), pp. 243–249.
- [171] —, *On even and odd Latin squares*, J. Combin. Theory Ser. A, 69 (1995), pp. 173–181.
- [172] X.-W. JIA AND Z.-P. QIN, *The number of Latin cubes and its isotopy*, J. Huazhong Univ. of Sci. Tech., 27 (1999), pp. 104–106. In Chinese.
- [173] D. M. JOHNSON, A. L. DULMAGE, AND N. S. MENDELSON, *Orthomorphisms of groups and orthogonal Latin squares I*, Canad. J. Math., 13 (1961), pp. 356–372.
- [174] A.-A. A. JUCYS, *The number of distinct Latin squares as a group-theoretical constant*, J. Combin. Theory Ser. A, 20 (1976), pp. 265–272.
- [175] D. JUNGnickel, *Latin squares, their geometries and their groups. A survey*, IMA Vol. Math. Appl., 21 (1990), pp. 166–225.
- [176] W. B. JURKAT AND H. J. RYSER, *Matrix factorizations of determinants and permanents*, J. Algebra, 3 (1966), pp. 1–27.
- [177] P. KASKI AND P. R. J. ÖSTERGÅRD, *The Steiner triple systems of order 19*, Math. Comp., 73 (2004), pp. 2075–2092.
- [178] —, *There are 1, 132, 835, 421, 602, 062, 347 nonisomorphic one-factorizations of K_{14}* , J. Combin. Des., 17 (2008), pp. 147–159.
- [179] A. D. KEEDWELL, *On orthogonal Latin squares and a class of neofields*, Rend. Mat. Appl., 5 (1966), pp. 519–561.
- [180] —, *On property D neofields and some problems concerning orthogonal Latin squares*, in Computational Problems in Abstract Algebra, Pergamon Press, 1970, pp. 315–319.
- [181] —, *Construction, properties and applications of finite neofields*, Comment. Math. Univ. Carolin., (2000), pp. 283–297.
- [182] M. G. KENDALL, *Who discovered the Latin square?*, Amer. Statist., 2 (1948), p. 13.
- [183] S. M. KERAWALA, *The enumeration of the Latin rectangle of depth three by means of a difference equation*, Bull. Calcutta Math. Soc., 33 (1941), pp. 119–127.

- [184] —, *The asymptotic number of three-deep Latin rectangles*, Bull. Calcutta Math. Soc., 39 (1947), pp. 71–72.
- [185] B. KERBY AND J. D. H. SMITH, *Latin square automorphisms and symmetric group characters*. In preparation.
- [186] D. KLYVE AND L. STEMKOSKI, *The Euler archive*. <http://www.math.dartmouth.edu/~euler/>.
- [187] —, *Graeco-Latin squares and a mistaken conjecture of Euler*, Cambridge Mathematical Journal, 37 (2006), pp. 2–15.
- [188] M. KOCHOL, *Latin $(n \times n \times (n - 2))$ -parallelepipeds not completing to a Latin cube*, Math. Slovaca, 39 (1989), pp. 121–125.
- [189] —, *Latin parallelepipeds not completing to a cube*, Math. Slovaca, 41 (1991), pp. 3–9.
- [190] —, *Relatively narrow Latin parallelepipeds that cannot be extended to a Latin cube*, Ars Combin., 40 (1995), pp. 247–260.
- [191] G. KOLESOVA, C. W. H. LAM, AND L. THIEL, *On the number of 8×8 Latin squares*, J. Combin. Theory Ser. A, 54 (1990), pp. 143–148.
- [192] I. N. KOVALENKO, *Upper bound on the number of complete mappings*, Cybernet. Systems Anal., 32 (1996), pp. 65–68.
- [193] D. S. KROTOV, *On reducibility of n -ary quasigroups*, Discrete Math., 308 (2008), pp. 5289–5297.
- [194] D. S. KROTOV AND V. N. POTAPOV, *n -ary quasigroups of order 4*, SIAM J. Discrete Math., 23 (2009), pp. 561–570.
- [195] —, *On reducibility of n -ary quasigroups, II*, (2009). arXiv:0801.0055v1 [math.CO].
- [196] D. S. KROTOV, V. N. POTAPOV, AND P. V. SOKOLOVA, *On reconstructing reducible n -ary quasigroups and switching subquasigroups*, Quasigroups Related Systems, 16 (2008), pp. 55–67.
- [197] V. KRČADINAC, *Frequency squares of orders 7 and 8*, Util. Math., 72 (2007), pp. 89–95.
- [198] N. Y. KUZNETSOV, *Applying fast simulation to find the number of good permutations*, Cybernet. Systems Anal., 43 (2007), pp. 830–837.
- [199] —, *Estimating the number of good permutations by a modified fast simulation method*, Cybernet. Systems Anal., 44 (2008), pp. 547–554.
- [200] —, *Estimating the number of Latin rectangles by the fast simulation method*, Cybernet. Systems Anal., 45 (2009), pp. 69–75.
- [201] C. LAYWINE, *An expression for the number of equivalence classes of Latin squares under row and column permutations*, J. Combin. Theory Ser. A, 30 (1981), pp. 317–320.
- [202] C. LAYWINE AND G. L. MULLEN, *Latin cubes and hypercubes of prime order*, Fibonacci Quart., 23 (1985), pp. 139–145.
- [203] —, *Discrete Mathematics using Latin Squares*, Wiley, 1998.

- [204] A. A. LEVITSKAYA, *A combinatorial problem in the class of permutations over the residue ring Z_n modulo odd n* , Problemy Upravlen. Inform., (1996), pp. 99–108. In Russian.
- [205] H. LIANG AND F. BAI, *An upper bound for the permanent of $(0, 1)$ -matrices*, Linear Algebra Appl., 377 (2004), pp. 291–295.
- [206] F. W. LIGHT, JR, *A procedure for the enumeration of $4 \times n$ Latin rectangles*, Fibonacci Quart., 11 (1973), pp. 241–246.
- [207] ———, *Enumeration of truncated Latin rectangles*, Fibonacci Quart., 17 (1979), pp. 34–36.
- [208] C. C. LINDNER, E. MENDELSON, AND A. ROSA, *On the number of 1-factorizations of the complete graph*, J. Combin. Theory Ser. B, 20 (1976), pp. 265–282.
- [209] P. A. MACMAHON, *A new method in combinatory analysis, with applications to Latin squares and associated questions*, Trans. Camb. Phil. Soc., 16 (1898), pp. 262–290.
- [210] ———, *Combinatorial analysis. the foundations of a new theory*, Philos. Trans. Roy. Soc. London Ser. A, 194 (1900), pp. 361–386.
- [211] ———, *Combinatory Analysis*, Chelsea, 1960.
- [212] ———, *Percy Alexander MacMahon : collected papers / edited by George E. Andrews*, MIT Press, 1986.
- [213] H. F. MACNEISH, *Euler squares*, Ann. of Math. (2), 23 (1922), pp. 221–227.
- [214] B. MAENHAUT, I. M. WANLESS, AND B. S. WEBB, *Subsquare-free Latin squares of odd order*, European J. Combin., 28 (2007), pp. 322–336.
- [215] H. B. MANN, *The construction of orthogonal Latin squares*, Ann. Math. Stat., 13 (1942), pp. 418–423.
- [216] M. MARCUS, *Henryk Minc – a biography*, Linear Multilinear Algebra, 51 (2003), pp. 1–10.
- [217] A. MARINI AND G. PIRILLO, *Signs on Latin squares*, Adv. in Appl. Math., 15 (1994), pp. 490–505.
- [218] ———, *Signs on group Latin squares*, Adv. in Appl. Math., 17 (1996), pp. 117–121.
- [219] K. MARKSTRÖM AND L.-D. ÖHMAN, *Unavoidable arrays*. Submitted.
- [220] B. D. MCKAY, *nauty – Graph isomorphic software*. <http://cs.anu.edu.au/~bdm/nauty/>.
- [221] B. D. MCKAY, J. C. MCLEOD, AND I. M. WANLESS, *The number of transversals in a Latin square*, Des. Codes Cryptogr., 40 (2006), pp. 269–284.
- [222] B. D. MCKAY, A. MEYNERT, AND W. MYRVOLD, *Small Latin squares, quasigroups and loops*, J. Combin. Des., 15 (2007), pp. 98–119.
- [223] B. D. MCKAY AND E. ROGOYSKI, *Latin squares of order ten*, Electron. J. Combin., 2 (1995). N3, 4 pp.
- [224] B. D. MCKAY AND I. M. WANLESS, *Most Latin squares have many subsquares*, J. Combin. Theory Ser. A, 86 (1999), pp. 323–347.
- [225] ———, *On the number of Latin squares*, Ann. Comb., 9 (2005), pp. 335–344.

- [226] ———, *A census of small Latin hypercubes*, SIAM J. Discrete Math., 22 (2008), pp. 719–736.
- [227] B. D. MCKAY AND N. C. WORMALD, *Uniform generation of random Latin rectangles*, J. Combin. Math. Combin. Comput., 9 (1991), pp. 179–186.
- [228] E. MENDELSON AND A. ROSA, *One-factorizations of the complete graph – a survey*, J. Graph Theory, 9 (1985), pp. 43–65.
- [229] K. MÉSZÁROS, *Generalized Latin squares and their defining sets*, Discrete Math., 308 (2008), pp. 2366–2378.
- [230] H. MINC, *Upper bounds for permanents of $(0, 1)$ -matrices*, Bull. Amer. Math. Soc., 69 (1963), pp. 789–791.
- [231] ———, *An inequality for permanents of $(0, 1)$ -matrices*, J. Combinatorial Theory, 2 (1967), pp. 321–326.
- [232] ———, *On lower bounds for permanents of $(0, 1)$ matrices*, Proc. Amer. Math. Soc., 22 (1969), pp. 117–123.
- [233] ———, *Permanents*, Addison-Wesley, 1978.
- [234] ———, *Theory of permanents, 1978–1981*, Linear Multilinear Algebra, 12 (1982/83), pp. 227–263.
- [235] ———, *Theory of permanents, 1982–1985*, Linear Multilinear Algebra, 21 (1987), pp. 109–148.
- [236] W. O. J. MOSER, *The number of very reduced $4 \times n$ Latin rectangles*, Canad. J. Math., 19 (1967), pp. 1011–1017.
- [237] ———, *A generalization of Riordan’s formula for $3 \times n$ Latin rectangles*, Discrete Math., 40 (1982), pp. 311–313.
- [238] R. MOUFANG, *Zur Struktur von Alternativkörpern*, Math. Ann., 110 (1935), pp. 416–430.
- [239] G. L. MULLEN, *How many $i-j$ reduced Latin squares are there?*, Amer. Math. Monthly, 82 (1978), pp. 751–752.
- [240] G. L. MULLEN AND D. PURDY, *Some data concerning the number of Latin rectangles*, J. Combin. Math. Combin. Comput., 13 (1993), pp. 161–165.
- [241] G. L. MULLEN AND R. E. WEBER, *Latin cubes of order ≤ 5* , Discrete Math., 32 (1980), pp. 291–297.
- [242] G. P. NAGY AND P. VOJTĚCHOVSKÝ, *LOOPS – Computing with quasigroups and loops in GAP*. <http://www.math.du.edu/loops/>.
- [243] ———, *Computing with small quasigroups and loops*, Quasigroups Related Systems, 15 (2007), pp. 77–94.
- [244] J. R. NECHVATAL, *Counting Latin Rectangles*, PhD thesis, University of Southern California, 1979.
- [245] ———, *Asymptotic enumeration of generalized Latin rectangles*, Util. Math., 20 (1981), pp. 273–292.
- [246] P. M. NEUMANN, *Proof of a conjecture by Garret Birkhoff and Philip Hall on the automorphisms of a finite group*, Bull. London Math. Soc., 27 (1995), pp. 222–224.

- [247] H. NIEDERREITER AND K. H. ROBINSON, *Complete mappings of finite fields*, J. Austral. Math. Soc. Ser. A, 33 (1982), pp. 197–212.
- [248] W. NÖBAUER, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math., 69 (1965), pp. 230–238.
- [249] —, *Compatible and conservative functions on residue-class rings of the integers*, in Topics in Number Theory, vol. 13, North-Holland, 1976, pp. 245–257.
- [250] D. A. NORTON, *Groups of orthogonal row-Latin squares*, Pacific J. Math., 2 (1952), pp. 335–341.
- [251] H. W. NORTON, *The 7×7 squares*, Ann. Eugenics, 2 (1939), pp. 269–307.
- [252] D. NOVAKOVICH, *Computation of the number of complete mappings for permutations*, Cybernet. Systems Anal., 36 (2000), pp. 244–247.
- [253] F. O’CARROLL, *A method of generating randomized Latin squares*, Biometrics, 19 (1963), pp. 652–653.
- [254] L.-D. ÖHMAN, *Latin squares with prescriptions and restrictions*. Submitted.
- [255] —, *The intricacy of avoiding arrays is 2*, Discrete Math., 306 (2006), pp. 531–532.
- [256] S. ONN, *A colorful determinantal identity, a conjecture of Rota, and Latin squares*, Amer. Math. Monthly, 104 (1997), pp. 156–159.
- [257] L. J. PAIGE, *A note on finite Abelian groups*, Bull. Amer. Math. Soc., 53 (1947), pp. 590–593.
- [258] L. J. PAIGE, *Neofields*, Duke Math. J., 16 (1949), pp. 39–60.
- [259] K. T. PHELPS, *Latin square graphs and their automorphism groups*, Ars Combin., 7 (1979), pp. 273–299.
- [260] —, *Automorphism-free Latin square graphs*, Discrete Math., 31 (1980), pp. 193–200.
- [261] B. POLSTER, *The mathematics of juggling*, Wiley, 2003.
- [262] V. N. POTAPOV AND D. S. KROTOV, *Asymptotics for the number of n -quasigroups of order 4*, Siberian Math. J., 47 (2006), pp. 720–731.
- [263] C. R. PRANESACHAR, *Enumeration of Latin rectangles via SDR’s*, in Lecture Notes in Math., Springer, 1981, pp. 380–390.
- [264] —, *On the number of two-line and three-line Latin rectangles – an alternative approach*, Discrete Math., 38 (1982), pp. 79–86.
- [265] D. A. PREECE, *Classifying Youden rectangles*, J. Roy. Statist. Soc. Ser. B, 28 (1966), pp. 118–130.
- [266] —, *Latin squares, Latin cubes, Latin rectangles*, in Encyclopedia of Statistical Sciences, Wiley, 2006.
- [267] J. RIORDAN, *Three-line Latin rectangles*, Amer. Math. Monthly, 51 (1944), pp. 450–452.
- [268] —, *Three-line Latin rectangles–II*, Amer. Math. Monthly, 53 (1946), pp. 18–20.
- [269] —, *A recurrence relation for three-line Latin rectangles*, Amer. Math. Monthly, 59 (1952), pp. 159–162.

- [270] ———, *Book review: Percy Alexander MacMahon: Collected Papers, Volume I, Combinatorics*, Bull. Amer. Math. Soc. (N.S.), 2 (1980), pp. 239–241.
- [271] I. RIVIN, I. VARDI, AND P. ZIMMERMANN, *The n -queens problem*, Amer. Math. Monthly, 101 (1994), pp. 629–639.
- [272] G.-C. ROTA, *On the foundations of combinatorial theory. I. Theory of Möbius functions*, Z. Wahrsch. und Verw. Gebiete, 2 (1964), pp. 340–368.
- [273] H. J. RYSER, *Combinatorial Mathematics*, Springer, 1963.
- [274] A. A. SADE, *Énumération des carrés latins, application au 7^e ordre, conjecture pour les ordres supérieurs*, privately published, (1948). 8 pp.
- [275] ———, *An omission in Norton's list of 7×7 squares*, Ann. Math. Stat., 22 (1951), pp. 306–307.
- [276] ———, *Morphismes de quasigroupes. Tables*, Univ. Lisboa Revista Fac. Ci. A, 13 (1970/71), pp. 149–172.
- [277] THE SAGE DEVELOPMENT TEAM, *SAGE mathematics software*. <http://www.sagemath.org/>.
- [278] P. N. SAXENA, *A simplified method of enumerating Latin squares by MacMahon's differential operators; I. the 6×6 squares*, J. Indian Soc. Agricultural Statist., 2 (1950), pp. 161–188.
- [279] ———, *A simplified method of enumerating Latin squares by MacMahon's differential operators; II. the 7×7 squares*, J. Indian Soc. Agricultural Statist., 3 (1951), pp. 24–79.
- [280] E. SCHÖNHARDT, *Über lateinische Quadrate und Unionen*, J. Reine Angew. Math., 163 (1930), pp. 183–229.
- [281] A. SCHRIJVER, *A short proof of Minc's conjecture*, J. Combin. Theory Ser. A, 25 (1978), pp. 80–83.
- [282] J.-Y. SHAO AND W.-D. WEI, *A formula for the number of Latin squares*, Discrete Math., 110 (1992), pp. 293–296.
- [283] H. D. SHAPIRO, *Generalized Latin squares on the torus*, Discrete Math., 24 (1978), pp. 63–77.
- [284] X. SHEN, *Generalized Latin squares. II*, Discrete Math., 143 (1995), pp. 221–242.
- [285] X. SHEN, Y. Z. CAI, C. L. LIU, AND C. P. KRUSKAL, *Generalized Latin squares. I*, in *Combinatorics and Complexity*, vol. 25, 1989, pp. 155–178.
- [286] Y.-P. SHIEH, *Partition Strategies for #P-Complete Problems with Applications to Enumerative Combinatorics*, PhD thesis, National Taiwan University, 2001.
- [287] R. SINKHORN, *Concerning a conjecture of Marshall Hall*, Proc. Amer. Math. Soc., 21 (1969), pp. 197–201.
- [288] I. SKAU, *A note on the asymptotic number of Latin rectangles*, European J. Combin., 19 (1998), pp. 617–620.
- [289] T. SLIVNIK, *Short proof of Galvin's theorem on the list-chromatic index of a bipartite multigraph*, Combin. Probab. Comput., 5 (1996), pp. 91–94.
- [290] N. J. A. SLOANE, *The on-line encyclopedia of integer sequences*. <http://www.research.att.com/~njas/sequences/>.

- [291] B. SMETANIUK, *A new construction of Latin squares. II. The number of Latin squares is strictly increasing*, Ars Combin., 14 (1982), pp. 131–145.
- [292] —, *Topics in the Theory of Latin Squares*, PhD thesis, University of Sydney, 1983.
- [293] H. S. SNEVILY, *Unsolved problems: The Cayley addition table of \mathbb{Z}_n* , Amer. Math. Monthly, 106 (1999), pp. 584–585.
- [294] E. SOEDARMADJI, *Latin hypercubes and MDS codes*, Discrete Math., 306 (2006), pp. 1232–1239.
- [295] L. H. SOICHER, *GRAPE – A GAP package for computing with graphs and groups*. <http://www.maths.qmul.ac.uk/~leonard/grape/>.
- [296] T. STEHLING, *On computing the number of subgroups of a finite Abelian group*, Combinatorica, 12 (1992), pp. 475–479.
- [297] C. STEIN, *Approximate Computation of Expectations*, Institute of Mathematical Statistics, 1986.
- [298] C. M. STEIN, *Asymptotic evaluation of the number of Latin rectangles*, J. Combin. Theory Ser. A, 25 (1978), pp. 38–49.
- [299] —, *A way of using auxiliary randomization*, in Probability Theory, Walter de Gruyter & Co., 1992, pp. 159–180.
- [300] S. K. STEIN, *Transversals of Latin squares and their generalizations*, Pacific J. Math., 59 (1975), pp. 567–575.
- [301] D. S. STONES, *The many formulae for the number of Latin rectangles*. In preparation.
- [302] —, (2009). <http://code.google.com/p/latinrectangles/downloads/list>.
- [303] D. S. STONES, P. VOJTĚCHOVSKÝ, AND I. M. WANLESS, *Autotopisms and automorphisms of Latin squares*. In preparation.
- [304] D. S. STONES AND I. M. WANLESS, *Compound orthomorphisms of the cyclic group*. Submitted.
- [305] —, *A congruence connecting Latin rectangles and partial orthomorphisms*. Submitted.
- [306] —, *How not to prove the Alon-Tarsi Conjecture*. In preparation.
- [307] —, *Latin squares with many subsquares and large autotopism groups*. In preparation.
- [308] —, *Divisors of the number of Latin rectangles*, J. Combin. Theory Ser. A, 117 (2010), pp. 204–215.
- [309] Q. SUN AND Q.-F. ZHANG, *A simple proof of a conjecture about complete mappings over finite fields*, Sichuan Daxue Xuebao, 35 (1998), pp. 840–842. In Chinese.
- [310] G. TARRY, *Le problème des 36 officers*, Ass. Franç. Paris, 29 (1901), pp. 170–203.
- [311] T.-S. TAY, *Some results on generalized Latin squares*, Graphs Combin., 12 (1996), pp. 199–207.
- [312] A. N. TIMASHOV, *On permanents of random doubly stochastic matrices and on asymptotic estimates for the number of Latin rectangles and Latin squares*, Discrete Math. Appl., 12 (2002), pp. 431–452.

- [313] B. L. VAN DER WAERDEN, *Aufgabe 45*, J. de Math. spéc., 35 (1926), p. 117.
- [314] D. C. VAN LEIJENHORST, *Symmetric functions, Latin squares and Van der Corput's "scriptum 3"*, Expo. Math., 18 (2000), pp. 343–356.
- [315] J. H. VAN LINT AND R. M. WILSON, *A Course in Combinatorics*, Cambridge University Press, 1992.
- [316] G. H. J. VAN REES, *On Latin queen squares*, Congr. Numer., 31 (1981), pp. 267–273.
- [317] —, *Subsquares and transversals in Latin squares*, Ars Combin., 29 (1990), pp. 193–204.
- [318] I. VARDI, *Computational Recreations in Mathematica*, Addison-Wesley, 1991.
- [319] D. Q. WAN, *On a problem of Niederreiter and Robinson about finite fields*, J. Austral. Math. Soc. Ser. A, 41 (1986), pp. 336–338.
- [320] I. M. WANLESS, *Latin squares with one subsquare*, J. Combin. Des., 9 (2001), pp. 128–146.
- [321] —, *A lower bound on the maximum permanent in Λ_n^k* , Linear Algebra Appl., 373 (2003), pp. 153–167.
- [322] —, *Cycle switches in Latin squares*, Graphs Combin., 20 (2004), pp. 545–570.
- [323] —, *Diagonally cyclic Latin squares*, European J. Combin., 25 (2004), pp. 393–413.
- [324] —, *Transversals in Latin squares*, Quasigroups Related Systems, 15 (2007), pp. 169–190.
- [325] I. M. WANLESS AND E. C. IHRIG, *Symmetries that Latin squares inherit from 1-factorizations*, J. Combin. Des., 13 (2005), pp. 157–172.
- [326] M. B. WELLS, *The number of Latin squares of order eight*, J. Combin. Theory, 3 (1967), pp. 98–99.
- [327] —, *Elements of Combinatorial Computing*, Pergamon Press, 1971.
- [328] H. S. WHITE, F. N. COLE, AND L. D. CUMMINGS, *Complete classification of triad systems on fifteen elements*, Memoirs Nat. Acad. Sci. USA, 14 (1919), pp. 1–89.
- [329] H. WHITNEY, *A logical expansion in mathematics*, Bull. Amer. Math. Soc., 38 (1932), pp. 572–579.
- [330] H. S. WILF, *What is an answer?*, Amer. Math. Monthly, 89 (1982), pp. 289–292.
- [331] H. C. WILLIAMS, *The primality of $N = 2A3^n - 1$* , Canad. Math. Bull., 15 (1972), pp. 585–589.
- [332] H. C. WILLIAMS AND C. R. ZARNKE, *Some prime numbers of the forms $2A3^n + 1$ and $2A3^n - 1$* , Math. Comp., 26 (1972), pp. 995–998.
- [333] K. YAMAMOTO, *Asymptotic number of Latin rectangles and the symbolic method*, Sûgaku, 2 (1949).
- [334] —, *An asymptotic series for the number of three-line Latin rectangles*, J. Math. Soc. Japan, 1 (1950), pp. 226–241.
- [335] —, *On the asymptotic number of Latin rectangles*, Japan. J. Math., 21 (1951), pp. 113–119.

- [336] ———, *Note on enumeration of 7×7 Latin squares*, Bull. Math. Statist., 5 (1952), pp. 1–8.
- [337] ———, *Symbolic methods in the problem of three-line Latin rectangles*, J. Math. Soc. Japan, 5 (1953), pp. 13–23.
- [338] ———, *On the number of Latin rectangles*, Res. Rep. Sci. Div. Tokyo Womens' Univ., 19 (1969), pp. 86–97.
- [339] P. ZAPPA, *Triplets of Latin squares*, Boll. Un. Mat. Ital. A (7), 10 (1996), pp. 63–69.
- [340] ———, *The Cayley determinant of the determinant tensor and the Alon-Tarsi Conjecture*, Adv. in Appl. Math., 13 (1997), pp. 31–44.
- [341] D. ZEILBERGER, *The method of undetermined generalization and specialization. Illustrated with Fred Galvin's amazing proof of the Dinitz Conjecture*, Amer. Math. Monthly, 103 (1996), pp. 233–239.
- [342] ———, *Enumerative and algebraic combinatorics*, in Princeton Companion to Mathematics, Princeton University Press, 2008, pp. 550–561.
- [343] J. ZENG, *The generating function for the difference in even and odd three-line Latin rectangles*, Ann. Sci. Math. Québec, 20 (1996), pp. 105–108.
- [344] C. ZHANG AND J. MA, *Counting solutions for the N -queens and Latin square problems by Monte Carlo simulations*, Phys. Rev. E, 79 (2009). 016703.

APPENDIX A

Appendix

A.1 Finding the autotopism and autoparatopism groups

In this section we list some GAP code that will enable us to compute the autotopism and autoparatopism groups of a Latin square using the GRAPE [295] package for GAP, which in turn requires McKay's nauty [220] package. A Latin square L will be treated as an $n \times n$ matrix on the symbol set $\{1, 2, \dots, n\}$; this is the same format as returned by `CayleyTable(Q)` in LOOPS [242].

Autotopism group

The following code receives a Latin square $L = (l_{ij})$ (or any other matrix) and returns the orthogonal array of L , that is a set of triplets (i, j, l_{ij}) .

```
OrthogonalArray:=function(L)
  local r,c,OA;
  OA:=[];
  for r in [1..DimensionsMat(L)[1]] do
    for c in [1..DimensionsMat(L)[2]] do
      Append(OA,[[r,c,L[r][c]]]);
    od;
  od;
  return OA;
end;;
```

The next functions construct the vertex-coloured graph G_2 described by McKay, Meynert and Myrvold [222] in GRAPE format. They prove in [222] that the automorphism group of the graph G_2 is isomorphic to the autotopism group of the Latin square L .

```
MMMLatinSquareGraphG2EdgeSet:=function(L)
  local o,n,E;
  E:=[];
```

```

for o in OrthogonalArrayLatinSquare(L) do
  Append(E, [[n*(o[1]-1)+((o[2]-1) mod n)+3*n+1,o[1]]]);
  Append(E, [[o[1],n*(o[1]-1)+((o[2]-1) mod n)+3*n+1]]);
  Append(E, [[n*(o[1]-1)+((o[2]-1) mod n)+3*n+1,o[2]+n]]);
  Append(E, [[o[2]+n,n*(o[1]-1)+((o[2]-1) mod n)+3*n+1]]);
  Append(E, [[n*(o[1]-1)+((o[2]-1) mod n)+3*n+1,o[3]+2*n]]);
  Append(E, [[o[3]+2*n,n*(o[1]-1)+((o[2]-1) mod n)+3*n+1]]);
od;
return E;
end;;

```

The above function `MMMLatinSquareGraphG2EdgeSet(L)` returns the edge set E of the graph G_2 constructed by L . We wish to consider simple graphs, however `nauty` requires a directed graph as its input. This is overcome by including every edge in both directions. The following function `MMMLatinSquareGraphG2(L)` will convert the edge set E into G_2 without a vertex-colouring that can be interpreted by `GRAPE`. The purpose of splitting the function in this way is so we can reuse the `MMMLatinSquareGraphG2EdgeSet(L)` function later for constructing the graph required for finding the autoparatopism group of L .

```

MMMLatinSquareGraphG2:=function(L)
  local n,E;
  n:=Size(L);
  E:=MMMLatinSquareGraphG2EdgeSet(L);
  return EdgeOrbitsGraph(Group(()),E,n);
end;;

```

Now we are ready to make the function `AutotopismGroupLatinSquare(L)` that returns a group isomorphic to the autotopism group of the Latin square L .

```

AutotopismGroupLatinSquare:=function(L)
  local n;
  n:=Size(L);
  return AutGroupGraph(MMMLatinSquareGraphG2(L),
    [[1..n],[n+1..2*n],[2*n+1..3*n],[3*n+1..3*n+n^2]]);
  # this defines the required vertex-colouring
end;;

```

To test the code we can type, for example,

```
AutotopismGroupLatinSquare(CayleyTable(RandomQuasigroup(n)));
```

for some n .

Autoparatopism group

The next function constructs the graph G_1 described by McKay, Meynert and Myrvold [222] in `GRAPE` format. They prove in [222] that the automorphism group of the graph G_1 is isomorphic to the autoparatopism group of the Latin square L .

We begin with the edge set generated by the `MMMLatinSquareGraphG2EdgeSet(L)` function and append some extra edges, implicitly creating 3 extra vertices in the process.

```

MMMLatinSquareGraphG1EdgeSet:=function(L)
  local count,E,n;
  E:=MMMLatinSquareGraphG2EdgeSet(L);
  n:=Size(L);
  for count in [1..n] do
    Append(E,[[count,n^2+3*n+1]]);
    Append(E,[[n^2+3*n+1,count]]);
    Append(E,[[count+n,n^2+3*n+2]]);
    Append(E,[[n^2+3*n+2,count+n]]);
    Append(E,[[count+2*n,n^2+3*n+3]]);
    Append(E,[[n^2+3*n+3,count+2*n]]);
  od;
  return E;
end;;

```

The remaining functions are analogues of the autotopism case.

```

MMMLatinSquareGraphG1:=function(L)
  local n,E;
  n:=Size(L);
  E:=MMMLatinSquareGraphG1EdgeSet(L);
  return GraphFromEdgeSet(EdgeOrbitsGraph(Group()),E,n));
end;;

```

```

AutoparatopismGroupLatinSquare:=function(L)
  local n;
  n:=Size(L);
  return AutGroupGraph(MMMLatinSquareGraphG1(L),
    [[1..n],[n+1..2*n],[2*n+1..3*n],[3*n+1..3*n+n^2]
    ,[3*n+n^2+1,3*n+n^2+3]]);
  # this defines the required vertex-colouring
end;;

```

A.2 The number of even and odd Latin squares

n	R_n^{EVEN}	R_n^{ODD}	$R_n^{\text{EVEN}} - R_n^{\text{ODD}}$	References
2	1	0	1	[5] [171, 217, 340]
3	1	0	1	
4	4	0	4	
5	40	16	24	
6	5856	3552	2304	
7	8609280	8332800	276480	
8	270746124288	264535277568	6210846720	
2	1	0	1	
3	1	0	1	
4	2^2	0	2^2	
5	$2^3 \cdot 5$	2^4	$2^3 \cdot 3$	
6	$2^5 \cdot 3 \cdot 61$	$2^5 \cdot 3 \cdot 37$	$2^8 \cdot 3^2$	
7	$2^9 \cdot 3 \cdot 5 \cdot 19 \cdot 59$	$2^9 \cdot 3 \cdot 5^2 \cdot 7 \cdot 31$	$2^{11} \cdot 3^3 \cdot 5$	
8	$2^{17} \cdot 3 \cdot 688543$	$2^{19} \cdot 3 \cdot 109 \cdot 1543$	$2^{17} \cdot 3^6 \cdot 5 \cdot 13$	

FIGURE A.1: Some values of R_n^{EVEN} and R_n^{ODD} , along with their difference and prime factorisation.

n	R_n^{RE}	R_n^{RO}	$R_n^{\text{RE}} - R_n^{\text{RO}}$
2	0	1	-1
3	1	0	1
4	4	0	4
5	16	40	-24
6	3552	5856	-2304
7	8286720	8655360	-368640
8	270746124288	264535277568	6210846720
2	0	1	-1
3	1	0	1
4	2^2	0	2^2
5	2^4	$2^3 \cdot 5$	$-2^3 \cdot 3$
6	$2^5 \cdot 3 \cdot 37$	$2^5 \cdot 3 \cdot 61$	$-2^8 \cdot 3^2$
7	$2^9 \cdot 3 \cdot 5 \cdot 13 \cdot 83$	$2^9 \cdot 3 \cdot 5 \cdot 7^2 \cdot 23$	$-2^{13} \cdot 3^2 \cdot 5$
8	$2^{17} \cdot 3 \cdot 688543$	$2^{19} \cdot 3 \cdot 109 \cdot 1543$	$2^{17} \cdot 3^6 \cdot 5 \cdot 13$

FIGURE A.2: Some values of R_n^{RE} and R_n^{RO} , along with their difference and prime factorisation.

n	U_n^{EVEN}	U_n^{ODD}	$U_n^{\text{EVEN}} - U_n^{\text{ODD}}$
2	1	0	1
3	0	1	-1
4	4	0	4
5	16	40	-24
6	5856	3552	2304
7	8655360	8286720	368640
8	270746124288	264535277568	6210846720
2	1	0	1
3	0	1	-1
4	2^2	0	2^2
5	2^4	$2^3 \cdot 5$	$-2^3 \cdot 3$
6	$2^5 \cdot 3 \cdot 61$	$2^5 \cdot 3 \cdot 37$	$2^8 \cdot 3^2$
7	$2^9 \cdot 3 \cdot 5 \cdot 7^2 \cdot 23$	$2^9 \cdot 3 \cdot 5 \cdot 13 \cdot 83$	$2^{13} \cdot 3^2 \cdot 5$
8	$2^{17} \cdot 3 \cdot 688543$	$2^{19} \cdot 3 \cdot 109 \cdot 1543$	$2^{17} \cdot 3^6 \cdot 5 \cdot 13$

FIGURE A.3: Some values of U_n^{EVEN} and U_n^{ODD} , along with their difference and prime factorisation.

A.3 The number of four-line and five-line Latin rectangles

The following numbers were found using (1.16) and the C code has been uploaded here [302]. The values for $n \leq 80$ are now listed at Sloane's [290] A000573.

n	$R_{4,n}$
4	4
5	56
6	6552
7	1293216
8	420909504
9	207624560256
10	147174521059584
11	143968880078466048
12	188237563987982390784
13	320510030393570671051776
14	695457005987768649183581184
15	1888143905499961681708381310976
16	6314083806394358817244705266941952
17	25655084790196439186603345691314159616
18	125151207879107507418595651580525408108544
19	725286528193978151376645991587386316447154176
20	4946695754673063706940982976280298177634970763264
21	39372620049112842147403644555875630051344172847464448
22	362953223623178176928985853358776023561076140898585411584
23	3848556868310251682051540453289191302911656946425858318401536
24	46646364890123254950981334346141630039665836277086889810449137664
25	642577452766632866336746626812914310810476309618605956127608795037696
26	10007844722789723474949164515246755752126297615867851579087218636333514752
27	175373037219837331563272997448082923441580267971837196568365005992563746799616
4	2^2
5	$2^3 \cdot 7$
6	$2^3 \cdot 3^2 \cdot 7 \cdot 13$
7	$2^5 \cdot 3 \cdot 19 \cdot 709$
8	$2^6 \cdot 3 \cdot 149 \cdot 14713$
9	$2^7 \cdot 3^4 \cdot 20025517$
10	$2^8 \cdot 3^3 \cdot 71 \cdot 271 \cdot 1106627$
11	$2^{10} \cdot 3^2 \cdot 1823 \cdot 8569184461$
12	$2^9 \cdot 3^3 \cdot 7 \cdot 1945245990285863$
13	$2^{10} \cdot 3^4 \cdot 7 \cdot 587 \cdot 50821 \cdot 18504497761$
14	$2^{10} \cdot 3^4 \cdot 8384657190246053351461$
15	$2^{12} \cdot 3^5 \cdot 30525787 \cdot 62144400106703441$
16	$2^{14} \cdot 3^5 \cdot 2693 \cdot 42787 \cdot 1699482467 \cdot 8098773443$
17	$2^{16} \cdot 3^5 \cdot 131 \cdot 271 \cdot 17104781 \cdot 166337753 \cdot 15949178369$
18	$2^{14} \cdot 3^7 \cdot 23 \cdot 61 \cdot 3938593 \cdot 632073448679498674606517$
19	$2^{17} \cdot 3^6 \cdot 7 \cdot 13 \cdot 61 \cdot 197007401 \cdot 158435451761 \cdot 43809270413057$
20	$2^{17} \cdot 3^6 \cdot 7^2 \cdot 1056529591513682816198269594516734004747$
21	$2^{18} \cdot 3^7 \cdot 19 \cdot 31253 \cdot 103657 \cdot 1115736555797150985616406088863209$
22	$2^{18} \cdot 3^8 \cdot 158419 \cdot 366314603941483807 \cdot 3636463205495660670300697$
23	$2^{20} \cdot 3^8 \cdot 58309 \cdot 1588208779694954759917 \cdot 6040665277134180218$
24	$2^{21} \cdot 3^9 \cdot 43 \cdot 283 \cdot 1373 \cdot 8191 \cdot 297652680582511 \cdot 27741149414473864785280935767$
25	$2^{22} \cdot 3^{11} \cdot 1938799914572671 \cdot 446065653297963631389971651136461400611927$
26	$2^{23} \cdot 3^9 \cdot 7 \cdot 19 \cdot 31 \cdot 5147 \cdot 694758890407 \cdot 4111097244170498224110627242779017943828829$
27	$2^{25} \cdot 3^{12} \cdot 7 \cdot 13127 \cdot 107027245883591876663734983579930090734219751042699442932337$

FIGURE A.4: The value of $R_{4,n}$ and its prime factorisation for $4 \leq n \leq 27$.

n	$R_{5,n}$
5	56
6	9408
7	11270400
8	27206658048
9	112681643083776
10	746988383076286464
11	7533492323047902093312
12	111048869433803210653040640
13	2315236533572491933131807916032
14	66415035616070432053233927044726784
15	2560483881619577552584872021599994249216
16	130003705747573381528820187969499352864391168
17	8540614065591861115863858023929942463204158341120
18	714772705022049580010386905464376609190681339062386688
19	75163163562802272546579759450749095599610461567358920032256
20	9809720003910626776223482379751753587443069548693920857303547904
21	1571535264701285629600025091867663915099001357016958197822862919729152
22	305967368069117220345719015650882351240204884316352710461216388953743032320
23	71742822040206698482547032648440680248173149276783605396347465027480511202721792
24	20093299726164942410036767774030176748339141446536947374523570181642887594307280175104
25	6671363422740192076170128383025874322430996291082893578356639976639833297028025599106482176
5	$2^3 \cdot 7$
6	$2^6 \cdot 3 \cdot 7^2$
7	$2^8 \cdot 3 \cdot 5^2 \cdot 587$
8	$2^{11} \cdot 3 \cdot 23 \cdot 192529$
9	$2^{11} \cdot 3^4 \cdot 13 \cdot 52251029$
10	$2^{16} \cdot 3^6 \cdot 19 \cdot 97 \cdot 8483617$
11	$2^{13} \cdot 3^2 \cdot 29 \cdot 168293 \cdot 20936295857$
12	$2^{17} \cdot 3^6 \cdot 5 \cdot 7 \cdot 47 \cdot 59 \cdot 313 \cdot 38257310467$
13	$2^{19} \cdot 3^3 \cdot 7 \cdot 23364884851571662672051$
14	$2^{27} \cdot 3^4 \cdot 101 \cdot 449 \cdot 1039 \cdot 3019 \cdot 22811 \cdot 1882698637$
15	$2^{22} \cdot 3^7 \cdot 19 \cdot 423843896863 \cdot 34662016427839511$
16	$2^{28} \cdot 3^6 \cdot 3604099 \cdot 40721862001 \cdot 4526515223205743$
17	$2^{25} \cdot 3^5 \cdot 5 \cdot 15001087 \cdot 13964976140347893908947110110827$
18	$2^{28} \cdot 3^9 \cdot 1019173084339 \cdot 237316919875331 \cdot 559319730817259$
19	$2^{28} \cdot 3^6 \cdot 7 \cdot 47 \cdot 149 \cdot 532451 \cdot 347100904121707 \cdot 42395531645181804688477$
20	$2^{32} \cdot 3^9 \cdot 7 \cdot 67 \cdot 163 \cdot 360046981713037753 \cdot 4215856658533108520354659333$
21	$2^{33} \cdot 3^8 \cdot 83 \cdot 281 \cdot 204292081063933 \cdot 5852323051960913177671486927343120669$
22	$2^{36} \cdot 3^7 \cdot 5 \cdot 13 \cdot 241559 \cdot 129661160424791080992764645120871929236425763066453631$
23	$2^{39} \cdot 3^{10} \cdot 5407 \cdot 120427 \cdot 901145309 \cdot 3766352936022215583264814011876189449770138391$
24	$2^{41} \cdot 3^{11} \cdot 107 \cdot 739951 \cdot 2418119033203 \cdot 318514544213636008246871 \cdot 845851172573304061243151$
25	$2^{41} \cdot 3^9 \cdot 94513 \cdot 54260027 \cdot 25093654805621 \cdot 1059078880359738933703 \cdot 1130914320793991851927211947$

FIGURE A.5: The value of $R_{5,n}$ and its prime factorisation for $5 \leq n \leq 25$.

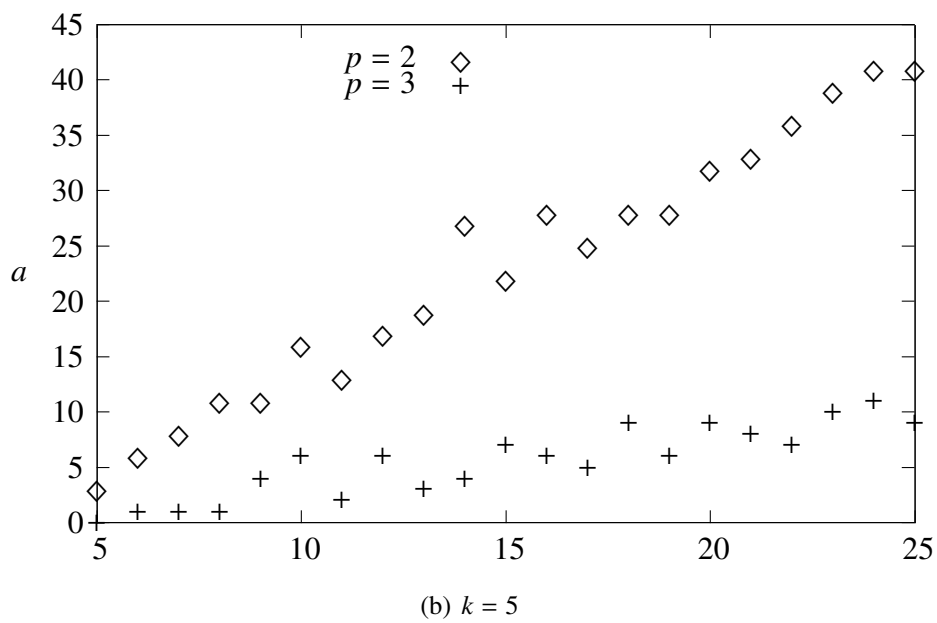
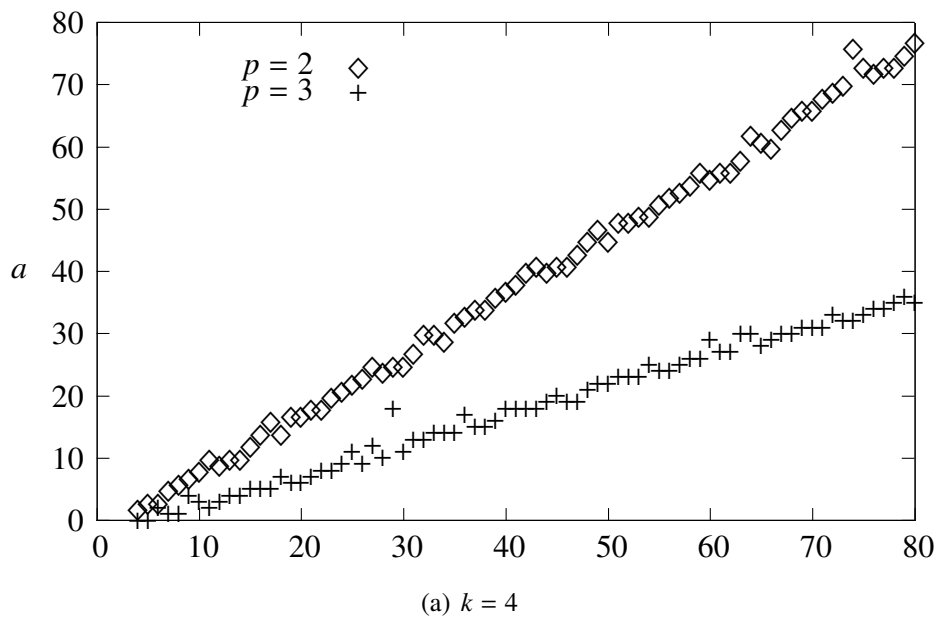


FIGURE A.6: Some values of the largest integer a such that p^a divides $R_{k,n}$ for $k \in \{4, 5\}$ and $p \in \{2, 3\}$.

A.4 Autotopisms of Latin squares of orders 12, 13 and 14.

In this section we list the cycle structures of the autotopisms of Latin squares of order n for $12 \leq n \leq 14$.

α	β if $\beta \sim \gamma$ else (β, γ)	α	β if $\beta \sim \gamma$ else (β, γ)	α	β if $\beta \sim \gamma$ else (β, γ)
1^{12}	$1^{12}, 2^6, 3^4, 4^3, 6^2, 12$	$4 \cdot 1^8$	$4^3, 12$	$6 \cdot 1^6$	$6 \cdot 1^6, 6 \cdot 3^2, 6^2, 12$
$2 \cdot 1^{10}$	$2^6, 4^3, 6^2, 12$	$4 \cdot 2 \cdot 1^6$	$4^3, 12$	$6 \cdot 2 \cdot 1^4$	$6^2, 12$
$2^2 \cdot 1^8$	$2^6, 4^3, 6^2, 12$	$4 \cdot 2^2 \cdot 1^4$	$4^3, 12$	$6 \cdot 2^2 \cdot 1^2$	$6 \cdot 2^2 \cdot 1^2, 6^2, 12$
$2^3 \cdot 1^6$	$2^3 \cdot 1^6, 2^6, 4^3, 6 \cdot 3^2, 6^2, 12$	$4 \cdot 2^3 \cdot 1^2$	$4^3, 12$	$6 \cdot 2^3$	$(6 \cdot 3^2, 6^2), 6^2, 12$
$2^4 \cdot 1^4$	$2^4 \cdot 1^4, 2^6, 4^3, 6^2, 12$	$4 \cdot 2^4$	$4^3, 12$	$6 \cdot 3 \cdot 1^3$	$6 \cdot 3 \cdot 1^3, 6 \cdot 3^2, 6^2, 12$
$2^5 \cdot 1^2$	$2^5 \cdot 1^2, 2^6, 4^3, 6^2, 12$	$4 \cdot 3 \cdot 1^5$	12	$6 \cdot 3 \cdot 2 \cdot 1$	$6 \cdot 3 \cdot 2 \cdot 1, 6^2, 12$
2^6	$2^6, (3^4, 6^2), 4^3, (6 \cdot 3^2, 6^2), 6^2, 12$	$4 \cdot 3 \cdot 2 \cdot 1^3$	12	$6 \cdot 3^2$	$6 \cdot 3^2, 6^2, 12$
$3 \cdot 1^9$	$3^4, 6^2, 12$	$4 \cdot 3 \cdot 2^2 \cdot 1$	12	$6 \cdot 4 \cdot 1^2$	12
$3 \cdot 2 \cdot 1^7$	$6^2, 12$	$4 \cdot 3^2 \cdot 1^3$	12	$6 \cdot 4 \cdot 2$	12
$3 \cdot 2^2 \cdot 1^5$	$6^2, 12$	$4 \cdot 3^2 \cdot 2 \cdot 1$	12	6^2	$6^2, 12$
$3 \cdot 2^3 \cdot 1^3$	$6 \cdot 3^2, 6^2, 12$	$4^2 \cdot 1^4$	$4^2 \cdot 1^4, 4^2 \cdot 2^2, 4^3, 12$	$7 \cdot 1^5$	$7 \cdot 1^5$
$3 \cdot 2^4 \cdot 1$	$6^2, 12$	$4^2 \cdot 2 \cdot 1^2$	$4^2 \cdot 2 \cdot 1^2, 4^2 \cdot 2^2, 4^3, 12$	$8 \cdot 1^4$	$8 \cdot 1^4, 8 \cdot 2^2, 8 \cdot 4$
$3^2 \cdot 1^6$	$3^2 \cdot 1^6, 3^4, 6 \cdot 2^3, 6^2, 12$	$4^2 \cdot 2^2$	$4^2 \cdot 2^2, 4^3, 12$	$8 \cdot 2 \cdot 1^2$	$8 \cdot 2 \cdot 1^2, 8 \cdot 2^2, 8 \cdot 4$
$3^2 \cdot 2 \cdot 1^4$	$6 \cdot 2^3, 6^2, 12$	$4^2 \cdot 3 \cdot 1$	12	$8 \cdot 2^2$	$8 \cdot 2^2, 8 \cdot 4$
$3^2 \cdot 2^2 \cdot 1^2$	$6 \cdot 2^3, 6^2, 12$	4^3	$(6 \cdot 3^2, 12), (6^2, 12)$	$9 \cdot 1^3$	$9 \cdot 1^3, 9 \cdot 3$
$3^2 \cdot 2^3$	$(3^2 \cdot 2^3, 6 \cdot 1^6), 6 \cdot 3^2, 6^2, 12$	$5^2 \cdot 1^2$	$5^2 \cdot 1^2, 10 \cdot 2$	$9 \cdot 3$	$9 \cdot 3$
$3^3 \cdot 1^3$	$3^3 \cdot 1^3, 3^4, 6^2, 12$			$10 \cdot 1^2$	$10 \cdot 1^2, 10 \cdot 2$
$3^3 \cdot 2 \cdot 1$	$6^2, 12$			$11 \cdot 1$	$11 \cdot 1$
3^4	$3^4, (4^3, 12), (6 \cdot 2^3, 6^2), 6^2, 12$				

FIGURE A.7: Cycle structures of the autotopisms of Latin squares of order 12.

α	$\beta \sim \gamma$	$\alpha \sim \beta \sim \gamma$	$\alpha \sim \beta \sim \gamma$	$\alpha \sim \beta \sim \gamma$	$\alpha \sim \beta \sim \gamma$
1^{13}	1^{13}	$2^4 \cdot 1^5$	$4^2 \cdot 1^5$	$6 \cdot 3 \cdot 2 \cdot 1^2$	$9 \cdot 1^4$
1^{13}	13	$2^5 \cdot 1^3$	$4^2 \cdot 2^2 \cdot 1$	$6 \cdot 3 \cdot 2^2$	$9 \cdot 3 \cdot 1$
		$2^6 \cdot 1$	$4^3 \cdot 1$	$6^2 \cdot 1$	$10 \cdot 1^3$
		$3^3 \cdot 1^4$	$5^2 \cdot 1^3$	$7 \cdot 1^6$	$10 \cdot 2 \cdot 1$
		$3^4 \cdot 1$		$8 \cdot 1^5$	$11 \cdot 1^2$
				$8 \cdot 2^2 \cdot 1$	$12 \cdot 1$
				$8 \cdot 4 \cdot 1$	13

FIGURE A.8: Cycle structures of the autotopisms of Latin squares of order 13.

α	β if $\beta \sim \gamma$ else (β, γ)				
1^{14}	$1^{14}, 2^7, 7^2, 14$	α	$\beta \sim \gamma$	α	$\beta \sim \gamma$
$2 \cdot 1^{12}$	$2^7, 14$	$5^2 \cdot 1^4$	$5^2 \cdot 1^4, 10 \cdot 2^2$	$8 \cdot 1^6$	$8 \cdot 1^6, 8 \cdot 2^3$
$2^2 \cdot 1^{10}$	$2^7, 14$	$5^2 \cdot 2 \cdot 1^2$	$10 \cdot 2^2$	$8 \cdot 2 \cdot 1^4$	$8 \cdot 2^3$
$2^3 \cdot 1^8$	$2^7, 14$	$5^2 \cdot 2^2$	$10 \cdot 2^2$	$8 \cdot 2^2 \cdot 1^2$	$8 \cdot 2^2 \cdot 1^2, 8 \cdot 2^3$
$2^4 \cdot 1^6$	$2^4 \cdot 1^6, 2^7, 14$	$6 \cdot 3 \cdot 2^2 \cdot 1$	$6 \cdot 3 \cdot 2^2 \cdot 1$	$8 \cdot 4 \cdot 1^2$	$8 \cdot 4 \cdot 1^2$
$2^5 \cdot 1^4$	$2^5 \cdot 1^4, 2^7, 14$	$6 \cdot 3^2 \cdot 1^2$	$6^2 \cdot 2$	$9 \cdot 1^5$	$9 \cdot 1^5$
$2^6 \cdot 1^2$	$2^6 \cdot 1^2, 2^7, 14$	$6^2 \cdot 1^2$	$6^2 \cdot 1^2, 6^2 \cdot 2$	$9 \cdot 3 \cdot 1^2$	$9 \cdot 3 \cdot 1^2$
2^7	$(7^2, 14)$	$7 \cdot 1^7$	$7 \cdot 1^7, 7^2, 14$	$10 \cdot 1^4$	$10 \cdot 1^4, 10 \cdot 2^2$
$3^3 \cdot 1^5$	$3^3 \cdot 1^5$	$7 \cdot 2 \cdot 1^5$	14	$10 \cdot 2 \cdot 1^2$	$10 \cdot 2 \cdot 1^2, 10 \cdot 2^2$
$3^4 \cdot 1^2$	$3^4 \cdot 1^2, 6^2 \cdot 2$	$7 \cdot 2^2 \cdot 1^3$	14	$11 \cdot 1^3$	$11 \cdot 1^3$
$4^2 \cdot 1^6$	$4^2 \cdot 1^6, 4^2 \cdot 2^3$	$7 \cdot 2^3 \cdot 1$	14	$12 \cdot 1^2$	$12 \cdot 1^2, 12 \cdot 2$
$4^2 \cdot 2 \cdot 1^4$	$4^2 \cdot 2^3$	7^2	$7^2, 14$	$13 \cdot 1$	$13 \cdot 1$
$4^2 \cdot 2^2 \cdot 1^2$	$4^2 \cdot 2^2 \cdot 1^2, 4^2 \cdot 2^3$				
$4^3 \cdot 1^2$	$4^3 \cdot 1^2, 4^3 \cdot 2$				

FIGURE A.9: Cycle structures of the autotopisms of Latin squares of order 14.

A.5 Data tables for Section 3.2.3

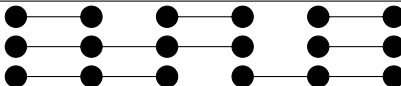


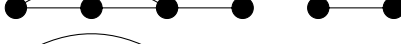

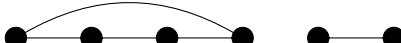

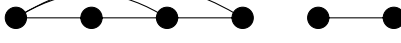



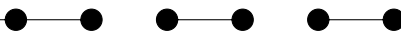
G	v	e	$ \text{Aut}(G) $	$P_G(a)$
	6	3	48	$27n^{2a-3} - 54n^{2a-4} + 36n^{2a-5} + 8n^{2a-6}$
	6	4	4	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	6	4	8	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	6	4	12	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	6	5	4	$27n^{2a-4} + 18n^{2a-5} - 132n^{2a-6} + 120n^{2a-7} - 32n^{2a-8}$
	6	5	12	$27n^{2a-4} + 18n^{2a-5} - 132n^{2a-6} + 120n^{2a-7} - 32n^{2a-8}$
	6	5	16	$9n^{2a-4} + 156n^{2a-5} - 468n^{2a-6} + 432n^{2a-7} - 128n^{2a-8}$
	6	6	8	$9n^{2a-4} + 48n^{2a-5} - 72n^{2a-6} + 16n^{2a-8}$
	6	6	72	$9n^{2a-4} + 36n^{2a-5} - 12n^{2a-6} - 96n^{2a-7} + 64n^{2a-8}$
	6	7	48	$9n^{2a-4} - 6n^{2a-5} + 108n^{2a-6} + (18g_2 - 204)n^{2a-7} \dots$ $\dots + (88 - 12 * g_2)n^{2a-8}$
	7	4	16	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	7	5	48	$27n^{2a-4} + 18n^{2a-5} - 132n^{2a-6} + 120n^{2a-7} - 32n^{2a-8}$
$K_2 \cup K_2 \cup K_2 \cup K_2$	8	4	384	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$

FIGURE A.10: The value of $P_G(a)$ for all $G \in \Gamma_{e,v}$ such that $v \geq 6$ and $P_G(a)$ has degree at least $2a - 4$ in n .

G	v	e	$ \text{Aut}(G) $	$P_G(a)$
	5	3	4	$27n^{2a-3} - 54n^{2a-4} + 36n^{2a-5} + 8n^{2a-6}$
	5	4	2	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	5	4	2	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	5	4	12	$9n^{2a-3} + 12n^{2a-4} - 36n^{2a-5} + 16n^{2a-6}$
	5	4	24	$81n^{2a-4} - 216n^{2a-5} + 216n^{2a-6} - 96n^{2a-7} + 16n^{2a-8}$
	5	5	2	$27n^{2a-4} + 18n^{2a-5} - 132n^{2a-6} + 120n^{2a-7} - 32n^{2a-8}$
	5	5	2	$27n^{2a-4} + 18n^{2a-5} - 132n^{2a-6} + 120n^{2a-7} - 32n^{2a-8}$
	5	5	2	$9n^{2a-4} + 156n^{2a-5} - 468n^{2a-6} + 432n^{2a-7} - 128n^{2a-8}$
	5	5	4	$27n^{2a-4} + 18n^{2a-5} - 132n^{2a-6} + 120n^{2a-7} - 32n^{2a-8}$
	5	5	10	$3n^{2a-4} + 210n^{2a-5} - 660n^{2a-6} + 720n^{2a-7} - 272n^{2a-8}$
	5	6	2	$9n^{2a-4} + 48n^{2a-5} - 72n^{2a-6} + 16n^{2a-8}$
	5	6	2	$9n^{2a-4} + 48n^{2a-5} - 72n^{2a-6} + 16n^{2a-8}$
	5	6	2	$3n^{2a-4} + 66n^{2a-5} - 12n^{2a-6} - 216n^{2a-7} + 160n^{2a-8}$
	5	6	8	$9n^{2a-4} + 36n^{2a-5} - 12n^{2a-6} - 96n^{2a-7} + 64n^{2a-8}$
	5	6	12	$3n^{2a-4} + 42n^{2a-5} + 180n^{2a-6} - 624n^{2a-7} + 400n^{2a-8}$
	5	7	2	$3n^{2a-4} + 30n^{2a-5} + 24n^{2a-6} - 72n^{2a-7} + 16n^{2a-8}$
	5	7	4	$3n^{2a-4} + 12n^{2a-5} + 144n^{2a-6} + (6g_2 - 300)n^{2a-7} + (160 - 24g_2)n^{2a-8}$
	5	7	6	$9n^{2a-4} - 6n^{2a-5} + 108n^{2a-6} + (18g_2 - 204)n^{2a-7} + (88 - g_2)n^{2a-8}$
	5	7	12	$3n^{2a-4} + 42n^{2a-5} - 36n^{2a-6} + 24n^{2a-7} - 32n^{2a-8}$
	5	8	4	$3n^{2a-4} + 12n^{2a-5} + 36n^{2a-6} + (6g_2 - 12)n^{2a-7} + (12g_2 - 56)n^{2a-8}$
	5	8	8	$3n^{2a-4} + 96n^{2a-6} - 78n^{2a-7} - 20n^{2a-8}$
	5	9	12	$3n^{2a-4} + 42n^{2a-6} + 42n^{2a-7} + (42g_2 - 128)n^{2a-8}$
	5	10	120	$3n^{2a-4} + 150n^{2a-7} + (60g_2 - 212)n^{2a-8}$

FIGURE A.11: The value of $P_G(a)$ for all $G \in \Gamma_{e,v}$ such that $v = 5$ and $P_G(a)$ has degree at least $2a - 4$ in n . Let $g_2 = \gcd(2, n)$.

- complete bipartite graph, 13
- complete mapping, 67
- complete tripartite graph, 15
- derangement, 18, 26
- Euler, Leonhard, 1, 26, 43, 68, 69
- graph decomposition, 14, 58
 - automorphism, 58
 - cycle, 60
 - isomorphic, 58
- isomorphism, 50
- Latin \vec{d} -cuboid, *see* Latin hypercuboid
- Latin cube, 47
- Latin hypercube, 47
 - sign, 52
- Latin hypercuboid, 46
 - automorphism, 50
 - autotopism, 50
 - diagonal, 52
 - isotopism, 50
 - isotopy class, 50
 - line, 52
 - normalised, 47
 - reduced, 47
 - subcuboid, 52
 - proper, 52
 - transversal, 52
- Latin rectangle, 2
 - automorphism, 8
 - autotopism, 8
 - five-line, 30
 - four-line, 27, 30
 - intercalate, 16
 - isomorphism, 8
 - isotopism, 6
 - isotopism group, 6
 - isotopy class, 8
 - normalised, 2
 - reduced, 2
 - subrectangle, 16
 - subsquare, 16
 - template, 18
 - three-line, 26, 43
 - two-line, 26, 43
- Latin square, 1
 - automorphism, 8
 - automorphism group, 9
 - autoparatopism, 9
 - autoparatopism group, 9
 - autotopism, 8
 - autotopism group, 9
 - bordered diagonally cyclic, 72
 - diagonal, 18
 - diagonally cyclic, 72
 - entry, 8
 - graph, 12
 - idempotent, 2, 61, 72
 - intercalate, 16
 - isomorphism, 8
 - isomorphism class, 8
 - isotopism, 6
 - principal, 9
 - isotopism group, 6
 - main class, 9

- orthogonal, 68
 - orthogonal array, 8
 - random, 25
 - subrectangle, 16
 - subsquare, 16
 - proper, 17
 - transversal, 18, 72
 - type, 9
 - unipotent, 2, 58, 72
- neofield, 70
- one-factorisation, 14, 58
- orthomorphism, 67
 - canonical, 67
 - compatible, 90
 - compound, 85
 - group of translations, 69
 - linear, 85
 - orthogonal, 97
 - polynomial, 90
- parastrophe, 8
- parastrophy group, 9
- paratopism, 9
- partial orthomorphism, 69
 - (n, d) -, 70
 - completion, 95
 - compound, 95
 - deficit, 69
 - size, 95
- permanent, 18, 27, 108
- Steiner triple system, 60
- strongly regular graph, 12