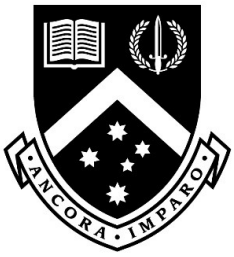

MONASH University

Latin Subrectangles

Jack Allsop
Bachelor of Science Advanced - Research (Honours), Monash University, 2021

A thesis submitted for the degree of Doctor of Philosophy at Monash University in 2025
School of Mathematics

Copyright notice

Abstract

Let n and k be positive integers with $k \leqslant n$. A $k \times n$ *Latin rectangle* is a $k \times n$ matrix of n symbols, each of which occurs exactly once in each row and at most once in each column. A *Latin square* of order n is an $n \times n$ Latin rectangle. Let L be a $k \times n$ Latin rectangle. A *Latin subrectangle* of L is a submatrix of L that is itself a Latin rectangle. A *proper subrectangle* of L is an $\ell \times m$ Latin subrectangle with $1 < \ell \leqslant m < n$. A *Latin subsquare* of L is a submatrix of L that is itself a Latin square. A *proper subsquare* of L is a Latin subsquare of order m with $1 < m < n$. In this thesis, we explore several problems regarding Latin subrectangles.

- We prove that with probability approaching 1 as $n \to \infty$, a uniformly random $k \times n$ Latin rectangle contains no proper subsquare of order 4 or more. This resolves a 25 year old conjecture of McKay and Wanless as well as a more recent conjecture of Divoux, Kelly, Kennedy, and Sidhu. We also study the expected number of Latin subsquares of orders 2 and 3 in uniformly random Latin rectangles.

- We prove that for all positive integers $n \notin \{4, 6\}$, there exists a Latin square of order n that does not contain any proper subsquares. This resolves a 50 year old conjecture of Hilton.

- The number of Latin squares of order at most 10 that do not contain any proper subrectangles has been known since 1999. We enumerate the Latin squares of order 11 that are devoid of proper subrectangles.

- Quadratic Latin squares are a special class of Latin squares that are defined over finite fields. They are highly structured and have lots of symmetry and thus have previously been used to construct many interesting mathematical objects. We investigate, and give at least partial answers to, several problems regarding Latin subrectangles of quadratic Latin squares such as: How many Latin subsquares of order 2 does a quadratic Latin square contain? When does a quadratic Latin square contain no proper subsquares?

Declaration

This thesis is an original work of my research and contains no material which has been accepted for the award of any other degree or diploma at any university or equivalent institution. To the best of my knowledge and belief, this thesis contains no material previously published or written by another person, except where due reference is made in the text of the thesis. This thesis contains no material that has been written by generative artificial intelligence.

Jack Allsop
21st July 2025

Publications during enrolment

- Chapter 3 is based on a paper published in Combinatorica [7]. This is joint work with Ian Wanless.
- Chapter 4 is based on a submitted paper [4]. This is joint work with Ian Wanless.
- Chapter 5 is based on a submitted paper [6]. This is joint work with Ian Wanless.
- Chapter 6 is based on two sole author papers. One is published in the Journal of Combinatorial Designs [2] and the other is submitted [3].

Acknowledgements

First, I would like to thank my supervisor Ian Wanless. It has been a great pleasure to work with you for the last few years and I am extremely appreciative of all the guidance you have given me. Thank you for everything.

Thank you to my associate supervisor Daniel Horsley. Thank you to David Wood, for being the chair of my PhD panel, and to Heiko Dietrich and Daniel Matthews, for being members of my PhD panel.

Thank you to Aleš Drápal and Melissa Lee, for many useful discussions that helped me obtain some of the results in Chapter 6.

Thank you to Elliot Marshall, for making the office a fun place to work.

Thank you to my family, for your constant support. Thank you to Emma, for the unwavering love and support you have given me, not only through this journey, but through everything.

Contents

Chapter 1

Introduction

The study of Latin rectangles goes back at least as far as the late 1600's or early 1700's, when the Korean mathematician Choi Seok-jeong published a Latin square of order 9 (see [30, Section I.2]). Since then, Latin rectangles have been the subject of thousands of papers and several books (see, e.g., [31, 32, 49, 80]). Latin rectangles have applications to, for example, experimental design (see, e.g., [32, Chapter 10]) and error correcting codes (see, e.g., [64]). The study of substructures of mathematical objects is a natural pursuit that has captivated mathematicians for centuries: Number theorists study prime factorisations, group theorists study subgroups, and graph theorists study subgraphs. This thesis is concerned with natural substructures of Latin rectangles known as Latin subrectangles. We investigate various problems related to Latin subrectangles and in doing so we resolve several old conjectures. Along with various combinatorial tools, we employ probabilistic, algorithmic, and algebraic methods in our investigations.

In Chapter 2, we give some important definitions that will be used throughout the thesis and we survey a variety of problems regarding Latin subrectangles. All undefined terms used in this chapter will be defined in Chapter 2.

A 1999 conjecture of McKay and Wanless [90] says that with probability $1-o(1)$ as $n \to \infty$, a uniformly random Latin square of order n has no proper subsquare of order 4 or more. This conjecture was recently generalised to Latin rectangles and was proved for 'thin' rectangles [39]. The main result of Chapter 3 is the resolution of these conjectures. The distributions of subsquares of orders 2 and 3 in Latin rectangles are also studied.

A conjecture of Hilton [31] from 1974 says that for all sufficiently large n, there exists a Latin square of order n that does not contain any proper subsquares. Though progress had previously been made on this conjecture, it remained unresolved. In Chapter 4, we resolve Hilton's conjecture by determining the existence spectrum of Latin squares without proper subsquares.

The number of perfect 1-factorisations of $K_{n,n}$ for $n \leqslant 10$ has been known since 1999 [116]. In Chapter 5, we enumerate the perfect 1-factorisations of $K_{11,11}$ and the associated Latin squares of order 11 that do not contain any proper subrectangles.

In Chapter 6, we study quadratic Latin squares. We consider and give at least partial answers to various questions related to or motivated by Latin subrectangles of quadratic Latin squares such as:

- How many subsquares of order 2 does a quadratic Latin square contain? In particular, when is a quadratic Latin square devoid of subsquares of order 2?

- When is a quadratic Latin square devoid of proper subrectangles?
- When can a quadratic Latin square be used to construct anti-perfect 1-factorisations of complete graphs or complete bipartite graphs? When is a quadratic Latin square anti-atomic?
- What are the autotopisms of a quadratic Latin square? When are two quadratic Latin squares isotopic?

Though we resolve some open problems in this thesis, there is an abundance of interesting problems regarding Latin subrectangles that are yet to be solved. In Chapter 7, we discuss some of these problems.

Concluding the thesis is a glossary of notation and a bibliography.

Chapter 2

Background

2.1 Basic definitions

We begin this chapter by giving some foundational definitions that will be used throughout this thesis. To avoid repetition, n will be a positive integer for the entirety of this chapter.

2.1.1 Latin rectangles and Latin subrectangles

Definition 2.1.1. Let $k \leqslant n$ be a positive integer. A $k \times n$ *Latin rectangle* is a $k \times n$ matrix of n symbols, each of which occurs exactly once in each row and at most once in each column. A *Latin square* of order n is an $n \times n$ Latin rectangle.

See Figure 2.1 for an example of a Latin rectangle and a Latin square.

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

Figure 2.1: A 3×6 Latin rectangle and a Latin square of order 5.

Definition 2.1.2. Let $k \leqslant n$ be a positive integer and let L be a $k \times n$ Latin rectangle. A *Latin subrectangle* of L is a submatrix of L that is itself a Latin rectangle. A *Latin subsquare* of L is a submatrix of L that is itself a Latin square.

We will generally refer to Latin subrectangles and Latin subsquares simply as subrectangles and subsquares, respectively. Every $k \times n$ Latin rectangle has kn subsquares of order 1 and every Latin square of order n has a single subsquare of order n. Furthermore, every $k \times n$ Latin rectangle has exactly $k(2^n - 1)$ subrectangles of dimension $1 \times m$ for some $m \leqslant n$ and exactly $2^k - 1$ subrectangles of dimension $\ell \times n$ for some $\ell \leqslant k$. These subsquares and subrectangles are unavoidable and somewhat uninteresting, which leads to the following definition.

Definition 2.1.3. Let $k \leqslant n$ be a positive integer and let L be a $k \times n$ Latin rectangle.

- A *proper subrectangle* of L is a $\ell \times m$ subrectangle of L with $1 < \ell \leqslant m < n$.

- A *proper subsquare* of L is a subsquare of L of order m with $1 < m < n$.
- An *intercalate* of L is a subsquare of L of order 2.

Intercalates will play a substantial role in this thesis. See Figure 2.2 for an example of a subrectangle, a subsquare, and an intercalate.

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

Figure 2.2: The highlighted yellow and green entries of the Latin square in this figure form a proper subsquare of order 3, the highlighted red entries form a proper 2×5 subrectangle, and the highlighted blue and green entries form an intercalate. The colour of cell $(2, 7)$ is green since it is involved in both the highlighted subsquare of order 3 and the highlighted intercalate.

For a positive integer m, let $[m]$ denote the set $\{1, 2, \ldots, m\}$. Let $k \leqslant n$ be a positive integer and let L be a $k \times n$ Latin rectangle with row index set R, column index set C, and symbol set S. In this thesis, we will sometimes take the sets R, C, and S to consist of elements of a group, elements of a field, or integers. However, we will always insist that R, C, and S have a total order on them. Any matrix has a total order on its rows and columns, thus the need for the total order on R and C. The reason for the insistence of a total order on S will become clear in §2.3.1. In most situations, the orders on R, C, and S will either be obvious or unimportant, thus will not specified. Of course, we can always relabel R to be $[k]$ and C and S to be $[n]$, both of which have a natural total order. For the remainder of this chapter, unless otherwise stated, we will assume that the row index set of a $k \times n$ Latin rectangle is $[k]$ and that its column index set and symbol set are $[n]$.

2.1.2 Quasigroups

Definition 2.1.4. A *quasigroup* is a pair $(Q, *)$ where Q is a non-empty set and $*$ is a binary operation on Q such that for all $(a, b) \in Q^2$ there exists a unique $(x, y) \in Q^2$ such that $a * x = b = y * a$.

The operation table of any finite quasigroup forms a Latin square. Conversely, if we index the rows and columns of a Latin square by its symbol set, then it can be interpreted as the operation table of some finite quasigroup. So Latin squares and finite quasigroups are, in a sense, equivalent mathematical objects.

We will often refer to a quasigroup $(Q, *)$ simply by Q. If Q is finite, then $|Q|$ is the *order* of Q. See Figure 2.3 for an example of a quasigroup and its corresponding Latin square.

$*$	0	1	2	3	4	5	6
0	0	3	6	1	5	4	2
1	3	1	4	0	2	6	5
2	6	4	2	5	1	3	0
3	1	0	5	3	6	2	4
4	5	2	1	6	4	0	3
5	4	6	3	2	0	5	1
6	2	5	0	4	3	1	6

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

Figure 2.3: Define a binary operation $*$ on $\mathbb{Z}_7$ by

$$x * y = \begin{cases} 3y - 2x & \text{if } y - x \in \{0, 1, 2, 4\}, \\ 3x - 2y & \text{otherwise,} \end{cases}$$

where all operations are to be taken modulo 7. This figure shows the operation table of $(\mathbb{Z}_7, *)$ and the corresponding Latin square.

2.1.3 Symmetries of Latin squares

Let M be a matrix with row index set R, column index set C, and symbol set S. For $i \in R$ and $j \in C$, we will denote the symbol in row i and column j of M by $M_{i,j}$. For subsets $I \subseteq R$ and $J \subseteq C$, we denote the submatrix of M induced by the rows in I and the columns in J by $M[I, J]$. The matrix $M[I, J]$ has row index set I and column index set J. A *cell* of M is a pair $(i, j) \in R \times C$ and an *entry* of M is a triple $(i, j, M_{i,j}) \in R \times C \times S$. We can identify M with the set of its $|R||C|$ entries. This allows us to use set notation such as $(i, j, \ell) \in M$, which means that $M_{i,j} = \ell$. For example, we can identify the 3×6 Latin rectangle from Figure 2.1 with the set

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

Definition 2.1.5. Let L be a Latin square. A *conjugate*, or *parastrophe*, of L is a Latin square obtained from L by uniformly permuting the elements of each of its entries.

Since there are six permutations of any set of cardinality 3, it follows that every Latin square has six, not necessarily distinct, conjugates. Let L be a Latin square and let L' be a conjugate of L. We label L' by a 1-line permutation corresponding to the permutation applied to the entries of L to obtain L'. So the $(1, 2, 3)$-conjugate of L is itself and the $(2, 1, 3)$-conjugate of L is its matrix transpose. The *row-inverse* of L is its $(1, 3, 2)$-conjugate. We will generally use the term conjugate rather than parastrophe, except when there is the possibility of confusion with the algebraic term conjugate.

Let X be a set. We denote by $\mathrm{Sym}(X)$ the group of permutations of X under composition. We denote by Id_X, or just Id if X is clear, the identity permutation in $\mathrm{Sym}(X)$. Unless otherwise stated, we will display permutations in disjoint cycle notation. This convention will be broken when discussing conjugate labels.

Definition 2.1.6. Let L and L' be Latin squares of order n.

- Suppose that there exists $\theta \in \mathrm{Sym}([n])$ such that

$$L' = \{(\theta(r), \theta(c), \theta(s)) : (r, c, s) \in L\}.$$

  Then L and L' are *isomorphic* and θ is an *isomorphism* from L to L'. Isomorphism is an equivalence relation on the set of Latin squares and the equivalence classes are called *isomorphism classes*.

- Suppose that there exists $\{\alpha, \beta, \gamma\} \subseteq \mathrm{Sym}([n])$ such that

$$L' = \{(\alpha(r), \beta(c), \gamma(s)) : (r, c, s) \in L\}.$$

  Then L and L' are *isotopic* and (α, β, γ) is an *isotopism* from L to L'. Isotopism is an equivalence relation on the set of Latin squares and the equivalence classes are called *isotopism classes*.

- Let Ψ be a 1-line permutation of $\{1, 2, 3\}$ and suppose that (α, β, γ) is an isotopism from L to the Ψ^{-1}-conjugate of L'. Then L and L' are *paratopic* and $(\alpha, \beta, \gamma, \Psi)$ is a *paratopism* from L to L'. Paratopism is an equivalence relation on the set of Latin squares and the equivalence classes are called *species*.

Let L and L' be paratopic Latin squares of order n. If $(\alpha, \beta, \gamma, \Psi)$ is a paratopism from L to L', then L' can be obtained from L by permuting its rows according to α, permuting its columns according to β, permuting its symbols according to γ, and then taking the Ψ-conjugate of the resulting square. See Figure 2.4 for an example of isotopic Latin squares.

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

Figure 2.4: The Latin square on the right in this figure can be obtained from the one on the left by applying the isotopism $((1, 2), \mathrm{Id}, (1, 2, 3, 4, 5, 6))$.

Definition 2.1.7. Let L be a Latin square of order n.

- An *automorphism* of L is an isomorphism from L to itself. The *automorphism group* of L, denoted by $\mathrm{Aut}(L)$, is the set of automorphisms of L under composition.

- An *autotopism* of L is an isotopism from L to itself. The *autotopism group* of L, denoted by $\mathrm{Atp}(L)$, is the set of autotopisms of L under composition.

- An *autoparatopism* of L is a paratopism from L to itself. The *autoparatopism group* of L, denoted by $\mathrm{Apar}(L)$, is the set of autoparatopisms of L under composition.

Definition 2.1.5, Definition 2.1.6, and Definition 2.1.7 all have natural analogs for quasigroups. These will be used in Chapter 6.

If L and L' are paratopic Latin squares, then $\mathrm{Apar}(L)$ and $\mathrm{Apar}(L')$ are isomorphic. Thus, we will say that a species X has autoparatopism group G if $\mathrm{Apar}(L)$ is isomorphic to G for some $L \in X$. Similarly, $\mathrm{Atp}(L)$ and $\mathrm{Atp}(L')$ are isomorphic and so we will say that X has autotopism group G if $\mathrm{Atp}(L)$ is isomorphic to G for some $L \in X$.

2.1.4 Asymptotic and probabilistic notation

Throughout this thesis we will use standard asymptotic notation. Let $f : \mathbb{N} \to \mathbb{R}$ and let $g : \mathbb{N} \to \mathbb{R}$. We say that $f = O(g)$ if there is a positive constant C such that $|f(n)| \leqslant C|g(n)|$ for all sufficiently large n. We say that $f = \Omega(g)$ if there is a positive constant K such that $|f(n)| \geqslant K|g(n)|$ for all sufficiently large n. We say that $f = \Theta(g)$ if $f = O(g)$ and $f = \Omega(g)$. We say that $f = o(g)$ if $f(n)/g(n) \to 0$ as $n \to \infty$.

All probability distributions will be discrete and uniform with $\Pr(\cdot)$ denoting probability. Random objects will be printed in bold.

2.2 Subsquares

In this section, we survey two problems related to subsquares in Latin rectangles. In §2.2.1, we discuss subsquares in random Latin rectangles, and in §2.2.2, we discuss Latin squares that have no proper subsquares.

2.2.1 Subsquares in random Latin rectangles

Throughout this subsection, k and m will be positive integers with $k \leqslant n$ and $m \leqslant \min\{k, n/2\}$. All asymptotics are as $n \to \infty$ with k and m being functions of n. We say that an event happens 'asymptotically almost surely' if the probability of it happening tends to 1 as $n \to \infty$.

Definition 2.2.1. Let $\mathbb{E}_m(k, n)$ denote the expected number of subsquares of order m in a random $k \times n$ Latin rectangle.

This subsection is devoted to surveying what is known about $\mathbb{E}_m(k, n)$.

Definition 2.2.2. A $k \times n$ *partial Latin rectangle* is a $k \times n$ matrix such that each cell is either empty or contains one of n symbols, such that no symbol appears more than once in any row or column.

Adopting a similar convention as for Latin rectangles, we will assume, unless otherwise stated, that the row index set of a $k \times n$ partial Latin rectangle is $[k]$ and the column index set and symbol set are $[n]$. Let P be a $k \times n$ partial Latin rectangle. The entries of P are the triples $(r, c, P_{r,c})$ where cell (r, c) is non-empty. As for Latin rectangles, we can identify a partial Latin rectangle with the set of its entries. Let $|P|$ denote the number of entries of P. Say that a $k \times n$ Latin rectangle L *contains* P, denoted $L \supseteq P$, if L contains each entry of P.

Godsil and McKay wrote a seminal paper [55] regarding subsquares in random Latin rectangles. One of their most important results is the following theorem.

Theorem 2.2.3. *Let P be a $k \times n$ partial Latin rectangle and let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. Let r denote the maximum number of non-empty entries that occur in any row of P. If $r \leqslant n - 5k$, then*

$$\Pr(\mathbf{L} \supseteq P) = n^{-|P|} \exp\left(O\left(\frac{k|P|}{n - 2k + 1 - r}\right)\right).$$

Suppose, temporarily, that $k \leqslant n/6$. Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle, let $R \subseteq [k]$ be of cardinality m, let C and S be subsets of $[n]$ of cardinality m, and let M be a Latin square of order m with row indices R, column indices C, and symbol set S. Let P be the $k \times n$ partial Latin rectangle such that $P[R, C] = M$ and every cell of P outside of $R \times C$ is empty. Then Theorem 2.2.3 implies that

$$\Pr(\mathbf{L} \supseteq P) = n^{-m^2} \exp\left(O\left(\frac{km^2}{n - 2k + 1 - m}\right)\right).$$

There are $\binom{k}{m}\binom{n}{m}^2 \leqslant (en/m)^{3m}$ ways to choose the sets R, C, and S and trivially at most m^{m^2} choices for M. Hence,

$$\begin{aligned}\mathbb{E}_m(k, n) &\leqslant m^{m^2}\binom{k}{m}\binom{n}{m}^2 n^{-m^2} \exp\left(O\left(\frac{km^2}{n - 2k + 1 - m}\right)\right) \qquad (2.1)\\ &\leqslant \exp\left((m^2 - 3m)\log\left(\frac{m}{n}\right) + O(m) + O\left(\frac{m^2 k}{n}\right)\right).\end{aligned}$$

In particular, $\mathbb{E}_m(k, n) = o(n^{-(4-\epsilon)})$ for any $\epsilon > 0$ when $m \geqslant 4$. Combining this with Markov's inequality proves that $\mathbf{L}$ asymptotically almost surely contains no proper subsquare of order 4 or more. Similar arguments as used to derive (2.1) combined with the fact that there are two Latin squares of order 2 can be used to obtain

$$\mathbb{E}_2(k, n) = 2\binom{k}{2}\binom{n}{2}^2 n^{-4} \exp\left(O\left(\frac{k}{n}\right)\right) = \frac{1}{2}\binom{k}{2} \exp\left(O\left(\frac{k}{n}\right)\right).$$

Similarly, since there are 12 Latin squares of order 3,

$$\mathbb{E}_3(k, n) = \frac{1}{3n^3}\binom{k}{3} \exp\left(O\left(\frac{k}{n}\right)\right).$$

So Theorem 2.2.3 tells us a lot about subsquares in $k \times n$ Latin rectangles with $k \leqslant n/6$. Of course, we would also like to know about subsquares in 'thicker' Latin rectangles, including Latin squares.

The first researchers to study subsquares of random Latin squares were McKay and Wanless [90]. They made the following conjectures.

Conjecture 2.2.4.

(i) Asymptotically almost surely a random Latin square of order n contains no proper sub-

square of order 4 or more.

(ii) $\mathbb{E}_3(n,n) = 1/18 + o(1)$.

They also provided estimates for the number of intercalates in random Latin squares and conjectured that $\mathbb{E}_2(n,n) = (1+o(1))n^2/4$. Their estimates were subsequently improved in [27, 76, 77, 78], leading to the following result.

Theorem 2.2.5. *Let* $\mathbf{N}$ *denote the number of intercalates in a random Latin square of order* n.

- *The expected value of* $\mathbf{N}$ *is* $\mathbb{E}_2(n,n) = (1+o(1))n^2/4$.
- $\Pr(\mathbf{N} \leqslant (1-\delta)n^2/4) = \exp(-\Theta(n^2))$ *for every* $\delta \in (0,1]$.
- $\Pr(\mathbf{N} \geqslant (1+\delta)n^2/4) = \exp(-\Theta(n^{4/3}\log n))$ *for every* $\delta > 0$.

After two decades of no progress on Conjecture 2.2.4, two research groups were able to prove a relaxation of Conjecture 2.2.4(i) for large subsquares. Divoux, Kelly, Kennedy and Sidhu [39] proved the following theorem.

Theorem 2.2.6. *There is a constant* $K > 0$ *such that asymptotically almost surely a random Latin square of order* n *contains no proper subsquare of order* $K(n\log n)^{1/2}$ *or more.*

Independently, Gill, Mammoliti, and Wanless [53] proved the following theorem, which is slightly weaker than Theorem 2.2.6.

Theorem 2.2.7. *For any* $\epsilon > 0$, *asymptotically almost surely a random Latin square of order* n *contains no proper subsquare of order* $n^{1/2}\log^{1/2+\epsilon} n$ *or more.*

Gill, Mammoliti, and Wanless [53] used Theorem 2.2.7 to prove that testing whether two random Latin squares are isotopic can be done in average-case polynomial time. A *canonical labelling* of a Latin square L of order n is a triple $(\alpha,\beta,\gamma) \in \mathrm{Sym}([n])^3$ such that the Latin square L' obtained from L by applying the isotopism (α,β,γ) depends only on the isotopism class of L. The Latin square L' is the *canonical representative* of L. Let L_1 and L_2 be Latin squares. One way to test whether L_1 and L_2 are isotopic is to construct the canonical representatives L_1' and L_2' of L_1 and L_2, respectively, and check whether $L_1' = L_2'$. Gill, Mammoliti, and Wanless designed an algorithm which, given a Latin square L, builds a canonical labelling of L. An obstruction to efficiently producing this labelling is the presence of large subsquares in L. Theorem 2.2.7 allowed them to prove that a canonical labelling of a Latin square can be produced in average-case polynomial time, thus, testing whether two random Latin squares are isotopic can be done in average-case polynomial time.

Divoux et al. [39] made the following generalisation of Conjecture 2.2.4.

Conjecture 2.2.8.

(i) Asymptotically almost surely a random $k \times n$ *Latin rectangle contains no proper subsquare of order 4 or more.*

(ii) $\mathbb{E}_3(k,n) = (1+o(1))\binom{k}{3}/(3n^3)$.

Conjecture 2.2.8 is implied by a more general conjecture that appeared in the same paper [39]. Let $\epsilon > 0$ and let P be a $k \times n$ partial Latin rectangle. If every row and column of P contains at most ϵn non-empty entries and every symbol appears in at most ϵn cells of P, then P is called *ϵ-dense*.

Conjecture 2.2.9. *Let $\delta \in (0,1)$ and let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. There is an $\epsilon > 0$ such that if P is an ϵ-dense $k \times n$ partial Latin rectangle then*

$$\left(\frac{1-\delta}{n}\right)^{|P|} \leqslant \Pr(\mathbf{L} \supseteq P) \leqslant \left(\frac{1+\delta}{n}\right)^{|P|}$$

for sufficiently large n.

Divoux et al. [39] proved Conjecture 2.2.9 for $k \leqslant (1/2 - o(1))n$. This implies that for these values of k, Conjecture 2.2.8 is true and $\mathbb{E}_2(k,n) = (1/2 + o(1))\binom{k}{2}$.

In Chapter 3, we prove Conjecture 2.2.8(i) and thus also Conjecture 2.2.4(i). We also make the first progress on Conjecture 2.2.8(ii) for $k \geqslant (1/2 - o(1))n$ and give asymptotics for $\mathbb{E}_2(k,n)$ for all $k \leqslant n$.

2.2.2 Latin squares without proper subsquares

Definition 2.2.10.

- An N_2 Latin square is a Latin square with no intercalates.
- An N_∞ Latin square is a Latin square with no proper subsquares.

Kotzig, Lindner, and Rosa [74] defined N_2 Latin squares in 1975. They proved that an N_2 Latin square of order n exists whenever n is not a power of 2 and they asked whether the only orders for which an N_2 Latin square does not exist are 2 and 4. In that same year, McLeish [93] proved the existence of an N_2 Latin square of order 2^a for all $a \geqslant 6$. Later, Regener found an N_2 Latin square of order 8, which was published in a 1976 paper by Kotzig and Turgeon [75]. In that same paper, Kotzig and Turgeon gave a construction of N_2 Latin squares of various orders including 16 and 32. Thus, the existence problem for N_2 Latin squares was resolved.

Theorem 2.2.11. *There exists an N_2 Latin square of order n for all $n \notin \{2,4\}$.*

Recently, Kwan, Sah, Sawhney, and Simkin [77] proved a strong asymptotic lower bound on the number of N_2 Latin squares.

Theorem 2.2.12. *There are at least*

$$\left(e^{-9/4}n - o(n)\right)^{n^2}$$

N_2 Latin squares of order n.

Comparatively much less was known about N_∞ Latin squares. In 1974, Hilton made the following conjecture.

Conjecture 2.2.13. *There exists an N_∞ Latin square of order n for all sufficiently large n.*

Conjecture 2.2.13 was first stated (incorrectly) in [31]. The first progress on Conjecture 2.2.13 came from Heinrich in 1980 [60]. She constructed N_∞ Latin squares of orders pq for all distinct primes p and q with $pq \neq 6$. Two years later, Andersen and Mendelsohn [8] generalised Heinrich's construction to build N_∞ Latin squares of all orders not of the form 2^a3^b with a and b non-negative integers. A third infinite family of N_∞ Latin squares was constructed by Maenhaut, Wanless, and Webb [85] in 2007. They constructed N_∞ squares of all orders $3m$ where m is an odd integer. In particular, they resolved the existence problem for N_∞ squares of orders that are a power of 3. There has also been work done on constructing N_∞ Latin squares of small orders [47, 52, 115, 117]. Combining all of these results we obtain the following existence theorem for N_∞ Latin squares.

Theorem 2.2.14. *There exists an N_∞ Latin square of order n for all positive integers n not of the form $2^a3^b \geqslant 256$ where a is a positive integer and b is a non-negative integer.*

In Chapter 4, we resolve the existence problem for N_∞ Latin squares, proving Conjecture 2.2.13.

2.3 Subrectangles

In this section, we survey some problems related to subrectangles of Latin squares. In §2.3.1, we discuss the relationship between Latin squares and 1-factorisations of complete bipartite graphs. In §2.3.2, §2.3.3, and §2.3.4, we discuss various problems regarding subrectangles of Latin squares and we consider the corresponding problems for 1-factorisations of complete bipartite graphs.

2.3.1 Latin squares and 1-factorisations

Let Γ be a graph. We denote by $V(\Gamma)$ the vertex set of Γ and by $E(\Gamma)$ the edge set of Γ. The *order* of Γ is $|V(\Gamma)|$. A 1-*factor*, or *perfect matching*, of Γ is a subset $M \subseteq E(\Gamma)$ such that every vertex in $V(\Gamma)$ is incident to exactly one edge in M.

Definition 2.3.1. A 1-*factorisation* of a graph Γ is a partition of $E(\Gamma)$ into 1-factors.

For a graph Γ to have a 1-factorisation, it is necessary that Γ is regular and $|V(\Gamma)|$ is even. However, these conditions are not sufficient. For example, the Petersen graph is a 3-regular graph on 10 vertices and it does not have a 1-factorisation.

Let Γ be a graph and suppose that $\mathcal{F}$ is a 1-factorisation of Γ. Let ϕ be a permutation of $V(\Gamma)$. For $f \in \mathcal{F}$, by $\phi(f)$ we mean $\{\{\phi(x), \phi(y)\} : \{x, y\} \in f\}$. By $\phi(\mathcal{F})$ we mean $\{\phi(f) : f \in \mathcal{F}\}$.

Definition 2.3.2. Let Γ be a graph and suppose that $\mathcal{F}_1$ and $\mathcal{F}_2$ are 1-factorisations of Γ.

- If there is a permutation θ of $V(\Gamma)$ such that $\theta(\mathcal{F}_1) = \mathcal{F}_2$, then $\mathcal{F}_1$ and $\mathcal{F}_2$ are *isomorphic* and θ is an *isomorphism* from $\mathcal{F}_1$ to $\mathcal{F}_2$. Isomorphism is an equivalence relation on the set of 1-factorisations of Γ and the equivalence classes are called *isomorphism classes*.
- An *automorphism* of $\mathcal{F}_1$ is an isomorphism from $\mathcal{F}_1$ to itself. The *automorphism group* of $\mathcal{F}_1$, denoted by $\mathrm{Aut}(\mathcal{F}_1)$, is the set of all automorphisms of $\mathcal{F}_1$ under composition.

Isomorphic 1-factorisations have isomorphic automorphism groups.

In this section, we are mostly concerned with 1-factorisations of complete bipartite graphs. The following definition will be convenient for us to describe the relationship between Latin squares and 1-factorisations of complete bipartite graphs.

Definition 2.3.3. Let Γ be a bipartite graph. Let $V(\Gamma) = U \cup W$ with bipartition (U, W). An *ordered* 1-*factorisation* of Γ is a 1-factorisation of Γ together with: a designation of U or W being the first part of Γ, a total order on U, a total order on W, and a total order on the 1-factors in $\mathcal{F}$.

Let Γ be a bipartite graph with vertex set $U \cup W$ with bipartition (U, W). We use $[f_1, f_2, \ldots, f_a]$ to denote an ordered 1-factorisation of Γ with 1-factors $f_1, f_2, \ldots, f_a$. Technically, to form an ordered 1-factorisation of Γ we also require a designation of U or W being the first part, a total order on U, and a total order on V. However, in many situations these requirements are unimportant and will not be specified.

In this section, various properties of 1-factorisations are defined. These properties will be extended to ordered 1-factorisations of bipartite graphs in a natural way: We will say that an ordered 1-factorisation has such a property if the corresponding unordered 1-factorisation has that property.

We will need the notions of isomorphisms and automorphisms for ordered 1-factorisations of bipartite graphs.

Definition 2.3.4. Let Γ be a bipartite graph and let $\mathcal{F} = [f_1, f_2, \ldots, f_n]$ and $\mathcal{F}' = [f'_1, f'_2, \ldots, f'_n]$ be ordered 1-factorisations of Γ.

- If there is a permutation θ of $V(\Gamma)$ and a permutation ψ of $[n]$ such that $\theta(f_i) = f'_{\psi(i)}$ for all $i \in [n]$, then $\mathcal{F}$ and $\mathcal{F}'$ are *ordered isomorphic* and (θ, ψ) is an *ordered isomorphism* from $\mathcal{F}$ to $\mathcal{F}'$. In this case we write $\mathcal{F}' = \mathcal{F}\langle\theta, \psi\rangle$. Ordered isomorphism is an equivalence relation on the set of ordered 1-factorisations of Γ and the equivalence classes are called isomorphism classes.

- An *ordered automorphism* of $\mathcal{F}$ is an ordered isomorphism from $\mathcal{F}$ to itself. The *ordered automorphism group* of $\mathcal{F}$, denoted by $\mathrm{OAut}(\mathcal{F})$, is the set of all ordered automorphisms of $\mathcal{F}$ under composition.

Let $\mathcal{F} = [f_1, f_2, \ldots, f_a]$ and $\mathcal{F}' = [f'_1, f'_2, \ldots, f'_a]$ be ordered 1-factorisations of a bipartite graph Γ. Then $\mathcal{F}$ and $\mathcal{F}'$ are ordered isomorphic if and only if the unordered 1-factorisations $\{f_1, f_2, \ldots, f_a\}$ and $\{f'_1, f'_2, \ldots, f'_a\}$ of Γ are isomorphic.

There is a nice equivalence between Latin squares of order n and ordered 1-factorisations of $K_{n,n}$, which we now briefly discuss. For a more detailed description, see, for example, [121]. Let $\mathcal{F}$ be an ordered 1-factorisation of $K_{n,n}$ and let the vertex set of $K_{n,n}$ be $U \cup W$ with bipartition (U, W). Since $\mathcal{F}$ is ordered, there is a designation of one of U or W as the first part of $K_{n,n}$. Without loss of generality, U is the first part. There is also a total order on U and a total order on W. Hence, we may relabel U to be $[n] \times \{1\}$ and we may relabel W to be $[n] \times \{2\}$. For the remainder of this section, unless otherwise stated, we will assume that the vertex set of $K_{n,n}$ is $([n] \times \{1\}) \cup ([n] \times \{2\})$ with bipartition $([n] \times \{1\}, [n] \times \{2\})$. We will always use the natural total order on $[n] \times \{1\}$ and $[n] \times \{2\}$, and $[n] \times \{1\}$ will be designated as the first part.

Let L be a Latin square of order n. For each $r \in [n]$, define a set f_r of edges of $K_{n,n}$ by $f_r = \{\{(c,1),(L_{r,c},2)\} : c \in [n]\}$. Since no symbol appears more than once in row r of L, it follows that f_r is a 1-factor of $K_{n,n}$. Define $\mathcal{F} = [f_1, f_2, \ldots, f_n]$. The fact that no symbol appears more than once in any column of L implies that if $r \neq r'$, then f_r and $f_{r'}$ are disjoint. Thus, $\mathcal{F}$ is an ordered 1-factorisation of $K_{n,n}$. Let the ordered 1-factorisation $\mathcal{F}$ obtained from L in this way be denoted by $\mathscr{F}(L)$.

Conversely, let $\mathcal{F} = [f_1, f_2, \ldots, f_n]$ be an ordered 1-factorisation of $K_{n,n}$. We will define a matrix L of order n with row index set, column index set, and symbol set $[n]$, by letting $L_{r,c}$ be the unique element $s \in [n]$ such that $(s,2)$ is adjacent to $(c,1)$ in f_r. The definition of a 1-factor implies that no symbol is repeated in any row of L, and the fact that f_r and $f_{r'}$ are disjoint for any $r \neq r'$ implies that no symbol is repeated in any column of L. Hence, L is a Latin square. Let the Latin square obtained from $\mathcal{F}$ in this way be denoted by $\mathscr{L}(\mathcal{F})$. Note that if ψ is a permutation of $[n]$ and $\mathcal{F}' = \mathcal{F}\langle \mathrm{Id}, \psi\rangle$, then $\mathscr{L}(\mathcal{F}')$ and $\mathscr{L}(\mathcal{F})$ are isotopic and $(\psi, \mathrm{Id}, \mathrm{Id}) \in \mathrm{Sym}([n])^3$ is an isotopism from $\mathscr{L}(\mathcal{F}')$ to $\mathscr{L}(\mathcal{F})$. Also note that $\mathscr{F}(\mathscr{L}(\mathcal{F})) = \mathcal{F}$.

Of course, if L is a Latin square of order n with general row indices R, column indices C, and symbols S, then we can still define an ordered 1-factorisation $\mathscr{F}(L)$ of $K_{n,n}$ by relabelling R, C, and S. The order of the 1-factors in $\mathscr{F}(L)$ comes from the order on R and the orders on the parts of $K_{n,n}$ come from the orders on C and S. This is the reason for the insistence in §2.1.1 of a total order on the symbol set of a Latin rectangle. Similarly, we can of course define $\mathscr{L}(\mathcal{F})$ for any ordered 1-factorisation $\mathcal{F}$ of a complete bipartite graph by relabelling vertices and 1-factors.

See Figure 2.5 for an example of a Latin square L and its associated ordered 1-factorisation $\mathscr{F}(L)$.

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

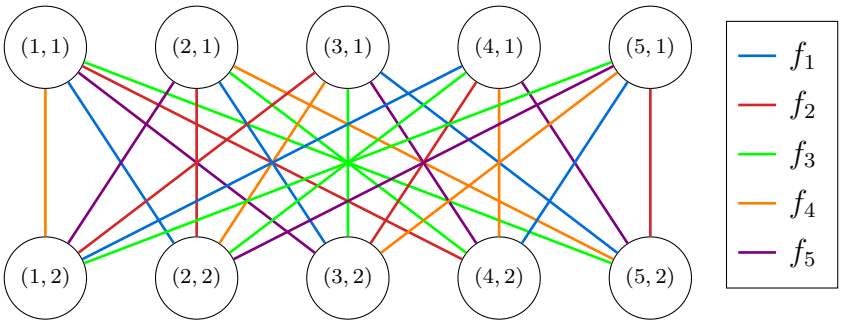

Figure 2.5: A Latin square L of order 5 and its associated ordered 1-factorisation $\mathscr{F}(L)$ of $K_{5,5}$. In this figure, a 1-factor is a maximal set of edges of the same colour.

Let $\mathcal{F}$ be an ordered 1-factorisation of $K_{n,n}$ and let $(\theta, \psi) \in \mathrm{OAut}(\mathcal{F})$. Let $U = [n] \times \{1\}$ and let $W = [n] \times \{2\}$. Then either $\theta(U) = U$ or $\theta(U) = W$. In the former case we say that (θ, ψ) is *part-preserving* and in the latter case we say that (θ, ψ) is *part-reversing*. We denote the set of part-preserving ordered automorphisms of $\mathcal{F}$ by $\mathrm{OAut}_{\mathrm{p}}(\mathcal{F})$. Let $L = \mathscr{L}(\mathcal{F})$.

Permuting the vertices in U corresponds to a permutation of the columns of L, permuting the vertices in W corresponds to a permutation of the symbols of L, and permuting the 1-factors in $\mathcal{F}$ corresponds to a permutation of the rows of L. We thus have the following theorem [121].

Theorem 2.3.5. *Let $\mathcal{F}$ and $\mathcal{F}'$ be ordered 1-factorisations of $K_{n,n}$. Let $L = \mathscr{L}(\mathcal{F})$ and let $L' = \mathscr{L}(\mathcal{F}')$.*

- $\mathrm{OAut_p}(\mathcal{F})$ *is isomorphic to* $\mathrm{Atp}(L)$.
- *$\mathcal{F}$ and $\mathcal{F}'$ are ordered isomorphic if and only if L is isotopic to L' or the row-inverse of L'.*

We now relate subrectangles of Latin squares to properties of 1-factorisations of complete bipartite graphs.

Definition 2.3.6. Let L be a Latin square of order n. A *row cycle of length ℓ* in L is a $2 \times \ell$ subrectangle of L that does not have any proper subrectangles.

The following simple lemma is due to Wanless [116].

Lemma 2.3.7. *Let L and L' be Latin squares. Let X and X' be the set of lengths of row cycles of L and L', respectively. If there is a paratopism $(\alpha, \beta, \gamma, \Psi)$ from L to L' with $\Psi \in \{(1,2,3),(1,3,2)\}$, then $X = X'$.*

Let Γ be a graph and let $M \subseteq E(\Gamma)$. Denote by $\Gamma[M]$ the subgraph of Γ with vertex set $V(\Gamma)$ and edge set M. Suppose that $\mathcal{F}$ is a 1-factorisation of Γ. Let $\{f, g\} \subseteq \mathcal{F}$ with $f \neq g$. It is simple to see that $\Gamma[f \cup g]$ is a union of cycles of even length. We will say that $\mathcal{F}$ *contains* a cycle of length 2ℓ if there are distinct 1-factors f and g in $\mathcal{F}$ such that $\Gamma[f \cup g]$ has a cycle of length 2ℓ. The following lemma [121] relates the row cycles of a Latin square L to the cycles that $\mathscr{F}(L)$ contains.

Lemma 2.3.8. *Let $\mathcal{F} = [f_1, f_2, \ldots, f_n]$ be an ordered 1-factorisation of $K_{n,n}$ and let $L = \mathscr{L}(\mathcal{F})$. Let $\{i, j\} \subseteq [n]$ with $i \neq j$. The Latin square L contains a row cycle of length ℓ involving rows i and j if and only if the graph $K_{n,n}[f_i \cup f_j]$ contains a cycle of length 2ℓ.*

2.3.2 Row-Hamiltonian Latin squares and perfect 1-factorisations

Definition 2.3.9. A Latin square is *row-Hamiltonian* if it does not contain any proper subrectangles.

The row-Hamiltonian property is much stronger than the N_∞ property. The following is a characterisation of row-Hamiltonian Latin squares: A Latin square of order n is row-Hamiltonian if and only if all of its row cycles are of dimension $2 \times n$. Thus, Lemma 2.3.7 implies that the row-Hamiltonian property is an isotopism class invariant.

Definition 2.3.10. Let Γ be a graph. A *perfect 1-factorisation* of Γ is a 1-factorisation $\mathcal{F}$ of Γ such that $\Gamma[f \cup g]$ is a Hamiltonian cycle in Γ for any distinct f and g in $\mathcal{F}$.

It is a simple fact that the perfect property of a 1-factorisation is an isomorphism class invariant.

Combining Lemma 2.3.8 with the characterisation of row-Hamiltonian Latin squares given after Definition 2.3.9, we obtain the following theorem (see, e.g., [121]).

Theorem 2.3.11. *Let $\mathcal{F}$ be an ordered 1-factorisation of $K_{n,n}$ and let $L = \mathscr{L}(\mathcal{F})$. Then L is row-Hamiltonian if and only if $\mathcal{F}$ is perfect.*

The Latin square depicted in Figure 2.5 is row-Hamiltonian, thus the ordered 1-factorisation depicted in Figure 2.5 is perfect.

The main point of this subsection is to discuss what is known about row-Hamiltonian Latin squares and perfect 1-factorisations of complete bipartite graphs. Before doing this, we take a slight detour to discuss perfect 1-factorisations of complete graphs.

In 1964, Kotzig made the following famous conjecture [73].

Conjecture 2.3.12. *There exists a perfect 1-factorisation of the complete graph K_n for every even integer n.*

Despite attracting lots of attention, Conjecture 2.3.12 remains far from resolved. There are three known infinite families of perfect 1-factorisations of complete graphs. In 1964, Kotzig [73] proved, for every odd prime p, the existence of a perfect 1-factorisation of K_{p+1}, denoted by GK_{p+1}. For each odd prime p, there is a well known 1-factorisation of K_{2p}, denoted by GA_{2p}. Kotzig also claimed to know that GA_{2p} is perfect for every odd prime p. This fact was proved by Anderson [9] in 1973. The third known infinite family was not constructed until 2006, when Bryant, Maenhaut, and Wanless [22] constructed, for every prime $p \geqslant 11$, a perfect 1-factorisation of K_{p+1} that is not isomorphic to GK_{p+1}. Denote this perfect 1-factorisation by GB_{p+1}. There has also been plenty of work done on constructing perfect 1-factorisations of complete graphs of small order [10, 11, 12, 14, 38, 66, 70, 71, 102, 109, 110, 120, 123]. Combining all of the results discussed above gives rise to the following existence theorem.

Theorem 2.3.13. *There exists a perfect 1-factorisation of K_n if $n \in \{p+1, 2p\}$ for an odd prime p or if n is an element of*

$$\{16, 28, 36, 40, 50, 52, 56, 126, 170, 244, 344, 530, 730, 1332, 1370, 1850, 2198, 2810, 3126,$$
$$4490, 6860, 6890, 11\,450, 11\,882, 12\,168, 15\,626, 16\,808, 22\,202, 24\,390, 24\,650, 26\,570, 29\,792,$$
$$29\,930, 32\,042, 38\,810, 44\,522, 50\,654, 51\,530, 52\,442, 63\,002, 72\,362, 76\,730, 78\,126, 79\,508,$$
$$103\,824, 148\,878, 161\,052, 205\,380, 226\,982, 300\,764, 357\,912, 371\,294, 493\,040, 571\,788,$$
$$1\,030\,302, 1\,092\,728, 1\,225\,044, 1\,295\,030, 2\,048\,384, 2\,248\,092, 2\,476\,100, 2\,685\,620, 3\,307\,950,$$
$$3\,442\,952, 4\,330\,748, 4\,657\,464, 5\,735\,340, 6\,436\,344, 6\,967\,872, 7\,880\,600, 9\,393\,932, 11\,089\,568,$$
$$11\,697\,084, 13\,651\,920, 15\,813\,252, 18\,191\,448, 19\,902\,512, 22\,665\,188\}.$$

It is unknown whether there exists a perfect 1-factorisation of K_{64}. This represents the smallest unresolved case of Conjecture 2.3.12.

There has also been work done on enumerating perfect 1-factorisations of complete graphs of small order. The number of 1-factorisations of K_n up to isomorphism and the number of those that are perfect are given in Table 2.1 for some small relevant values of n.

The number of isomorphism classes of 1-factorisations of K_n was determined by: Dickson and Safford [33] for $n = 8$; Gelling and Odeh [51] for $n = 10$; Dinitz, Garnick, and McKay [37] for $n = 12$; and Kaski and Östergård [67] for $n = 14$. The number of isomorphism classes of 1-factorisations of K_{16} is unknown. The number of isomorphism classes of perfect 1-factorisations of K_n was determined by: Gelling and Odeh [51] for $n = 10$; Petrenyuk and Petrenyuk [101]

n	1-factorisations	perfect 1-factorisations
2	1	1
4	1	1
6	1	1
8	6	1
10	396	1
12	526 915 620	5
14	1 132 835 421 602 062 347	23
16		3155

Table 2.1: The number of 1-factorisations and perfect 1-factorisations up to isomorphism of K_n for small values of n.

for $n = 12$; Dinitz and Garnick [36] for $n = 14$; and Gill and Wanless [54], and independently Meszka [95], for $n = 16$.

For more details about perfect 1-factorisations of complete graphs, see the surveys [104, 108].

We now give a brief description of the relationship between perfect 1-factorisations of complete graphs and perfect 1-factorisations of complete bipartite graphs. For a more detailed description, see [121].

Definition 2.3.14. Suppose that n is odd and let the vertex set of K_{n+1} be V. An *ordered 1-factorisation of* K_{n+1} is a 1-factorisation $\mathcal{F}$ of K_{n+1} together with a total order on V and a total order on the 1-factors in $\mathcal{F}$. A *rooted 1-factorisation of* K_{n+1} is a pair $(\mathcal{F}, v)$ where $\mathcal{F}$ is an ordered 1-factorisation of K_{n+1} and $v \in V$ is a vertex called the *root*.

As we did for bipartite graphs, we will use $[f_1, f_2, \ldots, f_n]$ to denote an ordered 1-factorisation of K_{n+1} with 1-factors $f_1, f_2, \ldots, f_n$. Technically, to form an ordered 1-factorisation we also need to specify an order on $V(K_{n+1})$. However, in many situations this information will be unimportant and thus omitted. We will also extend properties of 1-factorisations to ordered 1-factorisations of complete graphs in the same way as we extended those properties to ordered 1-factorisations of complete bipartite graphs.

There is a known method of building an ordered 1-factorisation of $K_{n,n}$ from a rooted 1-factorisation $(\mathcal{F}, v)$ of K_{n+1}, called the $\mathbb{K}$-construction. Let $V = V(K_{n+1})$. Define $U = (V \setminus \{v\}) \times \{1\}$ and $W = (V \setminus \{v\}) \times \{2\}$. Let the vertex set of $K_{n,n}$ be $U \cup W$ with bipartition (U, W). Designate U to be the first part of $K_{n,n}$. The total order on V induces a total order on U and a total order on W. Let $\mathcal{F} = [f_1, f_2, \ldots, f_n]$. For each 1-factor $f_i \in \mathcal{F}$, build a 1-factor f_i^* of $K_{n,n}$ as follows. Let $x \in V$ be the unique vertex such that $\{x, v\} \in f_i$. Add the edge $\{(x, 1), (x, 2)\}$ to f_i^*. For all edges $\{a, b\} \in f_i$ with $v \notin \{a, b\}$, add the edges $\{(a, 1), (b, 2)\}$ and $\{(a, 2), (b, 1)\}$ to f_i^*. It is routine to check that f_i^* is a 1-factor and $[f_1^*, f_2^*, \ldots, f_n^*]$ is an ordered 1-factorisation of $K_{n,n}$. Denote this ordered 1-factorisation by $\mathcal{K}(\mathcal{F}, v)$. For the rest of this subsection, if f is a 1-factor of K_{n+1}, then f^* will denote the 1-factor of $K_{n,n}$ built from f as described above. See Figure 2.6 for an example of the $\mathbb{K}$-construction.

Let $(\mathcal{F}, v)$ be a rooted 1-factorisation of K_{n+1}. Let $\mathcal{K} = \mathcal{K}(\mathcal{F}, v)$ and let f and g be distinct 1-factors in $\mathcal{F}$. Suppose that $(x_1, x_2, \ldots, x_j)$ is a cycle in $K_{n+1}[f \cup g]$ that does not contain

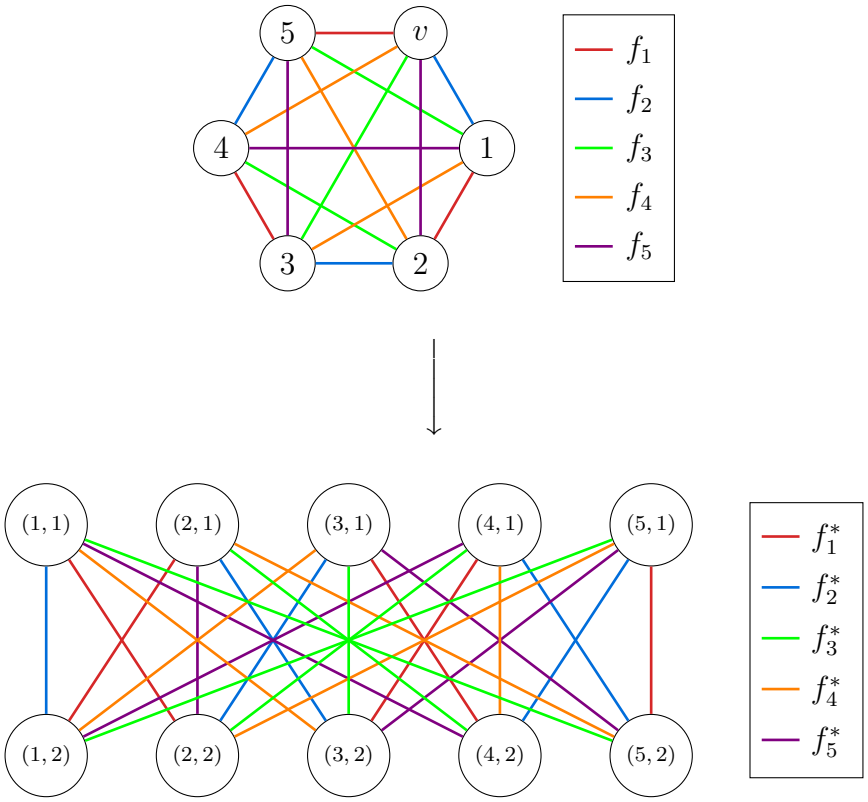

Figure 2.6: This figure shows an ordered 1-factorisation $\mathcal{F}$ of K_6 and the ordered 1-factorisation $\mathcal{K}(\mathcal{F}, v)$ of $K_{5,5}$.

vertex v. Note that j must be even. Then $K_{n,n}[f^* \cup g^*]$ contains the cycles

$$((x_1, 1), (x_2, 2), \ldots, (x_{j-1}, 1), (x_j, 2)) \text{ and } ((x_1, 2), (x_2, 1), \ldots, (x_{j-1}, 2), (x_j, 1)).$$

Now suppose that $(v, x_1, x_2, \ldots, x_j)$ is a cycle in $K_{n+1}[f \cup g]$ and note that j must be odd. Then $K_{n,n}[f^* \cup g^*]$ contains the cycle

$$((x_1, 1), (x_2, 2), \ldots, (x_{j-1}, 2), (x_j, 1), (x_j, 2), (x_{j-1}, 1), \ldots, (x_2, 1), (x_1, 2)).$$

We thus have the following theorem [121].

Theorem 2.3.15. *Let $(\mathcal{F}, v)$ be a rooted 1-factorisation of K_{n+1} and let $\mathcal{K} = \mathcal{K}(\mathcal{F}, v)$. Then $\mathcal{K}$ is perfect if and only if $\mathcal{F}$ is perfect.*

An immediate corollary of Theorem 2.3.15 is the following.

Corollary 2.3.16. *If there exists a perfect 1-factorisation of K_{n+1}, then there exists a perfect 1-factorisation of $K_{n,n}$.*

Corollary 2.3.16 was first proved by Laufer [79]. The converse to Corollary 2.3.16 is not known to hold in general, but there is a known partial converse, which we discuss now.

Let L be a Latin square of order n. If $L_{i,i} = i$ for all $i \in [n]$, then L is *idempotent*. If L is equal to its row-inverse, then L is *involutory*.

If n is odd, then given a rooted 1-factorisation $(\mathcal{F}, v)$ of K_{n+1} we can construct a 1-factorisation $\mathcal{K}(\mathcal{F}, v)$ of $K_{n,n}$ and then a Latin square $\mathscr{L}(\mathcal{K}(\mathcal{F}, v))$ of order n. For simplicity,

we will denote $\mathscr{L}(\mathcal{K}(\mathcal{F}, v))$ by $\mathscr{L}(\mathcal{F}, v)$. If we start with an idempotent and involutory Latin square, then we can reverse this construction to obtain an ordered 1-factorisation of K_{n+1}. Note that an idempotent, involutory Latin square of order n can exist only if n is odd.

Suppose that n is odd and let L be an idempotent, involutory Latin square of order n. Let the vertex set of K_{n+1} be $[n+1]$. For each $r \in [n]$, build a set g_r of edges of K_{n+1} as follows. Add the edge $\{r, n+1\}$ to g_r, and for each $c \in [n] \setminus \{r\}$, add the edge $\{c, L_{r,c}\}$ to g_r. Then g_r is well-defined because L is idempotent and involutory. Furthermore, the fact that every symbol in $[n]$ appears exactly once in each row and column of L implies that $[g_1, g_2, \ldots, g_n]$ is an ordered 1-factorisation of K_{n+1}, which we denote by $\mathscr{G}(L)$. Here we are using the natural total order on $[n+1] = V(K_{n+1})$. Note that $L = \mathscr{L}(\mathscr{G}(L), n+1)$. The following lemma [2] relates the row cycles of L to the cycles in $\mathscr{G}(L)$.

Lemma 2.3.17. *Suppose that n is odd. Let L be an idempotent, involutory Latin square of order n and let $\mathcal{F} = \mathscr{G}(L) = [g_1, g_2, \ldots, g_n]$. Let $\{i, j\} \subseteq [n]$ with $i \neq j$ and let $\mathcal{D}$ be a row cycle of length ℓ in L involving rows i and j.*

- *If $\mathcal{D}$ hits column i, then there is a cycle in $K_{n+1}[g_i, g_j]$ of length $\ell + 1$.*
- *If $\mathcal{D}$ does not hit column i, then $\ell < n/2$ and there is a cycle in $K_{n+1}[g_i, g_j]$ of length 2ℓ.*

We can now state a partial converse to Corollary 2.3.16, which was also stated in [121].

Corollary 2.3.18. *If there exists an idempotent, involutory, row-Hamiltonian Latin square of order n, then there exists a perfect 1-factorisation of K_{n+1}.*

Let $\mathcal{F}$ be an ordered 1-factorisation of K_{n+1} and let $v \in V(K_{n+1})$. A natural question to ask is whether the choice of v can affect the isomorphism class of $\mathcal{K}(\mathcal{F}, v)$ or the species of $\mathscr{L}(\mathcal{F}, v)$. This is answered by the following theorem [121].

Theorem 2.3.19. *Let $\mathcal{F} = [f_1, f_2, \ldots, f_n]$ be an ordered 1-factorisation of K_{n+1} and let $\{u, v\} \subseteq V(K_{n+1})$. Let $\mathcal{F}' = \{f_1, f_2, \ldots, f_n\}$ denote the unordered 1-factorisation of K_{n+1} corresponding to $\mathcal{F}$.*

- *$\mathcal{K}(\mathcal{F}, u)$ and $\mathcal{K}(\mathcal{F}, v)$ are isomorphic if and only if there is an automorphism of $\mathcal{F}'$ that maps u to v.*
- *$\mathscr{L}(\mathcal{F}, u)$ and $\mathscr{L}(\mathcal{F}, v)$ are paratopic if and only if there is an automorphism of $\mathcal{F}'$ that maps u to v.*

We now return to what is known about row-Hamiltonian Latin squares and perfect 1-factorisations of complete bipartite graphs.

A simple parity argument can be used to prove the following lemma [116].

Lemma 2.3.20. *If a row-Hamiltonian Latin square of order n exists, then $n = 2$ or n is odd.*

Combining Conjecture 2.3.12 with Corollary 2.3.16, we obtain the following conjecture (see, e.g., [116]).

Conjecture 2.3.21. *There exists a perfect 1-factorisation of $K_{n,n}$ for every odd integer n.*

There has been more progress on Conjecture 2.3.21 than on Conjecture 2.3.12. However, Conjecture 2.3.21 is still very far from being resolved. Theorem 2.3.13 and Corollary 2.3.16 together imply the existence of perfect 1-factorisations of $K_{n,n}$ for various values of n. Let $p \geqslant 11$ be prime. Applying the $\mathbb{K}$-construction to the 1-factorisations GK_{p+1} and GB_{p+1}, we obtain several non-isomorphic perfect 1-factorisations of $K_{p,p}$. Explicitly, if 2 is primitive modulo p, then there are 11 non-isomorphic perfect 1-factorisations of $K_{p,p}$ obtained in this way, and if 2 is not primitive modulo p, then there are five non-isomorphic perfect 1-factorisations of $K_{p,p}$ obtained in this way. These facts were proved by Bryant, Maenhaut, and Wanless [22]. Corollary 2.3.16 tells us that there are perfect 1-factorisations of $K_{2p-1,2p-1}$ for each odd prime p found by applying the $\mathbb{K}$-construction to GA_{2p}. In Chapter 5, we will prove that only one isomorphism class of perfect 1-factorisations of $K_{2p-1,2p-1}$ can be obtained in this way. There are two known infinite families of perfect 1-factorisations of complete bipartite graphs that do not come from the $\mathbb{K}$-construction. Bryant, Maenhaut, and Wanless [21] constructed $(p-1)/2$ non-isomorphic perfect 1-factorisations of K_{p^2,p^2} for each odd prime p. Allsop and Wanless [5] constructed a perfect 1-factorisation of $K_{p,p}$ for each prime p such that $p \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$. We thus have the following existence result for perfect 1-factorisations of complete bipartite graphs.

Theorem 2.3.22. *There exists a perfect 1-factorisation of $K_{n,n}$ if $n \in \{p, 2p-1, p^2\}$ for an odd prime p or n is an element of*

$\{15, 27, 35, 39, 49, 51, 55, 125, 169, 243, 343, 529, 729, 1331, 1369, 1849, 2197, 2809, 3125,$
$4489, 6859, 6889, 11\,449, 11\,881, 12\,167, 15\,625, 16\,807, 22\,201, 24\,389, 24\,649, 26\,569, 29\,791,$
$29\,929, 32\,041, 38\,809, 44\,521, 50\,653, 51\,529, 52\,441, 63\,001, 72\,361, 76\,729, 78\,125, 79\,507,$
$103\,823, 148\,877, 161\,051, 205\,379, 226\,981, 300\,763, 357\,911, 371\,293, 493\,039, 571\,787,$
$1\,030\,301, 1\,092\,727, 1\,225\,043, 1\,295\,029, 2\,048\,383, 2\,248\,091, 2\,476\,099, 2\,685\,619, 3\,307\,949,$
$3\,442\,951, 4\,330\,747, 4\,657\,463, 5\,735\,339, 6\,436\,343, 6\,967\,871, 7\,880\,599, 9\,393\,931, 11\,089\,567,$
$11\,697\,083, 13\,651\,919, 15\,813\,251, 18\,191\,447, 19\,902\,511, 22\,665\,187\}.$

By Theorem 2.3.11, the integers n for which it is known that a row-Hamiltonian Latin square of order n exists are the same integers n for which Theorem 2.3.22 tells us that a perfect 1-factorisation of $K_{n,n}$ exists. The row-Hamiltonian Latin squares that are obtained from the known infinite families of perfect 1-factorisations of complete bipartite graphs will be discussed in §2.3.4.

There has been work done on enumerating perfect 1-factorisations of complete bipartite graphs, as well as row-Hamiltonian Latin squares, of small orders. For $n \in \{2, 3, \ldots, 11\}$: Table 2.2 shows the number of 1-factorisations of $K_{n,n}$ up to isomorphism and the number of those that are perfect, Table 2.3 shows the number of species of Latin squares of order n and the number of those containing row-Hamiltonian Latin squares, and Table 2.4 shows the number of isotopism classes of Latin squares of order n and the number of those containing row-Hamiltonian Latin squares.

The number of species and isotopism classes of Latin squares of orders up to 6 were determined by Schönhardt [107]. The number of isomorphism classes of 1-factorisations of $K_{6,6}$ was known to Tarry [111] and also apparently to Clausen (see [98]). The number of species of Latin squares of order 7 was determined independently by Sade [105] and Saxena [106]. Sade [105]

n	1-factorisations	perfect 1-factorisations
2	1	1
3	1	1
4	2	—
5	2	1
6	17	—
7	324	2
8	842 227	—
9	57 810 418 543	37
10	104 452 188 344 901 572	—
11	6 108 088 657 705 958 932 053 657	687 121

Table 2.2: The number of 1-factorisations and perfect 1-factorisations up to isomorphism of $K_{n,n}$ for small values of n.

n	species	row-Hamiltonian species
2	1	1
3	1	1
4	2	—
5	2	1
6	12	—
7	147	2
8	283 657	—
9	19 270 853 541	37
10	34 817 397 894 749 939	—
11	2 036 029 552 582 883 134 196 099	687 115

Table 2.3: The number of species and species containing row-Hamiltonian Latin squares of order n for small values of n.

also determined the number of isotopism classes of Latin squares of order 7 (see also [103]). The number of species and isotopism classes of Latin squares of order 8 were determined by Kolesova, Lam, and Thiel [72]. The number of isomorphism classes of 1-factorisations of $K_{7,7}$ and $K_{8,8}$ were determined by McKay, Meynert, and Myrvold [88]. They also determined the number of species and isotopism classes of Latin squares of order n and the number of isomorphism classes of 1-factorisations of $K_{n,n}$ for $n \in \{9, 10\}$. The number of species and isotopism classes of Latin squares of order 11 and the number of isomorphism classes of 1-factorisations of $K_{11,11}$ were determined by Hulpke, Kaski, and Östergård [65]. For positive integers $n \leqslant 9$, the number of species containing row-Hamiltonian Latin squares of order n and the number of isomorphism classes of perfect 1-factorisations of $K_{n,n}$ were determined by Wanless [116]. From his results, it is easy to determine the number of isotopism classes containing row-Hamiltonian Latin squares of order n. The number of species and isotopism classes containing row-Hamiltonian Latin squares of order 11 and the number of isomorphism classes of perfect 1-factorisations of $K_{11,11}$ are the main topics of Chapter 5.

n	isotopism classes	row-Hamiltonian isotopism classes
2	1	1
3	1	1
4	2	—
5	2	1
6	22	—
7	564	2
8	1 676 267	—
9	115 618 721 533	64
10	208 904 371 354 363 006	—
11	12 216 177 315 369 229 261 482 540	1 374 132

Table 2.4: The number of isotopism classes and isotopism classes containing row-Hamiltonian Latin squares of order n for small values of n.

2.3.3 1-factorisations avoiding cycles of certain lengths

Recall that if $\mathcal{F}$ is a 1-factorisation of a graph Γ and $\mathcal{F}$ contains a cycle of length x, then x is even and satisfies $4 \leqslant x \leqslant |V(\Gamma)|$.

Definition 2.3.23. Let Γ be a graph and let x be an even integer satisfying $4 \leqslant x \leqslant |V(\Gamma)|$. An *$x$-cycle free* 1-factorisation of Γ is a 1-factorisation of Γ that does not contain any cycle of length x.

Meszka [94] studied x-cycle free 1-factorisations of complete graphs. One of his main results is the following.

Theorem 2.3.24. *Suppose that n is even and let x be an even integer satisfying $4 \leqslant x < n$. There exists an x-cycle free 1-factorisation of K_n.*

Thus, the only integer x for which it is unknown whether an x-cycle free 1-factorisation of K_n exists is $x = n$.

Definition 2.3.25. Let Γ be a graph. An *anti-perfect 1-factorisation* of Γ is a $|V(\Gamma)|$-cycle free 1-factorisation of Γ.

By Theorem 2.3.24, to resolve the existence problem for x-cycle free 1-factorisations of complete graphs, it remains to resolve the existence problem for anti-perfect 1-factorisations of complete graphs. There has been some work done in this direction, which will be discussed later in this subsection. Before doing this, we will consider 1-factorisations of graphs that do not contain any long cycles.

Let Γ be a graph and let x be an even integer satisfying $4 \leqslant x \leqslant |V(\Gamma)|$. An *$x^>$-cycle free* 1-factorisation of Γ is a 1-factorisation of Γ that is y-cycle free for every even integer y satisfying $x < y \leqslant |V(\Gamma)|$. In 1976, Häggkvist [56] asked the following question. For a graph Γ that has a 1-factorisation, what is the smallest even integer x with $4 \leqslant x \leqslant |V(\Gamma)|$ such that there is an $x^>$-cycle free 1-factorisation of Γ? This question has been studied mostly for the case where Γ is a complete bipartite graph [17, 23, 45, 46, 97, 124], but some attention has also been given to the case where Γ is a complete graph [23, 46]. Dukes and Ling [45] posed the following conjecture.

Conjecture 2.3.26. *There exists a $6^{>}$-cycle free 1-factorisation of $K_{n,n}$ for all sufficiently large n.*

Every 1-factorisation of $K_{5,5}$ has a cycle of length 10, thus the condition in Conjecture 2.3.26 that n must be 'sufficiently large' is necessary. Conjecture 2.3.26 is known to hold when n is a power of 2 or a power of 3 [23, 96, 124]. Ninčák and Owens [97] proved that the minimum x such that there is an $x^{>}$-cycle free 1-factorisation of $K_{n,n}$ is at most $2n-2$ if $n \notin \{2,3,5\}$. That is, they proved that there exists an anti-perfect 1-factorisation of $K_{n,n}$ if $n \notin \{2,3,5\}$. Dukes and Ling [45] improved the bound on x to a polylogarithmic function of n. In a subsequent paper, they improved the bound on x to a constant [46], which was further improved by Benson and Dukes [17].

Theorem 2.3.27. *There exists a $182^{>}$-cycle free 1-factorisation of $K_{n,n}$ for all positive integers n.*

The best known corresponding result for complete graphs is due to Dukes and Ling [46].

Theorem 2.3.28. *There exists a $1720^{>}$-cycle free 1-factorisation of K_n for all even integers n.*

We can now return to anti-perfect 1-factorisations of complete graphs. Meszka [94] gave some existence results for anti-perfect 1-factorisations of complete graphs, but did not resolve the existence problem completely. Combining his results with Theorem 2.3.28 we obtain the following theorem.

Theorem 2.3.29. *Suppose that n is even. There exists an anti-perfect 1-factorisation of K_n except possibly when $102 \leqslant n \leqslant 1720$ and one of the following is true:*

- *$n \equiv z \bmod 24$ for some $z \in \{6, 12, 18\}$,*
- *$n-1$ is prime.*

In Chapter 6, we resolve the existence problem for anti-perfect 1-factorisations of complete graphs. However, we note that our contribution to this is little more than an observation that construction of $x^{>}$-cycle free 1-factorisations of complete graphs by Dukes and Ling [46] can be used to construct anti-perfect 1-factorisations of K_n for almost all even n. By combining the existence result for anti-perfect 1-factorisations of complete graphs with Theorem 2.3.24, we can resolve the existence problem for x-cycle free 1-factorisations of complete graphs. In Chapter 6, we also provide some new methods of constructing anti-perfect 1-factorisations of complete graphs and complete bipartite graphs.

Let L be a Latin square of order n and let $x \in [n] \setminus \{1\}$. Say that L is *x-cycle free* if it has no row cycle of length x. By Lemma 2.3.8, if L is x-cycle free, then $\mathscr{F}(L)$ is $2x$-cycle free. So the problems stated in this subsection that apply to complete bipartite graphs can equivalently be viewed as problems regarding subrectangles in Latin squares.

2.3.4 Atomic and anti-atomic Latin squares

Definition 2.3.30. Let L be a Latin square of order n, let L^* denote its transpose, and let L' denote its $(3,2,1)$-conjugate. A *column cycle of length* ℓ in L is a set X of entries of L such that $\{(c,r,s) : (r,c,s) \in X\}$ forms a row cycle of length ℓ in L^*. A *symbol cycle of length* ℓ in L is a set Y of entries of L such that $\{(s,c,r) : (r,c,s) \in Y\}$ forms a row cycle of length ℓ in L'.

See Figure 2.7 for an example of a column cycle and a symbol cycle.

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

Figure 2.7: The blue highlighted entries of the Latin square in this figure form a column cycle of length 3 and the red highlighted entries form a symbol cycle of length 4.

Recall that a row-Hamiltonian Latin square of order n is a Latin square of order n whose row cycles are all of length n. A *column-Hamiltonian* Latin square of order n is a Latin square of order n whose column cycles are all of length n and a *symbol-Hamiltonian* Latin square of order n is a Latin square of order n whose symbol cycles are all of length n.

By Lemma 2.3.7, we know that the set of lengths of row cycles of a Latin square is the same as that of its row-inverse. Combining this with Definition 2.3.30, it is immediate that if L is a row-Hamiltonian Latin square, then:

- The row-inverse of L is row-Hamiltonian,
- The transpose and $(2,3,1)$-conjugate of L are column-Hamiltonian, and
- The $(3,2,1)$-conjugate and $(3,1,2)$-conjugate of L are symbol-Hamiltonian.

We now define a property that is stronger than the row-Hamiltonian property.

Definition 2.3.31. An *atomic Latin square* of order n is a Latin square of order n whose row cycles, column cycles, and symbol cycles are all of length n.

Equivalently, an atomic Latin square is a Latin square that is row-Hamiltonian, column-Hamiltonian, and symbol-Hamiltonian.

Definition 2.3.32. For a Latin square L, let $\nu(L)$ denote the number of conjugates of L that are row-Hamiltonian.

We will also say that a Latin square L has $\nu = \nu(L)$. It is immediate from the comments made before Definition 2.3.31 that atomic Latin squares are precisely the Latin squares with $\nu = 6$ and that $\nu(L) \in \{0,2,4,6\}$ for every Latin square L [116]. Lemma 2.3.7 tells us that

the row-Hamiltonian property is an isotopism class invariant, thus ν is a species invariant. Therefore, if L is a Latin square, then we will say that the species containing L has $\nu = \nu(L)$.

Next, we discuss the infinite families of row-Hamiltonian Latin squares and the associated ν values. Suppose that n is odd, let $\mathcal{F}$ be an ordered perfect 1-factorisation of K_{n+1}, and let $v \in V(K_{n+1})$. Let $L = \mathscr{L}(\mathcal{F}, v)$. It is known [121] that L is involutory, which implies that $\nu(L) \in \{2, 6\}$. This will be explored in more detail in Chapter 5.

Let $p \geqslant 11$ be prime. There are five species containing row-Hamiltonian Latin squares of order p that can be obtained by applying the $\mathbb{K}$-construction to GK_{p+1} or GB_{p+1}. If 2 is primitive modulo p, then all five of these species have $\nu = 6$. If 2 is not primitive modulo p, then exactly two of these species have $\nu = 6$ and the remaining three have $\nu = 2$ [22, 99, 116]. Now let p be any odd prime. Let v be a vertex of K_{2p} and let $L = \mathscr{L}(GA_{2p}, v)$. In Chapter 5, we prove that the species of L does not depend on the choice of v. We also prove that $\nu(L) = 6$ if $p = 3$ and $\nu(L) = 2$ otherwise. The row-Hamiltonian Latin squares of order p^2 constructed by Bryant, Maenhaut, and Wanless [21] have $\nu = 2$. Of the row-Hamiltonian Latin squares constructed by Allsop and Wanless [5], all except those of orders 3 and 19 have $\nu = 4$.

Atomic Latin squares have been studied in [22, 54, 86, 100, 116, 120]. In some of these papers, atomic Latin squares of small orders are constructed. Combining these constructions with the infinite families of atomic Latin squares discussed above, we obtain the following existence theorem.

Theorem 2.3.33. *There exists an atomic Latin square of order n if n is prime or n is an element of*

$$\{25, 27, 49, 121, 125, 289, 361, 625, 841, 1369, 1849, 2809, 4489, 24\,649, 39\,601\}.$$

It is unknown whether there exists an atomic Latin square of an order that is not a prime power.

The species containing atomic Latin squares of orders up to 11 have been enumerated. Table 2.5 displays the number of species of Latin squares of order n, and the number of those containing atomic Latin squares, for $n \in \{2, 3, \ldots, 11\}$.

n	species	atomic species
2	1	1
3	1	1
4	2	—
5	2	1
6	12	—
7	147	1
8	283 657	—
9	19 270 853 541	0
10	34 817 397 894 749 939	—
11	2 036 029 552 582 883 134 196 099	7

Table 2.5: The number of species and species containing atomic Latin squares of order n for small values of n.

The number of species containing atomic Latin squares of orders up to 9 were determined by Wanless [116] and the number of species containing atomic Latin squares of order 11 was determined by Maenhaut and Wanless [86].

From Lemma 2.3.8, we know that an anti-perfect 1-factorisation of $K_{n,n}$ corresponds to a Latin square of order n that has no row cycle of length n. We make the following definition.

Definition 2.3.34. An *anti-atomic Latin square* of order n is a Latin square of order n that does not have a row cycle of length n, does not have a column cycle of length n, and does not have a symbol cycle of length n.

Equivalently, a Latin square of order n is anti-atomic if none of its conjugates have a row cycle of length n. In Chapter 6, we resolve the existence problem for anti-atomic Latin squares and give some methods of constructing them.

2.4 Quadratic Latin squares

In this section, we discuss quadratic Latin squares, which are the main topic of Chapter 6.

Throughout this section, let q be an odd prime power. Let $\mathbb{F}_q$ denote the finite field of order q and let $\mathbb{F}_q^*$ denote the multiplicative group of units in $\mathbb{F}_q$. Let $\mathcal{R}_q$ denote the set of quadratic residues in $\mathbb{F}_q^*$ and let $\mathcal{N}_q$ denote the set of quadratic non-residues in $\mathbb{F}_q^*$.

Let $(G, +)$ be an abelian group. An *orthomorphism* of G is a permutation φ of G such that the map $x \mapsto \varphi(x) - x$ is also a permutation of G. Let $\varphi : G \to G$ be any map and define a $q \times q$ matrix M with row index set, column index set, and symbol set G by $M_{i,j} = i + \varphi(j - i)$. It is a well known fact that M is a Latin square if and only if φ is an orthomorphism of G (see, e.g., [49]). If φ is an orthomorphism of G, then we say that the Latin square M is *generated* by φ. We also say that the quasigroup whose operation table is M is *generated* by φ.

Let u and v be positive integers such that $q - 1 = uv$. Let ι be a primitive element of $\mathbb{F}_q^*$. For each $j \in \{0, 1, \ldots, u-1\}$, define $C_{u,j} = \{\iota^{ui+j} : i \in \{0, 1, \ldots, v-1\}\}$. Then $C_{u,j}$ is a *cyclotomic coset* of the unique subgroup $C_{u,0}$ in $\mathbb{F}_q^*$ of index u. For $(a_0, a_1, \ldots, a_{u-1}) \in \mathbb{F}_q^u$, let $\varphi = \varphi_\iota[a_0, a_1, \ldots, a_{u-1}]$ be the map defined by

$$\varphi(x) = \begin{cases} 0 & \text{if } x = 0, \\ a_j x & \text{if } x \in C_{u,j}. \end{cases} \tag{2.2}$$

Then φ is a *cyclotomic map of index* u. If a cyclotomic map is also an orthomorphism, then it is a *cyclotomic orthomorphism*. We are particularly interested in cyclotomic orthomorphisms of index 2.

Definition 2.4.1. A *quadratic orthomorphism* is a cyclotomic orthomorphism of index 2.

If $u = 2$, then $C_{u,0} = \mathcal{R}_q$ and $C_{u,1} = \mathcal{N}_q$, regardless of the choice of ι. Hence, for $(a, b) \in \mathbb{F}_q^2$, we denote $\varphi_\iota[a, b]$ simply by $\varphi[a, b]$. The following theorem of Evans [49] gives a simple characterisation of when a cyclotomic map of index 2 is a quadratic orthomorphism.

Theorem 2.4.2. *Let $(a, b) \in \mathbb{F}_q^2$. The map $\varphi[a, b]$ is a quadratic orthomorphism if and only if $\{ab, (a-1)(b-1)\} \subseteq \mathcal{R}_q$.*

We are now ready to define a quadratic Latin square.

Definition 2.4.3. A *quadratic Latin square* is a Latin square that is generated by a quadratic orthomorphism. A *quadratic quasigroup* is a quasigroup that is generated by a quadratic orthomorphism.

We can give a more explicit definition of a quadratic Latin square. Say that $(a, b) \in \mathbb{F}_q^2$ is a *valid pair* if $\{ab, (a-1)(b-1)\} \subseteq \mathcal{R}_q$. Let $(a, b) \in \mathbb{F}_q^2$ be a valid pair. Let $\mathcal{L} = \mathcal{L}[a, b]$ denote the Latin square with row index set, column index set, and symbol set $\mathbb{F}_q$ that is defined by

$$\mathcal{L}_{i,j} = \begin{cases} i & \text{if } i = j, \\ i + a(j-i), & \text{if } j - i \in \mathcal{R}_q, \\ i + b(j-i) & \text{if } j - i \in \mathcal{N}_q. \end{cases}$$

Then $\mathcal{L}$ is the Latin square generated by the quadratic orthomorphism $\varphi[a, b]$. So a quadratic Latin square of order q is a Latin square $\mathcal{L}[a, b]$ for some valid pair $(a, b) \in \mathbb{F}_q^2$. Denote the quasigroup whose operation table is $\mathcal{L}[a, b]$ by $\mathcal{Q}_{a,b}$. Equivalently, the quadratic quasigroup $\mathcal{Q}_{a,b}$ is the quasigroup $(\mathbb{F}_q, *_{a,b})$ where $*_{a,b}$ is the binary operation on $\mathbb{F}_q$ defined by $x *_{a,b} y = x + \varphi[a, b](y - x)$. See Figure 2.8 and Figure 2.9 for examples of quadratic Latin squares.

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

Figure 2.8: The quadratic Latin square $\mathcal{L}[2, 6]$ of order 11.

Quadratic Latin squares have previously been used to construct many interesting mathematical objects such as: perfect 1-factorisations [5, 120], mutually orthogonal Latin squares [48, 49], atomic Latin squares [120], Latin trades [26], Falconer varieties [5], and maximally non-associative quasigroups [42, 44, 84]. Quadratic Latin squares are the main topic of Chapter 6. We count the number of intercalates in quadratic Latin squares and give a characterisation of N_2 quadratic Latin squares. We prove that quadratic Latin squares are not row-Hamiltonian under certain conditions. We use quadratic Latin squares to build new examples of anti-perfect 1-factorisations of complete graphs, anti-perfect 1-factorisations of complete bipartite graphs, and anti-atomic Latin squares. We also determine the autotopism groups of quadratic Latin squares and determine exactly when two such squares are isotopic, generalising work of Drápal and Wanless [43].

$$\begin{bmatrix}
0 & x+2 & 2x+1 & 2x+2 & x & 2 & x+1 & 1 & 2x \\
2x+2 & 1 & x & 0 & 2x & x+1 & 2x+1 & x+2 & 2 \\
x+1 & 2x & 2 & x+2 & 1 & 2x+1 & 0 & 2x+2 & x \\
2x+1 & 2x+1 & 0 & x & 2x+2 & 1 & 2 & 2x & x+2 \\
1 & 2x+2 & x+2 & 2 & x+1 & 2x & x & 0 & 2x+1 \\
x & 2 & 2x & 2x+1 & 0 & x+2 & 2x+2 & x+1 & 1 \\
x+2 & 0 & 2x+2 & 1 & 2x+1 & x & 2x & 2 & x+1 \\
2x & x & 1 & x+1 & 2 & 2x+2 & x+2 & 2x+1 & 0 \\
2 & 2x+1 & x+1 & 2x & x+2 & 0 & 1 & x & 2x+2
\end{bmatrix}$$

Figure 2.9: Identify $\mathbb{F}_9$ with $\mathbb{F}_3[x]/(x^2 - x - 1)$. Then x is a primitive element of $\mathbb{F}_9^*$. This figure shows the quadratic Latin square $\mathcal{L}[x+2, 2x]$ of order 9 (here we are using the total order $0 < 1 < 2 < x < x+1 < x+2 < 2x < 2x+1 < 2x+2$ on $\mathbb{F}_9$).

Chapter 3

Subsquares in random Latin rectangles

Throughout this chapter, n and k will denote positive integers with $k \leqslant n$ and all asymptotics are as $n \to \infty$, with k some function of n.

Let m be an integer satisfying $2 \leqslant m \leqslant \min\{k, n/2\}$ and recall from §2.2.1 that $\mathbb{E}_m(k,n)$ is the expected number of subsquares of order m in a random $k \times n$ Latin rectangle. The first main result of this chapter is the following theorem.

Theorem 3.0.1. *If m and k are integer functions of n satisfying $4 \leqslant m \leqslant \min\{k, n/2\}$, then $\mathbb{E}_m(k,n) = O(n^{-2})$.*

An immediate corollary of Theorem 3.0.1 is the following result, which proves Conjecture 2.2.4(i) and Conjecture 2.2.8(i).

Corollary 3.0.2. *With probability $1 - O(1/n)$, a random $k \times n$ Latin rectangle has no proper subsquare of order 4 or more.*

We also make progress on Conjecture 2.2.4(ii) and Conjecture 2.2.8(ii).

Theorem 3.0.3. *For $3 \leqslant k \leqslant n$,*

$$\mathbb{E}_3(k,n) \leqslant \frac{2k}{3n}\left(1 + O\left(\frac{1}{k}\right)\right).$$

In particular,

$$\mathbb{E}_3(n,n) \leqslant \frac{2}{3} + o(1).$$

Our last main result for this chapter is the following theorem, which establishes the asymptotics of $\mathbb{E}_2(k,n)$ for all $k \leqslant n$.

Theorem 3.0.4. *For $2 \leqslant k \leqslant n$,*

$$\mathbb{E}_2(k,n) = \frac{1}{2}\binom{k}{2}(1 + o(1)).$$

The structure of this chapter is as follows. In §3.1, we give some definitions that we require to prove our main theorems. We prove Theorem 3.0.1 in §3.2 and we prove Theorem 3.0.3 and Theorem 3.0.4 in §3.3.

3.1 Background

The switching method underlies many of the results regarding subsquares in random Latin rectangles, including those in [27, 39, 53, 55, 76, 77, 78, 90]. However, often other ideas are also utilised, such as the triangle removal process [76, 77]. Let A and B be finite sets. Suppose that there is an operation, called a switching, that modifies elements of A to obtain elements of B. Let d_A be the average, over $a \in A$, of the number of switchings that can be applied to a to obtain an element of B. Let d_B be the average, over $b \in B$, of the number of switchings that can be applied to an element of A to obtain b. Then $d_A|A| = d_B|B|$. Thus, by estimating d_A and d_B, we can estimate the relative sizes of A and B. This is the simplest form of the switching method. See [50, 58] for more general versions of the switching method.

We will use the switching method to prove our main results. The main goal of this section is to define cycle switching and incomplete cycle switching. These will form the switching procedure that we will utilise in §3.2 and §3.3.

Throughout this chapter, unless otherwise stated, the row index set of any $k \times n$ partial Latin rectangle will be $[k]$ and the column index set and symbol set will be $[n]$. The convention that a Latin square of order n has row indices, column indices, and symbol set $[n]$ will be broken when dealing with subsquares.

Let P be a $k \times n$ partial Latin rectangle. A *row cycle of length* ℓ in P is a $2 \times \ell$ submatrix of P that contains exactly ℓ symbols and no empty cells and does not contain any smaller submatrix with these properties. Similarly, a *column cycle of length* ℓ in P is an $\ell \times 2$ submatrix of P that contains exactly ℓ symbols and no empty cells and does not contain any smaller submatrix with these properties. When P is a Latin square, these notions coincide with the row cycles and column cycles defined in Chapter 2.

Definition 3.1.1. Let L be a $k \times n$ Latin rectangle. Suppose that $\mathcal{C}$ is an $\ell \times 2$ submatrix of L that does not contain a column cycle and which hits columns i and j and rows R of L. Then $\mathcal{C}$ is an *incomplete column cycle of length* ℓ in L if there are unique rows r and r' in R such that $L_{r,i}$ does not occur in column j of L and $L_{r',j}$ does not occur in column i of L.

See Figure 3.1 for an example of an incomplete column cycle.

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

Figure 3.1: The blue highlighted entries of the Latin rectangle in this figure form an incomplete column cycle of length 3.

Let L be a $k \times n$ Latin rectangle. Let $\mathcal{D}$ be a row cycle of L that hits rows i and j and columns C, for some $\{i, j\} \subseteq [k]$ and $C \subseteq [n]$. Since $\mathcal{D}$ is uniquely determined by rows i, j and a single column in C, we denote $\mathcal{D}$ by $\rho(i, j, c)$, where c is any element of C. Row cycles give us a way of perturbing Latin rectangles to create new ones. We can define a Latin rectangle L'

by

$$L'_{x,y} = \begin{cases} L_{i,y} & \text{if } x = j \text{ and } y \in C, \\ L_{j,y} & \text{if } x = i \text{ and } y \in C, \\ L_{x,y} & \text{otherwise.} \end{cases}$$

We say that L' has been obtained from L by switching on $\rho(i, j, c)$.

Let L be a $k \times n$ Latin rectangle, let $\{i, j\} \subseteq [n]$ with $i \neq j$, and let $r \in [k]$. There is either a unique column cycle or a unique incomplete column cycle (but not both) which hits columns i and j and row r. Denote this column cycle or incomplete column cycle by $\sigma(i, j, r)$ and let R be the set of rows that it hits. The substructure $\sigma(i, j, r)$ gives us a way of perturbing L to create a new Latin rectangle. Define a Latin rectangle L' by

$$L'_{x,y} = \begin{cases} L_{x,i} & \text{if } x \in R \text{ and } y = j, \\ L_{x,j} & \text{if } x \in R \text{ and } y = i, \\ L_{x,y} & \text{otherwise.} \end{cases}$$

We say that L' has been obtained from L by switching on $\sigma(i, j, r)$.

There are also symbol cycles and incomplete symbol cycles of Latin rectangles, which are, respectively, the images of column cycles and incomplete column cycles under the map which replaces each entry (r, c, s) by the entry (r, s, c). Symbol cycles and incomplete symbol cycles can also be switched in an analogous way. See [118] for a study of switching on row, column and symbol cycles.

Definition 3.1.2. Let L be a $k \times n$ Latin rectangle and let $\{i, j\} \subseteq [k]$ with $i \neq j$. The permutation mapping row i of L to row j, denoted by $\tau_{i,j}$, is defined by $\tau_{i,j}(L_{i,\ell}) = L_{j,\ell}$ for every $\ell \in [n]$. Such a permutation is called a *row permutation* of L.

Definition 3.1.2 naturally generalises to Latin rectangles with more general row indices, column indices, and symbols. We will need this generalisation in future chapters.

Let L be a $k \times n$ Latin rectangle and let $\{i, j\} \subseteq [k]$ with $i \neq j$. Let ρ be a cycle in $\tau_{i,j}$ and in row i let C be the set of columns containing the symbols involved in ρ. Then the set of entries

$$\big\{(i, c, L_{i,c}), (j, c, L_{j,c}) : c \in C\big\}$$

is the row cycle $\rho(i, j, c)$ of L, where c is any element of C. Conversely, every row cycle of L corresponds to a cycle of a row permutation of L.

Let L be a $k \times n$ Latin rectangle and let $\{i, j\} \subseteq [n]$ with $i \neq j$. The partial permutation mapping column i of L to column j, denoted by $\xi_{i,j}$, is defined by $\xi_{i,j}(L_{\ell,i}) = L_{\ell,j}$ for every $\ell \in [k]$. A cycle in $\xi_{i,j}$ corresponds to a column cycle of L hitting columns i and j. Say that a list $[x_1, x_2, \ldots, x_u]$ is an *incomplete cycle* of $\xi_{i,j}$ if $\xi_{i,j}(x_i) = x_{i+1}$ for every $i \in [u-1]$ and $\xi_{i,j}(x_u)$ and $\xi_{i,j}^{-1}(x_1)$ are undefined. An incomplete cycle of $\xi_{i,j}$ corresponds to an incomplete column cycle of L hitting columns i and j.

3.2 Subsquares of order 4 or more

Throughout this section, $m = m(n)$ will be a positive integer satisfying $2 \leqslant m \leqslant \min\{k, n/2\}$. This section is split into three subsections. In §3.2.1 and §3.2.2, we prove two different bounds

on the probability that a random $k \times n$ Latin rectangle contains a subsquare of order m in a specific selection of rows and columns and on a specific symbol set. These bounds are effective for different but overlapping ranges of m. In §3.2.3, we combine them to prove Theorem 3.0.1, using the bound from §3.2.1 for $m \geqslant 6$ and the bound from §3.2.2 for $m \in \{4, 5\}$.

3.2.1 Bounding probability of large subsquares

The main result of this subsection is the following theorem. For $m = 4$, the bound that it gives is not strong enough to imply any result in the direction of Theorem 3.0.1 and for $m = 5$, it is not enough to imply the full strength of Theorem 3.0.1. The bound we prove in the next subsection will be better whenever $2 < m = O(1)$.

Theorem 3.2.1. *Let $R \subseteq [k]$ be of cardinality m, let C and S be subsets of $[n]$ of cardinality m, and let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. The probability that $\mathbf{L}[R, C]$ is a Latin square of order m with symbol set S is at most*

$$\frac{kn(k+1-m)(n+1-m)}{m^2\binom{n}{m}^3\binom{k}{m}}.$$

Without loss of generality we may assume that $R = C = S = [m]$ in Theorem 3.2.1. Let $T_0 = \varnothing$ and for $i \in [m^2]$, define T_i to be the set of all pairs $(r, c) \in [m]^2$ such that $(c-1)m+r \leqslant i$. We will consider the sets T_i to be sets of cells of $k \times n$ Latin rectangles. So if $a \in \{0, 1, \ldots, m-1\}$, $b \in [m]$, and L is a $k \times n$ Latin rectangle, then T_{am+b} consists of all cells of L in the first m rows and a columns or the first b rows and the $(a+1)$-st column. Define t_i to be the cell in $T_i \setminus T_{i-1}$. Let Δ_0 be the set of all $k \times n$ Latin rectangles and define Δ_i to be the set of $k \times n$ Latin rectangles such that the symbol in cell (r, c) is an element of $[m]$ for every $(r, c) \in T_i$.

Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. The probability that $\mathbf{L}[[m], [m]]$ is a Latin square of order m with symbol set $[m]$ is $\Pr(\mathbf{L} \in \Delta_{m^2})$. By the chain rule of probability,

$$\Pr(\mathbf{L} \in \Delta_{m^2}) = \prod_{i=1}^{m^2} \Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}). \tag{3.1}$$

Similar to the approach of Divoux et al. [39], our approach to proving Theorem 3.2.1 is to bound the terms

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}). \tag{3.2}$$

However, we will only provide a non-trivial bound on (3.2) when the cell $t_i = (r, c)$ satisfies $\{1, m\} \cap \{r, c\} \neq \varnothing$. That is, we only bound (3.2) when t_i lies in the first row, first column, m-th row, or m-th column. Slightly surprisingly, this turns out to be enough to derive our result. Consider when $k = 4$, $n = 6$, $m = 3$, and $i = 5$. The Latin rectangle

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

is a member of Δ_i due to the highlighted entries. Suppose that we want to use column cycle

or incomplete column cycle switching to get from L to a rectangle in $\Delta_{i-1} \setminus \Delta_i$. Clearly, we must switch on $\sigma(2, c, 2)$ for some $c \in \{3, 4, 5, 6\}$. If we take $c = 5$, it is clear that the resulting rectangle will lie in $\Delta_{i-1} \setminus \Delta_i$, as desired. However, if we take $c = 4$, the resulting rectangle will not be a member of Δ_{i-1}, since cell $(1, 2)$ will no longer contain a symbol in $\{1, 2, 3\}$. So to estimate the number of switchings from some rectangle $L' \in \Delta_i$ to a rectangle in $\Delta_{i-1} \setminus \Delta_i$, we ought to estimate the number of columns c of L' for which $\sigma(2, c, 2)$ does not hit row 1. When dealing with general n, m, and i with $t_i = (r, c)$, to estimate the number of switchings from a rectangle $L' \in \Delta_i$ to a rectangle in $\Delta_{i-1} \setminus \Delta_i$, we ought to estimate the number of columns c' of L' for which $\sigma(c, c', r)$ does not hit any row $r' < r$. This seems like a difficult task in general. However, when $r = 1$ this difficulty does not arise and it is clear that we can switch L' on $\sigma(c, c', 1)$ for any choice of $c' \in [n] \setminus [c]$ such that $L'_{r,c'} \notin [m]$ and obtain a rectangle in $\Delta_{i-1} \setminus \Delta_i$. This explains why we can provide non-trivial bounds on (3.2) when t_i is in the first row. By using symbol cycle and incomplete symbol cycle switching instead of column cycle and incomplete column cycle switching and applying the same logic, we see why we can obtain non-trivial bounds on (3.2) when t_i is in the first column. Note that we could also use row cycle switching to achieve this, but we get stronger bounds when we use symbol cycle and incomplete symbol cycle switching. When $t_i = (r, m)$ is in the m-th column and $c \in [n] \setminus [m]$, we can estimate the number of rectangles in Δ_i for which $\sigma(m, c, r)$ does not hit any row $r' < r$ (see Lemma 3.2.4). We can obtain similar results for when t_i is in the m-th row. This allows us to provide non-trivial bounds on (3.2) in these cases.

The following lemma allows us to bound (3.2) when t_i is in the first row or column.

Lemma 3.2.2. *Let $i \in \{m+1-\zeta, m^2+1-\zeta m\}$ for some $\zeta \in [m]$. For a random $k \times n$ Latin rectangle $\mathbf{L}$,*

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}) = \frac{\zeta}{n+\zeta-m}.$$

Proof. Let $\zeta \in [m]$ and first suppose that $i = m^2 + 1 - \zeta m$. We use column cycle and incomplete column cycle switching to find the relative sizes of Δ_i and $\Delta_{i-1} \setminus \Delta_i$. Let $L \in \Delta_i$. Let $c' \in [n] \setminus [m - \zeta + 1]$ be such that $L_{1,c'} \notin [m]$. Note that there are exactly $n - m$ choices for c'. Let L' be obtained from L by switching on $\sigma(m - \zeta + 1, c', 1)$. Then $L'_{1,m-\zeta+1} \notin [m]$ and $L'_{r,c} = L_{r,c}$ for every cell $(r, c) \in T_{i-1}$. Thus, $L' \in \Delta_{i-1} \setminus \Delta_i$. It follows that there are exactly $(n - m)|\Delta_i|$ switchings from a rectangle in Δ_i to a rectangle in $\Delta_{i-1} \setminus \Delta_i$.

Reversing the switching process, consider $L' \in \Delta_{i-1} \setminus \Delta_i$ that is obtained from some $L \in \Delta_i$ by switching on some $\sigma(m-\zeta+1, c', 1)$. Here, c' must be a column in $[n] \setminus [m-\zeta+1]$ such that $L'_{1,c'} \in [m]$. Since $L'_{1,\ell} \in [m]$ for $\ell \in [m - \zeta]$ and $L'_{1,m-\zeta+1} \notin [m]$, there are exactly ζ choices for c'. Thus, there are exactly $\zeta|\Delta_{i-1} \setminus \Delta_i|$ switchings from a rectangle in $\Delta_{i-1} \setminus \Delta_i$ to a rectangle in Δ_i.

We have shown that $(n - m)|\Delta_i| = \zeta|\Delta_{i-1} \setminus \Delta_i|$. Therefore,

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}) = \frac{|\Delta_i|}{|\Delta_i| + |\Delta_{i-1} \setminus \Delta_i|} = \frac{\zeta}{n+\zeta-m},$$

as required. To deal with the case where $i = m + 1 - \zeta$, we use symbol cycle and incomplete symbol cycle switching instead of column cycle and incomplete column cycle switching. Crucially, no two cells in $T_{m+1-\zeta}$ contain the same symbol, since we look at the first column before we look at any other cells. □

Our next task is to bound (3.2) when t_i is in the m-th row or column. To do that, we need to prove the preliminary results Lemma 3.2.3 and Lemma 3.2.4 below. We also need the following definitions. For a set $T \subseteq [m]^2$ of cells, define $\Upsilon(T)$ to be the set of $k \times n$ partial Latin rectangles P such that the set of non-empty cells of P is exactly T and every symbol of P is in $[m]$. Also define

$$\Upsilon^*(T) = \bigcup_{T' \subseteq T} \Upsilon(T'). \tag{3.3}$$

Lemma 3.2.3. *Let $P \in \Upsilon^*([m]^2)$ and let (r, c) be a non-empty cell of P. Also let $r' \in [k] \setminus [m]$. Define $C' = \{c, c_1, c_2, \ldots, c_\ell\} \subseteq [m]$ to be the set of columns c' for which cell (r, c') of P is non-empty. Suppose that the entries of P in columns c and c_i form a union of column cycles for every $i \in [\ell]$. Let A be the set of $k \times n$ Latin rectangles containing P and let $X \subseteq A$ be the set of rectangles in A such that the row cycle $\rho(r, r', c)$ does not hit any column in $C' \setminus \{c\}$. Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. Then*

$$\Pr(\mathbf{L} \in X \mid \mathbf{L} \in A) = \frac{1}{\ell + 1}.$$

Proof. Let $U \subseteq [m]$ be the set of rows containing a non-empty cell of P in column c. Define $Y = A \setminus X$ and a map $\phi : Y \to X$ as follows. Let $L \in Y$ and let $s = L_{r,c}$. Write the cycle of $\tau_{r,r'}$ containing s as $(s, x_1, x_2, \ldots, x_u)$. Let $v \leqslant u$ be maximal such that $x_v = L_{r,c_j}$ for some $j \in [\ell]$ and let $c' = c_j$ for this particular j. Note that v exists since $L \in Y$. Also note that $v < u$, since if $v = u$ this would imply that $(r', c', s) \in L$, contradicting the fact that the entries of P in columns c and c' form a union of column cycles. Define $\phi(L)$ by swapping the symbols in cells (r'', c) and (r'', c') for every $r'' \in [k] \setminus U$. The fact that the entries of P in columns c and c' form a union of column cycles implies that $\phi(L)$ is reached from L by switching one or more column cycles or incomplete column cycles. Hence, $\phi(L)$ is indeed a Latin rectangle and $\phi(L) \in A$. The cycle of $\tau_{r,r'}$ of $\phi(L)$ containing s is $(s, x_{v+1}, \ldots, x_u)$, meaning that $\phi(L) \in X$.

Let $L' \in X$. We now argue that there are exactly ℓ rectangles $L \in Y$ such that $\phi(L) = L'$. Note that L' is obtained from any such L by swapping all symbols in cells (r'', c) and (r'', c_w) for some $w \in [\ell]$ and all $r'' \in [k] \setminus U$. It is immediate that there are at most ℓ possible rectangles L such that $\phi(L) = L'$. We need to show that each of the ℓ possibilities is realised. Let $w \in [\ell]$. The fact that $L' \in X$ ensures that $\tau_{r,r'}$ of L' contains two separate cycles $(\eta_1, \eta_2, \ldots, \eta_a)$ and $(\zeta_1, \zeta_2, \ldots, \zeta_b)$ where $\eta_1 = L'_{r,c}$ and $\zeta_1 = L'_{r,c_w}$. Swapping the symbols in cells (r'', c) and (r'', c_w) for all $r'' \in [k] \setminus U$ produces a Latin rectangle in which $\tau_{r,r'}$ contains the cycle $(\eta_1, \zeta_2, \ldots, \zeta_b, \zeta_1, \eta_2, \ldots, \eta_a)$, which hits both columns c and c_w. By definition, such a rectangle is in Y. It follows that $|Y| = \ell |X|$ and

$$\Pr(\mathbf{L} \in X \mid \mathbf{L} \in A) = \frac{|X|}{|X| + |Y|} = \frac{1}{\ell + 1},$$

as required. □

Lemma 3.2.4. *Let $P \in \Upsilon^*([m]^2)$ and let (r, c) be a non-empty cell of P. Also let $c' \in [n] \setminus [m]$. Define $R' = \{r, r_1, r_2, \ldots, r_\ell\} \subseteq [m]$ to be the set of rows r' for which cell (r', c) of P is non-empty. Suppose that the entries of P in rows r and r_i form a union of row cycles for every $i \in [\ell]$. Let A be the set of $k \times n$ Latin rectangles containing P and let $X \subseteq A$ be the set of rectangles in A such that $\sigma(c, c', r)$ does not hit any row in $R' \setminus \{r\}$. Let $\mathbf{L}$ be a random $k \times n$*

Latin rectangle. Then

$$\Pr(\mathbf{L} \in X \mid \mathbf{L} \in A) \geqslant \frac{1}{\ell+1}.$$

Proof. The proof is similar to the proof of Lemma 3.2.3. Let $U \subseteq [m]$ be the set of columns containing a non-empty cell of P in row r. Define $Y = A \setminus X$ and a map $\phi : Y \to X$ as follows. Let $L \in Y$ and let $s = L_{r,c}$. First suppose that $\sigma(c, c', r)$ is a column cycle. Write the cycle of $\xi_{c,c'}$ containing s as $(s, x_1, x_2, \ldots, x_u)$. Let $v < u$ be maximal such that $x_v = L_{r_j,c}$ for some $j \in [\ell]$ and let $r' = r_j$ for this particular j. By the same arguments as used in the proof of Lemma 3.2.3, we know that v exists. Define $\phi(L)$ by swapping the symbols in cells (r, c'') and (r', c'') for every $c'' \in [n] \setminus U$. The fact that the entries of P in rows r and r' form a union of row cycles implies that $\phi(L)$ is reached from L by switching on one or more row cycles. Hence, $\phi(L)$ is indeed a Latin rectangle and $\phi(L) \in A$. The cycle of $\xi_{c,c'}$ of $\phi(L)$ containing symbol s is $(s, x_{v+1}, \ldots, x_u)$, meaning that $\phi(L) \in X$. Now suppose that $\sigma(c, c', r)$ is an incomplete column cycle. Write the incomplete cycle of $\xi_{c,c'}$ as $[y_1, \ldots, y_{u'}, s, x_1, \ldots, x_u]$. We now consider two cases. First, suppose that there is some $v \in [u']$ such that $L_{r_j,c} = y_v$ for some $j \in [\ell]$. Let such a v be maximal and let $r' = r_j$ for this value of j. If $v = u'$, then L must contain the entry (r', c', s), contradicting the fact that the entries of P in rows r and r' form a union of row cycles. So $v < u'$. Let $\phi(L)$ be obtained from L by swapping the symbols in cells (r, c'') and (r', c'') for every $c'' \in [n] \setminus U$. The fact that the entries of P in rows r and r' form a union of row cycles implies that $\phi(L)$ is reached from L by switching one or more row cycles. Hence, $\phi(L)$ is indeed a Latin rectangle and $\phi(L) \in A$. In $\phi(L)$, $\sigma(c, c', r)$ is a column cycle and the cycle of $\xi_{c,c'}$ of $\phi(L)$ containing s is $(s, y_{v+1}, \ldots, y_{u'})$. Thus, $\phi(L) \in X$. Finally, suppose that there is no $v \in [u']$ such that $L_{r_j,c} = y_v$ for some $j \in [\ell]$. Since $L \in Y$, there is some $v' < u$ such that $L_{r_j,c} = x_{v'}$. Let such a v' be maximal and let $r' = r_j$ for this value of j. Let $\phi(L)$ be obtained from L by swapping the symbols in cells (r, c'') and (r', c'') for every $c'' \in [n] \setminus U$. Then $\phi(L) \in A$. Also, in $\phi(L)$, $\sigma(c, c', r)$ is an incomplete column cycle and the incomplete cycle of $\xi_{c,c'}$ containing s is $[y_1, \ldots, y_{u'}, s, x_{v'+1}, \ldots, x_u]$. Therefore, $\phi(L) \in X$.

Let $L' \in X$. We now argue that there are at most ℓ rectangles $L \in Y$ such that $\phi(L) = L'$. This is true since L' is obtained from any such L by swapping all symbols in cells (r, c'') and (r_w, c'') for some $w \in [\ell]$ and all $c'' \in [n] \setminus U$. It follows that $|Y| \leqslant \ell|X|$ and

$$\Pr(\mathbf{L} \in X \mid \mathbf{L} \in A) = \frac{|X|}{|X| + |Y|} \geqslant \frac{1}{\ell+1},$$

as required. □

We can now bound (3.2) when t_i is in the m-th row or column.

Lemma 3.2.5. *Let $i = jm$ where $j \in [m]$ and let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. Then*

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}) \leqslant \frac{j}{k+j-m}.$$

Proof. We use row cycle switching to estimate the relative sizes of Δ_i and $\Delta_{i-1} \setminus \Delta_i$. For a partial Latin rectangle $P \in \Upsilon(T_i)$, let $\mathbb{L}_P$ denote the set of $k \times n$ Latin rectangles containing P. So Δ_i is the disjoint union

$$\bigcup_{P \in \Upsilon(T_i)} \mathbb{L}_P.$$

Let $r' \in [k] \setminus [m]$. Note that if $L \in \Delta_i$, then $L_{m,j} \in [m]$ and $L_{r',j} \notin [m]$. Let $P \in \Upsilon(T_i)$. By Lemma 3.2.3, there are $|\mathbb{L}_P|/j$ rectangles $L \in \mathbb{L}_P$ such that switching L on $\rho(m, r', j)$ yields a rectangle in $\Delta_{i-1} \setminus \Delta_i$. Thus, the number of switchings from a rectangle in Δ_i to one in $\Delta_{i-1} \setminus \Delta_i$ is $(k-m)|\Delta_i|/j$.

Reversing the switching process, consider $L' \in \Delta_{i-1} \setminus \Delta_i$ that is obtained from some $L \in \Delta_i$ by switching on some $\rho(m, r', j)$. Note that $L'_{m,j} \notin [m]$ and there is at most one $r' \in [k] \setminus [m]$ such that $L'_{r',j} \in [m]$. Therefore, there is at most one switch from L' to a rectangle in Δ_i.

We have thus shown that $(k-m)|\Delta_i|/j \leqslant |\Delta_{i-1} \setminus \Delta_i|$ and so

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}) = \frac{|\Delta_i|}{|\Delta_i| + |\Delta_{i-1} \setminus \Delta_i|} \leqslant \frac{j}{k+j-m},$$

as required. □

Lemma 3.2.6. *Let $i = m^2 - m + j$ where $j \in [m]$ and let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. Then*

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}) \leqslant \frac{j}{n+j-m}.$$

Proof. The proof is similar to the proof of Lemma 3.2.5. We will again denote the set of $k \times n$ Latin rectangles containing P by $\mathbb{L}_P$ for $P \in \Upsilon(T_i)$.

Let $c' \in [n] \setminus [m]$. Note that if $L \in \Delta_i$, then $L_{j,m} \in [m]$ and $L_{j,c'} \notin [m]$. Let $P \in \Upsilon(T_i)$. By Lemma 3.2.4, there are at least $|\mathbb{L}_P|/j$ rectangles $L \in \mathbb{L}_P$ such that switching L on $\sigma(m, c', j)$ yields a rectangle in $\Delta_{i-1} \setminus \Delta_i$. Thus, the number of switchings from a rectangle in Δ_i to one in $\Delta_{i-1} \setminus \Delta_i$ is at least $(n-m)|\Delta_i|/j$.

Reversing the switching process, consider $L' \in \Delta_{i-1} \setminus \Delta_i$ that is obtained from some $L \in \Delta_i$ by switching on some $\sigma(m, c', j)$. Note that $L'_{j,m} \notin [m]$ and there is a unique $c' \in [n] \setminus [m]$ such that $L'_{j,c'} \in [m]$. Therefore, there is at most one switch from L' to a rectangle in Δ_i, namely $\sigma(m, c', j)$.

We have thus shown that $(n-m)|\Delta_i|/j \leqslant |\Delta_{i-1} \setminus \Delta_i|$ and so

$$\Pr(\mathbf{L} \in \Delta_i \mid \mathbf{L} \in \Delta_{i-1}) = \frac{|\Delta_i|}{|\Delta_i| + |\Delta_{i-1} \setminus \Delta_i|} \leqslant \frac{j}{n+j-m},$$

as required. □

We are now ready to prove Theorem 3.2.1.

Proof of Theorem 3.2.1. As previously mentioned, the probability that $\mathbf{L}[R, C]$ is a Latin square of order m with symbol set S is equal to the probability that $\mathbf{L} \in \Delta_{m^2}$. By (3.1) combined with Lemma 3.2.2, Lemma 3.2.5, and Lemma 3.2.6, we obtain the bound

$$\begin{aligned}\Pr(\mathbf{L} \in \Delta_{m^2}) &\leqslant \left(\prod_{j=1}^{m} \frac{j}{n+j-m}\right)^2 \left(\prod_{j=2}^{m-1} \frac{j}{n+j-m}\right)\left(\prod_{j=2}^{m-1} \frac{j}{k+j-m}\right) \\ &= \frac{nk(n+1-m)(k+1-m)}{m^2\binom{n}{m}^3\binom{k}{m}},\end{aligned}$$

as required. □

3.2.2 Bounding probability of small subsquares

The aim of this subsection is to prove the following theorem, which will enable us to bound the expected number of small subsquares in a random Latin rectangle. The bound it gives improves the bound in the previous subsection when $2 < m = O(1)$, although it is worse when m grows at least logarithmically in n. The new bound will be used when $m \in \{4, 5\}$ to get the accuracy required for Theorem 3.0.1.

Theorem 3.2.7. *Let $R \subseteq [k]$ be of cardinality m, let C and S be subsets of $[n]$ of cardinality m, and let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. Suppose that $k > m > 2$. The probability that $\mathbf{L}[R, C]$ is a Latin square of order m with symbol set S is at most*

$$\frac{2^{m-1} m^{m^2+2m-5}}{(k-m)^{5m/2-6}} \left(\frac{1+O(m/n)}{n}\right)^{3m-2}$$

if m is even and at most

$$\frac{2^{m-2} m^{m^2+2m-5}}{(k-m)^{(5m-13)/2}} \left(\frac{1+O(m/n)}{n}\right)^{3m-2}$$

if m is odd. If $k = m > 2$, then the same bounds hold with $k - m$ replaced by 1.

As in §3.2.1, we may assume that $R = C = S = [m]$ in Theorem 3.2.7. Also, if M and M' are any two Latin squares of order m, then replacing M by M' gives an easy bijection from Latin rectangles containing M as a subsquare to Latin rectangles containing M'. Hence, if $\mathbf{L}$ is a random $k \times n$ Latin rectangle, then

$$\Pr(\mathbf{L}[[m], [m]] = M) = \Pr(\mathbf{L}[[m], [m]] = M'). \tag{3.4}$$

Thus, without loss of generality we may assume that $\mathbf{L}[[m], [m]] = M$ is a specific Latin square of order m, which we will choose later. Ultimately, we will multiply by m^{m^2}, which is a trivial upper bound on the number of Latin squares of order m, to obtain Theorem 3.2.7. The proof of Theorem 3.2.7 is similar to the proof of Theorem 3.2.1. Recalling (3.3), let P and P' be elements of $\Upsilon^*([m]^2)$ such that $P \subseteq P'$ and $P' \setminus P = \{(r, c, s)\}$. We will give non-trivial upper bounds on

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) \tag{3.5}$$

when P and P' satisfy certain conditions.

First, we bound (3.5) when (r, c, s) is the only occurrence of row r, the only occurrence of column c, or the only occurrence of symbol s in P'.

Lemma 3.2.8. *Let $\{P, P'\} \subseteq \Upsilon^*([m]^2)$ be such that $P \subseteq P'$ and $P' \setminus P = \{(r, c, s)\}$. Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle where $k > m$. Suppose that P has no entry in row r. Then*

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) \leqslant \frac{1}{k-m}.$$

If P has no entry in column c or no entry with symbol s, then

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) \leqslant \frac{1+O(m/n)}{n}.$$

Proof. First consider the case where P has no entry in row r. Let Y be the set of $k \times n$ Latin rectangles containing P and let $X \subseteq Y$ be the set of rectangles containing P'. We use row cycle switching to find bounds on the relative sizes of X and $Y \setminus X$.

Let $L \in X$. For every row $r' \in [k] \setminus [m]$, switching on $\rho(r, r', c)$ yields a rectangle in $Y \setminus X$. This gives exactly $k - m$ switchings from L to a rectangle in $Y \setminus X$.

Now consider $L' \in Y \setminus X$ and note that there is at most one $r' \in [k]$ such that $L'_{r',c} = s$. Thus, there is at most one row cycle that can be switched back to change L' into some rectangle in X.

We have deduced that $(k-m)|X| \leqslant |Y \setminus X| \leqslant |Y|$. Thus,

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) = \frac{|X|}{|Y|} \leqslant \frac{1}{k-m}.$$

To deal with the case where P has no entry in column c or has no entry with symbol s, we use analogous arguments with column cycle and incomplete column cycle switching or symbol cycle and incomplete symbol cycle switching, respectively. In each case, for a Latin rectangle $L \in X$, there are exactly $n - m$ switchings to a rectangle in $Y \setminus X$. Hence,

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) \leqslant \frac{1}{n-m} = \frac{1 + O(m/n)}{n}.$$ □

We now bound (3.5) when P' and (r, c) satisfy the conditions of Lemma 3.2.3.

Lemma 3.2.9. *Let $\{P, P'\} \subseteq \Upsilon^*([m]^2)$ be such that $P \subseteq P'$ and $P' \setminus P = \{(r, c, s)\}$. Let C' be the set of columns c' for which the cell (r, c') of P' is non-empty. Suppose further that for every $c' \in C' \setminus \{c\}$, the entries of P' in columns c and c' form a union of column cycles. Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle where $k > m$. Then*

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) \leqslant \frac{|C'|}{k-m}.$$

Proof. Let Y be the set of $k \times n$ Latin rectangles containing P and let $X \subseteq Y$ be the set of rectangles containing P'.

Let $r' \in [k] \setminus [m]$. By Lemma 3.2.3, there are $|X|/|C'|$ rectangles in X for which switching on $\rho(r, r', c)$ yields a rectangle in $Y \setminus X$. Thus, there are $(k-m)|X|/|C'|$ switchings from X to $Y \setminus X$.

Now let $L' \in Y \setminus X$. The same argument as given in the proof of Lemma 3.2.8 tells us that there is at most one row cycle of L' that can be switched to reach a rectangle in X.

We have shown that $(k-m)|X|/|C'| \leqslant |Y \setminus X| \leqslant |Y|$. Thus,

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) = \frac{|X|}{|Y|} \leqslant \frac{|C'|}{k-m},$$

as required. □

Modifying the proof of Lemma 3.2.9 by using column cycle and incomplete column cycle switching rather than row cycle switching and using Lemma 3.2.4 instead of Lemma 3.2.3, we can prove the following lemma.

Lemma 3.2.10. *Let $\{P, P'\} \subseteq \Upsilon^*([m]^2)$ be such that $P \subseteq P'$ and $P' \setminus P = \{(r, c, s)\}$. Let R' be the set of rows r' for which the cell (r', c) of P' is non-empty. Suppose further that for every $r' \in R' \setminus \{r\}$, the entries of P' in rows r and r' form a union of row cycles. Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle. Then*

$$\Pr(\mathbf{L} \supseteq P' \mid \mathbf{L} \supseteq P) \leqslant \frac{|R'|}{n}\left(1 + O\left(\frac{m}{n}\right)\right).$$

Our next task is to choose the Latin square M of order m discussed after (3.4). Our choice of M allows us to apply Lemma 3.2.8, Lemma 3.2.9, or Lemma 3.2.10 many times to give non-trivial bounds on (3.5). If m is even, then define M to be a Latin square of order m with the following properties:

- $M_{1,i} = M_{i,1} = i$ for every $i \in [m]$,
- $M_{2,i} = M_{i,2} = i + 1$ for every odd $i \in [m]$,
- $M_{2,i} = M_{i,2} = i - 1$ for every even $i \in [m]$.

If m is odd, then define M to be a Latin square of order m satisfying:

- $M_{1,i} = M_{i,1} = i$ for every $i \in [m]$,
- $M_{2,i} = M_{i,2} = i + 1$ for every odd $i \in [m-3]$,
- $M_{2,i} = M_{i,2} = i - 1$ for every even $i \in [m-3]$,
- $(M_{2,m-2}, M_{2,m-1}, M_{2,m}) = (M_{m-2,2}, M_{m-1,2}, M_{m,2}) = (m-1, m, m-2)$.

Such a square M exists by [1, Theorem 1.5]. See Figure 3.2 for examples of such squares when $m = 4$ and $m = 5$. These are the only two orders for which Theorem 3.2.7 will be used in the proof of Theorem 3.0.1.

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

Figure 3.2: Possible Latin squares M when $m \in \{4, 5\}$. Colour coding , , indicates cells to which Lemma 3.2.8, Lemma 3.2.9, and Lemma 3.2.10, respectively, will be applied in the proof of Theorem 3.2.7.

We are now ready to prove Theorem 3.2.7.

Proof of Theorem 3.2.7. First suppose that m is even and $k > m$. We assume that $R = C = S = [m]$ and that M is the Latin square of order m defined above. Let P be the $k \times n$ partial Latin rectangle such that $P[[m], [m]] = M$ and every cell of P outside of $[m]^2$ is empty. We define a family of partial Latin rectangles $P_i \subseteq P$ as follows. Firstly, $P_0 = \varnothing$. Then, for $i \in [m^2]$, define P_i by adding an entry of P to P_{i-1}.

For $i \in [2m]$, we add the entry of P in cell $(1, (i+1)/2)$ if i is odd and we add the entry in cell $(2, i/2)$ if i is even. If i is odd, then

$$\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant \frac{1 + O(m/n)}{n} \tag{3.6}$$

by Lemma 3.2.8, since there is only one non-empty cell of P_i in column $(i+1)/2$. Similarly, if $i \equiv 2 \bmod 4$, then (3.6) holds by Lemma 3.2.8, since the entry $(2, i/2, i/2+1)$ is the only entry of P_i with symbol $i/2+1$. If $i \equiv 0 \bmod 4$, then

$$\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant \frac{2(1 + O(m/n))}{n} \tag{3.7}$$

by Lemma 3.2.10.

For $i \in \{2m+1, \ldots, 4m-4\}$, we add the entry of P in cell $((i-2m+5)/2, 1)$ if i is odd and we add the entry in cell $((i-2m+4)/2, 2)$ if i is even. If i is odd, then

$$\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant \frac{1}{k-m} \tag{3.8}$$

by Lemma 3.2.8, since there is only one non-empty cell of P_i in row $(i-2m+5)/2$. If $i \equiv 0 \bmod 4$, then

$$\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant \frac{2}{k-m} \tag{3.9}$$

by Lemma 3.2.9. If $i \equiv 2 \bmod 4$, we simply use $\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant 1$.

For $i \in \{4m-3, \ldots, m^2\}$, we add the entry of P in cell $(3 + \lfloor (i-4m+3)/(m-2) \rfloor, 3 + ((i-4m+3) \bmod (m-2)))$ (this is the natural ordering for the cells in $\{3, 4, \ldots, m\}^2$). If $i \equiv 4 \bmod (m-2)$ (in which case the added entry is in column m), then

$$\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant \frac{m(1 + O(m/n))}{n} \tag{3.10}$$

by Lemma 3.2.10. If $i \geqslant m^2 - m + 3$ (in which case the added entry is in row m), then

$$\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant \frac{m}{k-m} \tag{3.11}$$

by Lemma 3.2.9. For all other values of i, we use $\Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \leqslant 1$.

Overall, we use (3.6) for $3m/2$ values of i, corresponding to the m entries in the first row and $m/2$ entries in the second row. We use (3.7) for $m/2$ values of i, corresponding to entries in the second row. We use (3.8) for $m-2$ values of i, corresponding to entries in the first column. We use (3.9) for $m/2-1$ values of i, corresponding to entries in the second column. We use (3.10) for $m-2$ values of i, corresponding to entries in the m-th column. We use (3.11) for $m-3$ values of i, corresponding to entries in the m-th row. Hence, by the chain rule of probability,

$$\begin{aligned}\Pr(\mathbf{L} \supseteq P) &= \prod_{i=1}^{m^2} \Pr(\mathbf{L} \supseteq P_i \mid \mathbf{L} \supseteq P_{i-1}) \\ &\leqslant \left(\frac{1 + O(m/n)}{n}\right)^{3m/2} \left(\frac{2(1 + O(m/n))}{n}\right)^{m/2} \left(\frac{1}{k-m}\right)^{m-2}\end{aligned}$$

$$\cdot \left(\frac{2}{k-m}\right)^{m/2-1} \left(\frac{m(1+O(m/n))}{n}\right)^{m-2} \left(\frac{m}{k-m}\right)^{m-3}$$
$$= \frac{2^{m-1}m^{2m-5}}{(k-m)^{5m/2-6}} \left(\frac{1+O(m/n)}{n}\right)^{3m-2}.$$

If m is even and $k = m$, then the same bounds hold except we use the trivial bound in place of (3.8), (3.9), and (3.11).

The argument when m is odd is similar. We use (3.6) for $(3m+1)/2$ entries, namely m entries in the first row and $(m+1)/2$ entries in the second row. We use (3.7) for $(m-1)/2$ entries in the second row. If $k > m$, then we use (3.8) for $m-2$ entries in the first column and (3.9) for $(m-3)/2$ entries in the second column. We use (3.10) for $m-2$ entries in the m-th column and if $k > m$, then we use (3.11) for $m-3$ entries in the m-th row. As a consequence,

$$\Pr(\mathbf{L} \supseteq P) \leqslant \frac{2^{m-2}m^{2m-5}}{(k-m)^{(5m-13)/2}} \left(\frac{1+O(m/n)}{n}\right)^{3m-2}, \tag{3.12}$$

with $k-m$ replaced by 1 in the case where $k = m$. As foreshadowed after (3.4), we now multiply by m^{m^2} to give the claimed upper bound on $\mathbf{L}[R, C]$ being any subsquare on the symbols $[m]$. □

3.2.3 Proof of Theorem 3.0.1

We are now ready to prove our first main theorem.

Proof of Theorem 3.0.1. There are $\binom{k}{m}$ choices for the set R and there are $\binom{n}{m}^2$ choices for the sets C and S in Theorem 3.2.1 and Theorem 3.2.7. From Theorem 3.2.1 and $\binom{n}{m} \geqslant (n/m)^m$, we obtain

$$\mathbb{E}_m(k,n) \leqslant \frac{kn(k+1-m)(n+1-m)}{m^2\binom{n}{m}} \leqslant \frac{m^{m-2}}{n^{m-4}} = \frac{m^4}{n^2}\left(\frac{m}{n}\right)^{m-6} \leqslant \frac{m^4}{n^2 2^{m-6}} = O(n^{-2}), \tag{3.13}$$

provided $m \geqslant 6$.

For $m \in \{4,5\}$ and $k > m$, we use Theorem 3.2.7 to deduce that

$$\mathbb{E}_4(k,n) \leqslant \binom{k}{4}\binom{n}{4}^2 O(1) \left(\frac{1+O(1/n)}{n}\right)^{10} \left(\frac{1}{k-4}\right)^4 = O(n^{-2})$$

and

$$\mathbb{E}_5(k,n) \leqslant \binom{k}{5}\binom{n}{5}^2 O(1) \left(\frac{1+O(1/n)}{n}\right)^{13} \left(\frac{1}{k-5}\right)^6 = O(n^{-3}).$$

When $k = m \in \{4,5\}$, all terms involving k can be omitted, with the conclusion unchanged. Combining with (3.13), we have the result. □

3.3 Subsquares of order 2 or 3

From Theorem 3.0.1, we know that $\mathbb{E}_m(k,n)$ is asymptotically 0 whenever $4 \leqslant m \leqslant \min\{k, n/2\}$. In this last section, we prove our main results concerning subsquares of orders 2 and 3. We first consider subsquares of order 3. Although we are not able to resolve the situation completely, Theorem 3.0.3 marks the first progress on Conjecture 2.2.4(*ii*) as well as the first progress on Conjecture 2.2.8(*ii*) that applies for all $k \leqslant n$. The proof of Theorem 3.0.3 follows the derivation of (3.12) closely, but when $m = 3$ that derivation was slightly conservative when counting entries in the second column to which Lemma 3.2.9 can be applied.

Proof of Theorem 3.0.3. Let M denote the Latin square

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

with the same colouring convention as used in Figure 3.2. Let P be the partial $k \times n$ Latin rectangle such that $P[\{1,2,3\},\{1,2,3\}] = M$ and every cell of P outside of $\{1,2,3\}^2$ is empty. We first bound the probability that a random $k \times n$ Latin rectangle $\mathbf{L}$ contains P in the case where $k > 3$. We define a family of partial Latin rectangles $P_i \subseteq P$ as follows. Let $P_0 = \varnothing$ and for $i \in \{1,2,\dots,9\}$, let P_i be obtained from P_{i-1} by adding the entry of P in the cell given by the i-th element of the tuple $((1,1),(2,1),(1,2),(2,2),(1,3),(2,3),(3,1),(3,2),(3,3))$. For $i \in \{1,2,3,4,5\}$, Lemma 3.2.8 implies that (3.6) holds. For $i = 6$, Lemma 3.2.10 implies that (3.7) holds. For $i = 7$, Lemma 3.2.8 implies that (3.8) holds. For $i = 8$, Lemma 3.2.9 implies that (3.9) holds. Finally, Lemma 3.2.10 implies that $\Pr(\mathbf{L} \supseteq P_9 \mid \mathbf{L} \supseteq P_8) \leqslant 3(1+O(1/n))/n$. The chain rule of probability implies that

$$\Pr(\mathbf{L} \supseteq P) \leqslant 12\left(\frac{1+O(1/n)}{n}\right)^7\left(\frac{1}{k-3}\right)^2 = \frac{12}{n^7(k-3)^2}\left(1+O\left(\frac{1}{n}\right)\right).$$

Since there are 12 Latin squares of order 3 we obtain

$$\mathbb{E}_3(k,n) \leqslant \binom{k}{3}\binom{n}{3}^2\frac{144}{n^7(k-3)^2}\left(1+O\left(\frac{1}{n}\right)\right) = \frac{2k}{3n}\left(1+O\left(\frac{1}{k}\right)\right),$$

as required. If $k = 3$, then we instead get

$$\mathbb{E}_3(k,n) \leqslant \binom{n}{3}^2\frac{72}{n^7}\left(1+O\left(\frac{1}{n}\right)\right) = \frac{2}{n}\left(1+O\left(\frac{1}{n}\right)\right). \qquad \square$$

Finally, we turn our attention to intercalates. Before proving Theorem 3.0.4, we need the following lemma.

Lemma 3.3.1. *Let $\mathbf{L}$ be a random $k \times n$ Latin rectangle and let $\{i,j\} \subseteq [k]$ with $i \neq j$. The probability that $\mathbf{L}[\{i,j\},[n]]$ contains at least $t = t(n)$ intercalates is at most $\exp(-\Omega(t \log t))$.*

Proof. Let P be the partial $k \times n$ Latin rectangle which is empty except that:

- $P_{i,\ell} = \ell$ for every $\ell \in [2t]$,
- $P_{j,\ell} = \ell + 1$ for every odd $\ell \in [2t]$, and
- $P_{j,\ell} = \ell - 1$ for every even $\ell \in [2t]$.

First suppose that $t \leqslant n/4$, so that we can use the arguments behind (3.6) and (3.7) to obtain

$$\Pr(\mathbf{L} \supseteq P) \leqslant 2^t n^{-4t} \left(1 + O\left(\frac{t}{n}\right)\right)^{4t}.$$

For t intercalates in general position in a $k \times n$ Latin rectangle, there are $\binom{n}{2t}$ choices for the symbols, $(2t)!/(2^t t!)$ ways to pair them, and then $n!/(n-2t)!$ ways to allocate the columns. Thus, the probability that $\mathbf{L}[\{i,j\},[n]]$ contains at least t intercalates is at most

$$\left(\frac{n!}{(n-2t)!}\right)^2 \frac{1}{2^t t!} 2^t n^{-4t} \left(1 + O\left(\frac{t}{n}\right)\right)^{4t} = \exp(-\Omega(t \log t)),$$

as required.

Now suppose that $n/4 < t \leqslant n/2$. The probability that $\mathbf{L}[\{i,j\},[n]]$ contains t intercalates is at most the probability that $\mathbf{L}[\{i,j\},[n]]$ contains $n/4$ intercalates, which is $\exp(-\Omega((n/4)\log(n/4)) = \exp(-\Omega(t \log t))$, as required. □

We are now ready to prove Theorem 3.0.4.

Proof of Theorem 3.0.4. Since [39, Corollary 1.7] proves the claim when $k \leqslant (1/2 - o(1))n$, we may assume that $k = \Theta(n)$, which means that arguments that have previously been used for counting intercalates in Latin squares apply with only minor changes. Let k' be an integer function of n with $0 \leqslant k' \leqslant k$. For a $k' \times n$ Latin rectangle T, let $\mathcal{R}(T)$ be the set of $k \times n$ Latin rectangles L such that $L[[k'],[n]] = T$. By [90, Proposition 4], if T and T' are $k' \times n$ Latin rectangles, then

$$\frac{|\mathcal{R}(T)|}{|\mathcal{R}(T')|} \leqslant \exp(O(n \log^2 n)). \tag{3.14}$$

Let $\mathbf{N}$ denote the number of intercalates in a random $k \times n$ Latin rectangle. Modifying the proof of [78, Theorem 4] by using Lemma 3.3.1 instead of [78, Theorem 3] and using (3.14) gives

$$\Pr(\mathbf{N} \leqslant (1-\delta)k^2/4) \leqslant \exp(-\Omega(n^{1/2} \log^{-1} n)), \tag{3.15}$$

for fixed $\delta \in (0,1]$. Similarly, a simple adaptation of the proof of [77, Theorem 2.1] using (3.14) gives

$$\Pr(\mathbf{N} \geqslant (1+\delta)k^2/4) \leqslant \exp(-\Omega(n^{4/3} \log n)), \tag{3.16}$$

for fixed $\delta > 0$. Combining (3.15) and (3.16) proves the theorem. □

Chapter 4

Latin squares without proper subsquares

We begin this chapter by generalising Latin squares to higher dimensions. Throughout this chapter, n and d will be positive integers and throughout this introductory section, I_i will be a set of cardinality n for each $i \in [d]$, I will be the set $I_1 \times I_2 \times \cdots \times I_d$, and Σ will be a set of cardinality n.

Definition 4.0.1. A map $H : I \to \Sigma$ is a d-dimensional *Latin hypercube* of order n if

$$\{H(c_1, \ldots, c_{k-1}, x, c_{k+1}, \ldots, c_d) : x \in I_k\} = \Sigma$$

for each $(c_1, c_2, \ldots, c_d) \in I$ and $k \in [d]$.

We can naturally think of a Latin hypercube $H : I \to \Sigma$ as a d-dimensional array whose i-th axis is indexed by I_i. We will treat the map H and the corresponding array as interchangeable objects. Thus, a 1-dimensional Latin hypercube is a bijection and a 2-dimensional Latin hypercube is a Latin square. A *Latin cube* is a 3-dimensional Latin hypercube.

Definition 4.0.2. Suppose that $d \geqslant 2$ and let $H : I \to \Sigma$ be a d-dimensional Latin hypercube of order n.

- A *Latin subhypercube* of H is a restriction $H|_J$ of H for some $J \subseteq I$ such that $H|_J : J \to H(J)$ is a Latin hypercube.
- A *proper subhypercube* of H is a Latin subhypercube of H of order k with $1 < k < n$.
- An N_∞ Latin hypercube is a Latin hypercube with no proper subhypercubes.

We will generally refer to a Latin subhypercube simply as a subhypercube. Also, if $H : I \to \Sigma$ is a d-dimensional Latin hypercube of order n, then we will generally assume that $I = [n]^d$ and $\Sigma = [n]$. However, we need to allow subhypercubes to have more general index sets.

The goal of this chapter is to resolve the existence problem for N_∞ Latin hypercubes by proving the following theorem.

Theorem 4.0.3. *Let $d \geqslant 2$ and n be positive integers. There exists an N_∞ Latin hypercube of order n and dimension d if and only if $(n, d) \notin \{(4, 2), (6, 2)\}$.*

The $d = 2$ case of Theorem 4.0.3 resolves Conjecture 2.2.13.

The structure of this chapter is as follows. In §4.1, we present some background material. In §4.2, we resolve Conjecture 2.2.13 by constructing N_∞ Latin squares of orders of the form $2^a 3^b$ with $a \geqslant 1$ and $b \geqslant 0$. In §4.3, we extend our results from §4.2 to prove Theorem 4.0.3.

4.1 Background

In this section, we introduce some material needed to prove Theorem 4.0.3. Throughout this chapter, unless otherwise stated, the row indices and column indices of an $n \times n$ matrix will be $[n]$ and the symbol set of a Latin square of order n will be $[n]$. When dealing with the set $[n]$, all operations will be modulo n.

Let L be a Latin square. For this chapter, we will extend Definition 2.1.6 so that any Latin square that can be obtained from L by permuting its rows, permuting its columns, and renaming its symbols is *isotopic* to L. With this extended definition, the Latin squares in Figure 4.1 are isotopic.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \\ 6 & 5 & 2 & 1 & 3 & 4 \\ 4 & 6 & 5 & 3 & 1 & 2 \\ 2 & 1 & 4 & 5 & 6 & 3 \\ 5 & 3 & 6 & 2 & 4 & 1 \end{bmatrix} \qquad \begin{bmatrix} c & d & a & f & b & e \\ a & b & c & d & e & f \\ b & a & d & e & f & c \\ f & e & b & a & c & d \\ d & f & e & c & a & b \\ e & c & f & b & d & a \end{bmatrix}$$

Figure 4.1: The square on the right in this figure can be obtained from the square on the left by applying the permutation $(1, 2)(3, 4, 5)$ to its rows, applying the identity permutation Id to its columns, and renaming its symbols via the map γ defined by

x	1	2	3	4	5	6
$\gamma(x)$	a	b	c	d	e	f

.

We will also extend the definition of a species to Latin hypercubes. Let $H : [n]^d \to [n]$ and $H' : [n]^d \to [n]$ be Latin hypercubes. We can identify H with the set of $(d+1)$-tuples

$$\left\{(x_1, x_2, \ldots, x_d, H(x_1, x_2, \ldots, x_d)) : (x_1, x_2, \ldots, x_d) \in [n]^d\right\}.$$

A *conjugate* of H is a Latin hypercube obtained from H by uniformly permuting the elements of each of its $(d+1)$-tuples. If there exists $\{\alpha_1, \alpha_2, \ldots, \alpha_{d+1}\} \subseteq \mathrm{Sym}([n])$ such that

$$H' = \{(\alpha_1(x_1), \alpha_2(x_2), \ldots, \alpha_{d+1}(x_{d+1})) : (x_1, x_2, \ldots, x_{d+1}) \in H\},$$

then H and H' are *isotopic*. If H is isotopic to some conjugate of H', then H and H' are *paratopic*. A *species* is a maximal set of pairwise paratopic Latin hypercubes.

Let L be an $n \times n$ matrix. The *principal entry* of L is the entry $(1, 1, L_{1,1})$. If L' is another $n \times n$ matrix such that $|L \cap L'| = n^2 - k$, then we say that L and L' *agree* in all but k entries.

Let L be an $n \times n$ matrix, let M be another matrix (not necessarily of dimension $n \times n$), and let $\mathcal{S}$ be a set of entries of M. Suppose that each entry in $\mathcal{S}$ is in a cell (i, j) for some $\{i, j\} \subseteq [n]$. Then the *shadow of* $\mathcal{S}$ *in* L is the set of entries $\{(i, j, L_{i,j}) : (i, j, M_{i,j}) \in \mathcal{S}\}$ of L. See Figure 4.2 for an example of this concept.

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

Figure 4.2: Let L be the Latin square on the left, let M be the Latin square on the right, and let $\mathcal{S}$ be the set of blue highlighted entries of M. Then the green highlighted entries of L form the shadow of $\mathcal{S}$ in L.

Definition 4.1.1. Let L be a Latin square of order n, let $\{i, j\} \subseteq [n]$, and let σ be any symbol other than $L_{i,j}$. The matrix obtained from L by replacing the entry $(i, j, L_{i,j})$ by (i, j, σ) is denoted by $\sigma \hookrightarrow L_{i,j}$. Such a matrix is called a *near copy* of L.

Let L be a Latin square of order n and let $\sigma \hookrightarrow L_{i,j}$ be a near copy of L. We stress that σ may or may not be a member of $[n]$, but if it is, then $\sigma \hookrightarrow L_{i,j}$ will contain two copies of σ in row i and column j.

The following definition generalises Definition 4.1.1.

Definition 4.1.2. Let L be a Latin square of order n and let $k \leqslant n^2$ be a positive integer. Let $\{(x_i, y_i) : i \in [k]\}$ be a set of k distinct cells in L. Also, let σ_i be a symbol other than L_{x_i,y_i} for each $i \in [k]$. Let L' be obtained from L by replacing each entry (x_i, y_i, L_{x_i,y_i}) by (x_i, y_i, σ_i). Then L' is a *k-near copy* of L.

(*i*) An *alien entry* of L' is an entry (x_i, y_i, σ_i) for some $i \in [k]$.

(*ii*) A *native entry* of L' is any entry of L' that is not an alien entry.

(*iii*) A *native symbol* of L' is a symbol in a native entry of L'.

(*iv*) A *hole* in L' is a cell (x_i, y_i) for some $i \in [k]$.

(*v*) The *displaced native* of L' from hole (x_i, y_i) is the symbol L_{x_i,y_i}.

Let L' be an $n \times n$ matrix and let $\pi \in L'$. Let L_1 and L_2 be Latin squares of order n such that L' is a k_1-near copy of L_1 and a k_2-near copy of L_2 for some positive integers $k_1 \leqslant n^2$ and $k_2 \leqslant n^2$. Whether π is an alien entry of L' depends on which Latin square we are considering L' to be a k-near copy of. Thus, if we are considering L' to be both a k_1-near copy of L_1 and a k_2-near copy of L_2, then we will adopt the following convention for clarity: If $\pi \notin L_1$, then we will say that π is an alien entry of L' with respect to L_1 and if $\pi \notin L_2$, then we will say that π is an alien entry of L' with respect to L_2. We will adopt analogous conventions for Definitions 4.1.2(*ii*)–(*v*) as required.

Let L and L' be as in Definition 4.1.2 and let T be a submatrix of L' that contains an alien entry π of L'. Then we will say that π is an alien entry of T (with respect to L). We will extend Definitions 4.1.2(ii)–(v) to submatrices of L' in a similar fashion.

We next extend the definition of subsquares to k-near copies of Latin squares. Let L' be a k-near copy of a Latin square L for some integer k. A *subsquare* of L' is a submatrix of L' that is itself a Latin square. As for Latin squares, we call a subsquare of order 2 an intercalate.

It is well known that any proper subsquare of a Latin square L cannot have order more than half the order of L. However, this is not true in near copies of Latin squares, as demonstrated by the shaded subsquare in

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

Nevertheless, a subsquare of a near copy of L cannot have order much larger than half the order of L.

Lemma 4.1.3. *Let M be a near copy of a Latin square L of order $n > 1$. Suppose that $\mathcal{S}$ is a subsquare of M of order s. Then $s \leqslant (n+1)/2$.*

Proof. Let T be the submatrix of M induced by the rows and columns that do not hit $\mathcal{S}$. Note that T is not empty, because M is not a Latin square. Suppose that σ is any symbol that occurs in $\mathcal{S}$ and does not occur in the alien entry of M. Then σ must occur s times in $\mathcal{S}$ and $n-s$ times in T. We have at least $s-1$ choices for σ, but we only have room for $n-s$ of them within T. Hence, $s-1 \leqslant n-s$, as required. □

Another simple result we will need is the following well known lemma.

Lemma 4.1.4. *Let L and M be distinct Latin squares on the same set of symbols. If M is a k-near copy of L, then $k \geqslant 4$ with equality only possible if L and M both contain an intercalate.*

For the remainder of this section, let m be a positive integer. Denote by $\prec_1$ the total order on $[n] \times [m]$ defined by $(a_1, b_1) \prec_1 (a_2, b_2)$ if $a_1 < a_2$ or $a_1 = a_2$ and $b_1 < b_2$. In any context where a total order on $[n] \times [m]$ is required, we will implicitly be using $\prec_1$.

We now discuss ways to 'multiply' Latin squares together to build larger ones. We start with the most natural definition of a product of Latin squares.

Definition 4.1.5. Let L be a Latin square of order n and let M be a Latin square of order m. The *direct product* of L and M, denoted by $L \times M$, is the Latin square of order nm whose rows and columns are indexed by $[n] \times [m]$ that is defined by $(L \times M)_{(i,j),(k,\ell)} = (L_{i,k}, M_{j,\ell})$.

Let L be a Latin square of order n and let M be a Latin square of order m. The direct product $L \times M$ decomposes into n^2 subsquares, each of which is isotopic to M. These subsquares are referred to as *M-blocks*. Explicitly, for $i \in [n]$ define $\mathscr{J}_i = \{(i, \ell) : \ell \in [m]\}$. Then an M-block of $L \times M$ is a submatrix $(L \times M)[\mathscr{J}_i, \mathscr{J}_j]$ for some $\{i, j\} \subseteq [n]$. For $i \in [m]$, define $\mathscr{K}_i = \{(\ell, i) : \ell \in [n]\}$. Then any submatrix $(L \times M)[\mathscr{K}_i, \mathscr{K}_j]$ with $\{i, j\} \subseteq [m]$ is a subsquare that is isotopic to L, which we will refer to as an *L-block*.

Let $\mathcal{S}$ be a submatrix of any matrix whose row indices, column indices, and symbol set are $[n] \times [m]$. Let $\Phi_1 : [n] \times [m] \to [n]$ denote the projection onto the first coordinate and let

$\Phi_2 : [n] \times [m] \to [m]$ denote the projection onto the second coordinate. We denote by $\Phi_1(\mathcal{S})$ the set of triples $\{(\Phi_1(r), \Phi_1(c), \Phi_1(s)) : (r, c, s) \in \mathcal{S}\}$. Let L be a Latin square of order n that contains $\Phi_1(\mathcal{S})$. We can consider $\Phi_1(\mathcal{S})$ as a set of entries of L, which we call the *projection of* $\mathcal{S}$ *onto* L. Similarly, if M is a Latin square of order m and $\Phi_2(\mathcal{S}) = \{(\Phi_2(r), \Phi_2(c), \Phi_2(s)) : (r, c, s) \in \mathcal{S}\} \subseteq M$, then we can consider $\Phi_2(\mathcal{S})$ to be a set of entries of M called the *projection of* $\mathcal{S}$ *onto* M.

In order to prove Theorem 4.0.3, we need the *corrupted product* defined in [117]. Let ζ be a positive integer, let A be an N_∞ square of order ζ, and let B be a square that is isotopic to A and which has the same symbol set as A. The pair (A, B) is a *corrupting pair* of order ζ if:

- $A_{i,j} = B_{i,j}$ if and only if $i = j = 1$, and
- for all $\{i, j\} \subseteq [\zeta]$, there is no proper subsquare of $B_{i,j} \hookrightarrow A_{i,j}$ involving its principal entry.

See Figure 4.3 for an example of a corrupting pair.

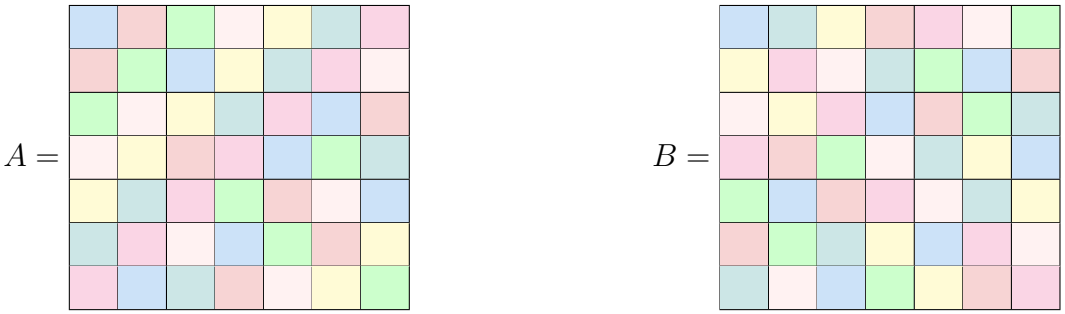

Figure 4.3: The pair (A, B) forms a corrupting pair of order 7. Note that here we are using colours as the 'symbols' of the Latin squares A and B.

Definition 4.1.6. Let ζ and μ be positive integers, let (A, B) be a corrupting pair of order ζ, let M be an N_∞ square of order μ, and let $s \in [\mu - 1]$. The *corrupted product* $\mathbb{P} = (A, B) *_s M$ of shift s is the Latin square of order $\zeta\mu$ whose rows and columns are indexed by $[\zeta] \times [\mu]$ that is defined by

$$\mathbb{P}_{(i,j),(k,l)} = \begin{cases} (A_{i,k}, M_{j,\ell} + s) & \text{if } i = k = 1, \\ (B_{i,k}, M_{j,\ell}) & \text{if } j = l = 1 \text{ and } (i, k) \neq (1, 1), \\ (A_{i,k}, M_{j,\ell}) & \text{otherwise.} \end{cases}$$

See Figure 4.4 and Figure 4.5 for an example of a direct product and a corrupted product, respectively.

Let L be a Latin square of order n, let M be a Latin square of order m, and let F be a k-near copy of $L \times M$ for some positive integer $k \leqslant nm$. We extend the definitions of M-blocks and L-blocks to near copies of $L \times M$ as follows. An *M-block* of F is a submatrix $T = F[\mathscr{J}_i, \mathscr{J}_j]$ for some $\{i, j\} \subseteq [n]$. The position of T is (i, j). If $(i, j) = (1, 1)$, then T is the *principal M-block* of F. The *principal entry* of T is the entry $((i, 1), (j, 1), F_{(i,1),(j,1)})$. Similarly, the *$L$-block* of F in position (i, j) is the submatrix $F[\mathscr{K}_i, \mathscr{K}_j]$, which has principal entry $((1, i), (1, j), F_{(1,i),(1,j)})$. The *principal L-block* of F is the L-block in position $(1, 1)$. We will refer to M-blocks and L-blocks collectively as *blocks*. Note that in $L \times M$, any block is a subsquare. This is not

1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	3	3	1	2	3	1	2

Figure 4.4: The direct product $A \times M$ where A is from Figure 4.3 and M is the Latin square

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}. \tag{4.1}$$

Instead of an ordered pair, every 'symbol' of this Latin square is a colour-integer pair.

necessarily true in F. We call the first coordinate of a symbol of F the L-coordinate and we call the second coordinate the M-coordinate.

With the above terminology, we can give an intuitive description of the corrupted product. The square $\mathbb{P}$ from Definition 4.1.6 can be obtained from the direct product $A \times M$ as follows. First, replace the principal A-block of $A \times M$ by the principal B-block of $B \times M$. Then, add s to the M-coordinate of each symbol in the principal M-block of the resulting matrix.

Let ζ and μ be positive integers, let (A, B) be a corrupting pair of order ζ, let M be an N_∞ square of order μ, let $s \in [\mu - 1]$, and let $\mathbb{P} = (A, B) *_s M$. Each A-block of $\mathbb{P}$ is a near copy of a Latin square that is isotopic to A. The principal M-block of $\mathbb{P}$ is a subsquare of $\mathbb{P}$, which we will denote by $\mathbb{T}_M$. Any other M-block of $\mathbb{P}$ is a near copy of a Latin square that is isotopic to M. If the matrix $(M_{i,j} + s) \hookrightarrow M_{i,j}$ does not contain a subsquare isotopic to A for any $\{i, j\} \subseteq [\mu]$, then s is an *allowable shift* with respect to (A, M). If $(M_{i,j} + s) \hookrightarrow M_{i,j}$ does not contain a subsquare of order ζ for any $\{i, j\} \subseteq [\mu]$, then s is a *strong allowable shift* with respect to (A, M). Our interest in corrupted products is due to the following result [117].

2	3	1	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
3	1	2	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
1	2	3	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
3	1	2	3	1	2	3	1	2	3	1	2	3	1	3	3	1	2	3	1	2

Figure 4.5: The corrupted product $(A, B) *_1 M$ where A and B are from Figure 4.3 and M is the square (4.1). As in Figure 4.4, every 'symbol' of this Latin square is a colour-integer pair.

Theorem 4.1.7. *Let ζ and μ be positive integers with $\zeta < \mu$, let (A, B) be a corrupting pair of order ζ, let M be an N_∞ square of order μ, and let $s \in [\mu - 1]$. If s is an allowable shift with respect to (A, M), then the only proper subsquare of the corrupted product $(A, B) *_s M$ is $\mathbb{T}_M$.*

Recall the definition of row cycle switching from §3.1. To prove Theorem 4.0.3, we will first resolve Conjecture 2.2.13 by constructing an N_∞ Latin square of order n for any $n \notin \{4, 6\}$ of the form $2^a 3^b$ where $a \geqslant 1$ and $b \geqslant 0$ are integers. The construction is recursive and will work as follows. Given an N_∞ Latin square of some order μ, we use the corrupted product to construct Latin squares of orders 8μ and 9μ that contain exactly one proper subsquare. We then use row cycle switching to destroy this subsquare in such a way as to not create any new subsquares.

We now describe a method to create new Latin squares from old ones that is similar to cycle switching. This method will only be used to construct N_∞ squares that we need as the base cases for our recursive construction. Let L be a Latin square of order n. Suppose that there are three distinct rows i, j, and k, distinct columns x and y, and symbols a and b of L such that: $L_{i,x} = a = L_{k,y}$, $L_{i,y} = b = L_{j,x}$, and b is contained in the cycle of the row permutation $\tau_{j,k}$ of L that contains a. Write this cycle as $(a, z_1, z_2, \ldots, z_\ell, b, \ldots)$. Let $c_0 \in [n]$ be such that $L_{j,c_0} = a$

and for $w \in [\ell]$, let $c_w \in [n]$ be such that $L_{j,c_w} = z_w$. A Latin square L' can be defined by

$$L'_{u,v} = \begin{cases} b & \text{if } (u,v) \in \{(i,x),(k,y),(j,c_\ell)\}, \\ a & \text{if } (u,v) \in \{(j,x),(i,y),(k,c_0)\}, \\ z_w & \text{if } (u,v) \in \{(j,c_{w-1}),(k,c_w)\}, \\ L_{u,v} & \text{otherwise.} \end{cases}$$

We will let $\eta(i,j,x)$ denote the set of entries in cells

$$\{(i,x),(i,y),(j,x),(k,y)\} \cup \{(j,c_w),(k,c_w) : w \in [\ell] \cup \{0\}\},$$

and we will say that L' has been obtained from L by switching on $\eta(i,j,x)$. See Figure 4.6 for an example.

$$\begin{array}{c} \\ k \\ i \\ \\ \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} c_0 & x & & y & c_1 & & & \end{array} \\ \left[\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 7 & 8 & 1 & 6 & 4 \\ 3 & 1 & 8 & 5 & 6 & 4 & 2 & 7 \\ 4 & 7 & 1 & 8 & 3 & 2 & 5 & 6 \\ 5 & 6 & 7 & 1 & 4 & 3 & 8 & 2 \\ 6 & 4 & 2 & 3 & 7 & 8 & 1 & 5 \\ 7 & 8 & 4 & 6 & 2 & 5 & 3 & 1 \\ 8 & 5 & 6 & 2 & 1 & 7 & 4 & 3 \end{array}\right] \end{array} \tag{4.2}$$

Figure 4.6: The highlighted entries of this Latin square form $\eta(4,7,2)$. Switching on $\eta(4,7,2)$ involves swapping each highlighted symbol with the other highlighted symbol in the same column.

4.2 Latin squares without proper subsquares

In this section, we resolve Conjecture 2.2.13 by proving the following theorem.

Theorem 4.2.1. *There exists an N_∞ Latin square of order n for all $n \notin \{4,6\}$.*

To prove Theorem 4.2.1, we will need some preliminary lemmas.

Lemma 4.2.2. *Let L' be a near copy of a Latin square L and let π be the alien entry of L'. Let T be a submatrix of L' that does not contain π. Suppose that T is a k-near copy of some N_∞ square N where $k \in \{0,1,2\}$. Suppose further that no symbol in an alien entry of T is native to T. Also suppose that L' has a subsquare $\mathcal{S}$ that meets T in at least two entries. Let $V = \mathcal{S} \cap T$ and suppose that*

- *V has more than k columns, and*
- *V hits a row r of L' that contains none of the holes in T.*

Then one of the following is true:

- $V = T$,
- V *has exactly* k *rows and* $k+1$ *columns,*
- $k = 2$ *and the two alien entries of* T *are* $(x_1, y_1, \sigma_1) \in V$ *and* $(x_2, y_2, \sigma_2) \notin V$. *Furthermore, the shadow of* V *in* $\epsilon \hookrightarrow N_{x_1,y_1}$ *is a subsquare, where* ϵ *is the displaced native of* T *from* (x_2, y_2). *Also, either* $x_1 = x_2$ *and* π *is in column* y_1 *or* $y_1 = y_2$ *and* π *is in row* x_1.

Proof. Let R be the set of rows of V and let C be the set of columns of V. We will assume that $|R| \neq k$ or $|C| \neq k+1$, since otherwise the lemma holds. Let Σ be the set of native symbols of T in V. Since $|C| > k$, there is some column $c \in C$ that contains no holes in T.

Aiming for a contradiction, suppose that $|R| > |C|$. Since $|C| > k$, it follows that $|R| \geqslant k+2$ and V must hit at least two rows that contain none of the holes in T. Let r' be one such row that does not contain π. Each of the $|R|$ symbols in column c of V is native to T and hence must occur in row r' of T. But these symbols must also occur in row r' of $\mathcal{S}$, since $\mathcal{S}$ is a Latin square. So there are at least $|R|$ symbols in row r' of V, which forces $|C| \geqslant |R|$.

We now show that $|R| = |C| = |\Sigma|$. Row r of T contains only native symbols of T and so $|\Sigma| \geqslant |C|$. Suppose, for a contradiction, that $|\Sigma| > |R|$ and hence there is some symbol $\sigma \in \Sigma$ that does not occur in column c of V. But σ does occur in column c of T, say in row r''. So $\mathcal{S}$ is a Latin square that hits column c, contains symbol σ, but does not hit row r''. Thus, π must occur in column c and have symbol σ. Since L' contains only one alien entry with respect to L, we know that our choices for c and σ were both forced. It follows that $|R| + 1 = |\Sigma| \geqslant |C| = k+1 \geqslant |R|$. We are assuming that $|R| \neq k$ or $|C| \neq k+1$, thus the only possibility is that $|R| = |C| = k+1$ and $|\Sigma| = k+2$. Since $|\Sigma| > |C|$, it follows that there is a symbol $\sigma' \in \Sigma$ that does not occur in row r of V. Transposing the argument we just used for σ, but applying it to σ', we deduce that π must occur in row r. But then π occurs in row r and column c, thus $\pi \in T$, which is a contradiction. This contradiction implies that $|R| = |C| = |\Sigma|$.

Consider the $|R| \times |R|$ matrix M that is the shadow of V in N. If M contains exactly $|R|$ symbols, then it is a subsquare of N, so must be equal to N, since N is N_∞. In that case we would have $V = T$, so we may assume that V contains a hole (x, y) such that $M_{x,y} \notin \Sigma$. Row r contains no hole in T and thus there is a symbol $\lambda \in \Sigma$ that occurs in row r of M but not in row x of M. Since $\mathcal{S}$ is a Latin square that hits row x and symbol λ, we must have that either (i) π occurs in row x and contains symbol λ or (ii) λ is the displaced native from a hole (x, y') in row x. In the latter case, (x, y') is outside of V because λ does not occur in row x of M. Similar logic can be applied to show that an analogue of options (i) or (ii) must also hold for columns. However, π cannot be in row x and also in column y because $\pi \notin T$. Also, there is at most one hole in T other than (x, y). We conclude that there must be two holes, with the second hole lying in whichever of row x and column y does not contain π. Let ϵ be the displaced native from the hole that is not (x, y) and consider the matrix $M' = \epsilon \hookrightarrow M_{x,y}$. We note that the symbols in M' must be precisely Σ and that no symbol is duplicated within any row or column of M' with the possible exception that ϵ might occur twice within row x or within column y (but not both). A consequence is that each of the $|R|$ symbols in Σ occurs exactly $|R|$ times in M'. It then follows that ϵ cannot be duplicated within row x or column y, so M' is a Latin square. □

We next use Lemma 4.2.2 to prove the following result (c.f. [117, Lemma 7]).

Lemma 4.2.3. *Let L' be a near copy of a Latin square L and let π be the alien entry of L'. Let T be a submatrix of L' that does not contain π. Suppose that T is a k-near copy of some N_∞ square N where $k \in \{0,1,2\}$. Suppose further that no symbol in an alien entry of T is native to T. Also suppose that L' has a subsquare $\mathcal{S}$ that meets T in at least two entries. Let $V = \mathcal{S} \cap T$, let R be the set of rows of V, and let C be the set of columns of V.*

(i) If $k = 0$, then $\mathcal{S}$ contains T,

(ii) If $k = 1$, then let (r, c, σ) be the alien entry of T. One of the following is true:

(1) $\mathcal{S}$ contains T,

(2) $R = \{r\}$ and $C = \{c, c'\}$ for some c'. Furthermore, π is in column c and has symbol $L'_{r,c'}$,

(3) $R = \{r, r'\}$ for some r' and $C = \{c\}$. Furthermore, π is in row r and has symbol $L'_{r',c}$,

(4) $R = \{r'\} \neq \{r\}$ and $C = \{c, c'\}$ for some c'. Furthermore, π is in column c' and has symbol $L'_{r',c}$ and $L'_{r',c'}$ is the displaced native from the hole (r, c) in T,

(5) $R = \{r, r'\}$ for some r' and $C = \{c'\} \neq \{c\}$. Furthermore, π is in row r' and has symbol $L'_{r,c'}$ and $L'_{r',c'}$ is the displaced native from the hole (r, c) in T.

(iii) If $k = 2$, then one of the following is true:

(1) $\mathcal{S}$ contains T,

(2) $|R| \leqslant 3$ and $|C| \leqslant 3$ with $\min\{|R|, |C|\} < 3$,

(3) T has alien entries $(r, c, \sigma) \in V$ and $(r', c', \sigma') \notin V$. The shadow of V in $\epsilon \hookrightarrow N_{r,c}$ is a subsquare where ϵ is the displaced native from (r', c'). Also, either $r = r'$ and π is in column c or $c = c'$ and π is in row r.

Proof. If $k = 0$, then the claim is true by Lemma 4.2.2. Suppose that $k = 1$. Since V contains at least two entries, we know that $|R| \geqslant 2$ or $|C| \geqslant 2$. If both $|R| \geqslant 2$ and $|C| \geqslant 2$, then Lemma 4.2.2 implies that $\mathcal{S}$ contains T. Thus, we may assume that $|R| = 1$ or $|C| = 1$. We consider only the case where $|R| = 1$, the other case can be resolved by transposing our arguments. First suppose that V contains the alien entry (r, c, σ) of T. So $R = \{r\}$ and $c \in C$. Let $c' \in C \setminus \{c\}$ and let $\epsilon = L'_{r,c'}$. Since T contains only one hole, it follows that ϵ does occur in column c of T, say in row r'. Since $\mathcal{S}$ is a Latin square that hits column c and symbol ϵ but not row r', it follows that π occurs in column c and has symbol ϵ. Furthermore, our choice of c' was forced and hence $C = \{c, c'\}$.

Now suppose that V does not contain (r, c, σ). Suppose that $R = \{r\}$, so that $c \notin C$. Let c_1 and c_2 be distinct elements of C and for $i \in \{1, 2\}$, let $\epsilon_i = L'_{r,c_i}$. Without loss of generality, π does not occur in column c_1. Since $c \neq c_1$, it follows that ϵ_2 occurs in column c_1 of T, say in row r_1. But then $\mathcal{S}$ is a Latin square that hits column c_1, has symbol ϵ_2, but does not hit row r_1, which is a contradiction. This contradiction implies that $R \neq \{r\}$. Hence, $R = \{r'\} \neq \{r\}$. Assuming that $T \not\subseteq \mathcal{S}$, Lemma 4.2.2 implies that $|C| = 2$ and so we can write $C = \{c_1, c_2\}$. For $i \in \{1, 2\}$, let $\epsilon_i = L'_{r',c_i}$. Without loss of generality, $c_2 \neq c$. We know that ϵ_1 occurs in column

c_2 of T, say in row r_2. Since $\mathcal{S}$ hits column c_2 and has symbol ϵ_1 but does not hit row r_2, it follows that π occurs in column c_2 and has symbol ϵ_1. If $c_1 \neq c$ or both $c_1 = c$ and ϵ_2 is not the displaced native from the hole (r, c) in T, then the same argument we just applied to ϵ_1 can be applied to ϵ_2 to show that π occurs in column c_1, which is false. Thus, $c_1 = c$ and ϵ_2 is the displaced native from the hole (r, c) in T.

Finally, we deal with the case $k = 2$. By Lemma 4.2.2, it suffices to consider the case where both $|R| \leqslant 2$ and $|C| \geqslant 4$ or where both $|R| \geqslant 4$ and $|C| \leqslant 2$. We treat the former case, the latter case can be resolved by transposing our arguments. Let c_1, c_2, c_3, and c_4 be distinct columns in C and let $r_1 \in R$. By relabelling if necessary, we may assume that $\{c_1, c_2\} \cap \{c, c'\} = \varnothing$ and π does not occur in column c_1. Let $\epsilon = L'_{r_1,c_2}$. Since ϵ is native to T, it follows that ϵ occurs in column c_1 of T, say in row r_2. Since $\mathcal{S}$ is a Latin square that hits column c_1 and has symbol ϵ and π does not occur in column c_1, it follows that $\mathcal{S}$ must contain row r_2, so $|R| = 2$. But then the fact that $k = 2$ implies that there are at least three symbols in V that are native to T. Each of them must occur in column c_1 of V, contradicting the fact that $|R| \leqslant 2$. □

The following lemma is straightforward.

Lemma 4.2.4. *Let L be a Latin square with a row cycle $\mathcal{D}$ of length 3. Suppose that $\mathcal{S}$ is a subsquare of L that contains more than one entry in $\mathcal{D}$. Then $\mathcal{S}$ contains all entries of $\mathcal{D}$.*

We will need the following two results, which are analogs of Lemma 4.2.4 in the case where L is a near copy of a Latin square. Lemma 4.2.5 deals with the case where the alien entry of L is not a member of $\mathcal{D}$ and Lemma 4.2.6 deals with the case where the alien entry of L is a member of $\mathcal{D}$.

Lemma 4.2.5. *Let L be a near copy of a Latin square with alien entry π. Suppose that L contains the entries,*

$$\mathcal{D} = \{(r_1, c_1, k_1), (r_2, c_1, k_2), (r_1, c_2, k_2), (r_2, c_2, k_3), (r_1, c_3, k_3), (r_2, c_3, k_1)\},$$

for rows r_1 and r_2, columns c_1, c_2, and c_3, and symbols k_1, k_2, and k_3. Suppose that $\pi \notin \mathcal{D}$. Also suppose that $\mathcal{S}$ is a subsquare of L that contains the entry (r_1, c_1, k_1). Then one of the following holds:

- $\mathcal{S} \cap \mathcal{D} = \mathcal{D}$,
- $\mathcal{S} \cap \mathcal{D}$ *contains at most one entry in $\{(r_1, c_2, k_2), (r_1, c_3, k_3)\}$ and none of the entries in $\{(r_2, c_1, k_2), (r_2, c_2, k_3), (r_2, c_3, k_1)\}$.*

Proof. Let R be the set of rows of $\mathcal{S}$. We will first show that if $r_2 \in R$, then $\mathcal{S}$ contains $\mathcal{D}$. Suppose that $r_2 \in R$. Then $\mathcal{S}$ contains the entry (r_2, c_1, k_2). So $\mathcal{S}$ is a Latin square that hits row r_1 and has symbol k_2. It follows that $\mathcal{S}$ must hit column c_2 or π occurs in row r_1 of L and has symbol k_2. Suppose first that $\mathcal{S}$ does not hit column c_2. Since π is in row r_1 and $\mathcal{S}$ is a Latin square that hits row r_2 and has symbol k_1, it follows that $\mathcal{S}$ must hit column c_3. Therefore, $\mathcal{S}$ contains symbol k_3. Since π is in row r_1 and $\mathcal{S}$ contains symbol k_3 and hits row r_2, it follows that $\mathcal{S}$ must also hit column c_2. But we were assuming that $\mathcal{S}$ does not hit column c_2, so this is a contradiction. Now suppose that $\mathcal{S}$ does hit column c_2. Then $\mathcal{S}$ is a Latin square that hits row r_2 and has symbol k_1, so $\mathcal{S}$ hits column c_3 unless π is in row r_2 and has symbol k_1. Similarly,

since $\mathcal{S}$ contains symbol k_3 and hits row r_1 we know that $\mathcal{S}$ must contain column c_3 unless π is in row r_1 and has symbol k_3. Therefore, $\mathcal{S}$ must hit column c_3, hence $\mathcal{S}$ contains $\mathcal{D}$.

We now assume that $r_2 \notin R$. If $(r_1, c_2, k_2) \in \mathcal{S}$, then since $\mathcal{S}$ is a Latin square that contains symbol k_2 and hits column c_1 but does not hit row r_2, we know that π must be in column c_1 and have symbol k_2. Similarly, if $(r_1, c_3, k_3) \in \mathcal{S}$, then π must be in column c_3 and have symbol k_1. The lemma follows because π cannot be in both column c_1 and c_3. □

Lemma 4.2.6. *Let L be a near copy of a Latin square with alien entry $\pi = (r_1, c_1, k_1)$ and displaced native k_4. Suppose that L contains the entries*

$$\mathcal{D} = \{(r_1, c_1, k_1), (r_2, c_1, k_2), (r_1, c_2, k_2), (r_2, c_2, k_3), (r_1, c_3, k_3), (r_2, c_3, k_4)\},$$

for rows r_1 and r_2, columns c_1, c_2, and c_3, and distinct symbols k_1, k_2, k_3, and k_4. Suppose that $\mathcal{S}$ is a subsquare of L that contains π. Then $\mathcal{S} \cap \mathcal{D} \subseteq \{(r_1, c_1, k_1), (r_1, c_3, k_3)\}$.

Proof. Let R be the set of rows of $\mathcal{S}$. We first show that $r_2 \notin R$. Suppose that $r_2 \in R$. Then $\mathcal{S}$ contains the entry (r_2, c_1, k_2). Since $\mathcal{S}$ is a Latin square that contains symbol k_2 and hits row r_1, it follows that $\mathcal{S}$ must also hit column c_2. Hence, $\mathcal{S}$ contains symbol k_3 and therefore $\mathcal{S}$ must also hit column c_3 and contain symbol k_4. However, k_4 does not occur in row r_1 of L, which contradicts the fact that $\mathcal{S}$ is a subsquare. Thus, $r_2 \notin R$.

If $\mathcal{S}$ contains (r_1, c_2, k_2), then since $\mathcal{S}$ is a Latin square that hits column c_1 and contains symbol k_2, it follows that $\mathcal{S}$ must also hit row r_2, which we have just shown is impossible. □

As mentioned in §3.1, we will utilise the corrupted product in our construction of N_∞ Latin squares. So, we will need some corrupting pairs. Throughout the rest of this chapter, we will be using the following four Latin squares frequently and the symbols A^8, B^8, A^9, and B^9 will be reserved for them.

$$A^8 = \begin{bmatrix} 4 & 8 & 6 & 7 & 5 & 1 & 3 & 2 \\ 8 & 6 & 4 & 2 & 7 & 5 & 1 & 3 \\ 1 & 7 & 5 & 3 & 4 & 2 & 6 & 8 \\ 5 & 4 & 3 & 1 & 2 & 6 & 8 & 7 \\ 3 & 2 & 1 & 4 & 6 & 8 & 7 & 5 \\ 2 & 1 & 7 & 5 & 8 & 3 & 4 & 6 \\ 6 & 3 & 2 & 8 & 1 & 7 & 5 & 4 \\ 7 & 5 & 8 & 6 & 3 & 4 & 2 & 1 \end{bmatrix} \quad B^8 = \begin{bmatrix} 4 & 1 & 7 & 2 & 8 & 6 & 5 & 3 \\ 7 & 3 & 5 & 8 & 6 & 1 & 4 & 2 \\ 3 & 5 & 8 & 4 & 1 & 7 & 2 & 6 \\ 2 & 7 & 4 & 6 & 3 & 8 & 1 & 5 \\ 1 & 8 & 6 & 5 & 4 & 2 & 3 & 7 \\ 6 & 4 & 3 & 7 & 2 & 5 & 8 & 1 \\ 5 & 2 & 1 & 3 & 7 & 4 & 6 & 8 \\ 8 & 6 & 2 & 1 & 5 & 3 & 7 & 4 \end{bmatrix} \tag{4.3}$$

$$A^9 = \begin{bmatrix} 2 & 8 & 6 & 3 & 1 & 4 & 5 & 9 & 7 \\ 8 & 6 & 2 & 9 & 5 & 1 & 3 & 7 & 4 \\ 3 & 4 & 7 & 1 & 2 & 5 & 6 & 8 & 9 \\ 1 & 3 & 5 & 2 & 4 & 9 & 7 & 6 & 8 \\ 9 & 1 & 8 & 7 & 3 & 2 & 4 & 5 & 6 \\ 7 & 2 & 1 & 6 & 9 & 3 & 8 & 4 & 5 \\ 4 & 5 & 9 & 8 & 7 & 6 & 1 & 2 & 3 \\ 5 & 7 & 3 & 4 & 6 & 8 & 9 & 1 & 2 \\ 6 & 9 & 4 & 5 & 8 & 7 & 2 & 3 & 1 \end{bmatrix} \quad B^9 = \begin{bmatrix} 2 & 4 & 3 & 7 & 8 & 6 & 9 & 5 & 1 \\ 3 & 7 & 9 & 5 & 4 & 8 & 2 & 1 & 6 \\ 4 & 6 & 1 & 3 & 9 & 2 & 5 & 7 & 8 \\ 6 & 2 & 4 & 9 & 5 & 1 & 8 & 3 & 7 \\ 7 & 5 & 6 & 8 & 1 & 4 & 3 & 9 & 2 \\ 5 & 9 & 2 & 1 & 3 & 7 & 6 & 8 & 4 \\ 1 & 3 & 8 & 2 & 6 & 5 & 7 & 4 & 9 \\ 8 & 1 & 5 & 6 & 7 & 9 & 4 & 2 & 3 \\ 9 & 8 & 7 & 4 & 2 & 3 & 1 & 6 & 5 \end{bmatrix} \tag{4.4}$$

Let $\zeta \in \{8, 9\}$, let $A = A^\zeta$, and let $B = B^\zeta$. The following properties of A and B can be verified computationally.

Property 1: (A, B) is a corrupting pair.

Property 2: For $i \in \{1, 2, 3\}$, let $\mathit{d}_i = A_{1,i}$. The row permutation $\tau_{1,2}$ of A contains the cycle $(\mathit{d}_1, \mathit{d}_2, \mathit{d}_3)$. Furthermore, $\{\mathit{d}_i + 1 : i \in \{1, 2, 3\}\} \cap \{\mathit{d}_i : i \in \{1, 2, 3\}\} = \varnothing$.

Property 3: As highlighted in (4.3) and (4.4), there is a row permutation $\tau_{i,j}$ of A with $3 \leqslant i < j$ and symbol k such that $\tau_{i,j}^3(k) = k + 1 \notin \{\mathit{d}_1, \mathit{d}_2, \mathit{d}_3\}$ and none of k, $\tau_{i,j}(k)$, or $\tau_{i,j}^2(k)$ occur in cell $(i, 1)$.

Property 4: $\{((i, j), (i', j')) \in (\{1, 2\} \times \{1, 2, 3\})^2 : A_{i,j} = B_{i',j'}\} = \{((1, 1), (1, 1))\}$.

Property 5: The only matrix in the set,

$$\left\{\mathit{d}_1 \hookrightarrow A_{2,1}, \mathit{d}_2 \hookrightarrow A_{1,1}, \mathit{d}_2 \hookrightarrow A_{2,2}, \mathit{d}_3 \hookrightarrow A_{1,2}, \mathit{d}_3 \hookrightarrow A_{2,3}, \mathit{d}_1 \hookrightarrow A_{1,3}\right\} \tag{4.5}$$

that contains a subsquare of order at least 2 is the matrix $\mathit{d}_1 \hookrightarrow A_{1,3}$. Furthermore, any proper subsquare of this matrix is an intercalate.

Property 6: Suppose that C is one of the matrices in (4.5), that D is a matrix in

$$\left\{B_{i,j} \hookrightarrow C_{i,j} : \{i, j\} \subseteq [\zeta]\right\}, \tag{4.6}$$

and that $\mathcal{S}$ is a square submatrix of D that includes two alien entries with respect to A. Then $\mathcal{S}$ contains at least two different symbols. Also, if $\mathcal{S}$ is a subsquare, then it is an intercalate.

Property 7: No matrix in the set

$$\left\{\mathit{d}_2 \hookrightarrow A_{1,1}, \mathit{d}_3 \hookrightarrow A_{1,1}, \mathit{d}_1 \hookrightarrow A_{1,2}, \mathit{d}_1 \hookrightarrow A_{1,3}, \mathit{d}_1 \hookrightarrow A_{2,1}\right\} \tag{4.7}$$

contains a subsquare of order more than 2.

The definitions of d_1, d_2, and d_3 from Property 2 will be fixed for the remainder of this section. Also, there is overlap between Property 5 and Property 7, but it is convenient to state them both given the distinct roles that these properties will play in our proof of Theorem 4.2.1.

Let $\mathcal{X}$ denote the set of pairs (L, s) where L is an N_∞ Latin square of some order $\mu \geqslant 10$ with row indices, column indices, and symbol set $[\mu]$ and $s \in [\mu - 1]$ such that the following conditions hold:

Condition (*i*): s is a strong allowable shift with respect to (A^8, L) and (A^9, L).

Condition (*ii*): L contains a row cycle of length 3 that involves rows x_1 and x_2, columns y_1, y_2, and y_3, and symbols z_1, z_2, and z_3 with $1 \notin \{x_1, x_2, y_1, y_2, y_3\}$ and $L_{1,1} + s \notin \{z_1, z_2, z_3\}$. Moreover, the matrix $L_{x_2,y_3} \hookrightarrow L_{x_1,y_3}$ does not contain an intercalate.

Condition (*iii*): There exist rows r_1 and r_2, columns c_1, c_2, and c_3, and a symbol σ of L with $1 \notin \{r_1, r_2, c_1, c_2, c_3\}$ such that L contains the entries

$$\big\{(r_1, c_1, \sigma), (r_2, c_1, \tau(\sigma)), (r_1, c_2, \tau(\sigma)), (r_2, c_2, \tau^2(\sigma)), (r_1, c_3, \tau^2(\sigma)), (r_2, c_3, \sigma + s)\big\} \tag{4.8}$$

where $\tau = \tau_{r_1,r_2}$. Also, the matrix $L_{r_2,c_3} \hookrightarrow L_{r_1,c_3}$ contains no intercalates and neither $L_{1,1}$ nor $L_{1,1} + s$ are elements of $\{\tau(\sigma), \tau^2(\sigma), \sigma + s\}$.

Define $N(\mathcal{X}) = \{\mu \in \mathbb{N} : \text{there is a pair } (L, s) \in \mathcal{X} \text{ where } L \text{ is of order } \mu\}$. We aim to show that $N(\mathcal{X})$ contains all integers of the form $2^a 3^b \geqslant 10$ where $a \geqslant 1$ and $b \geqslant 0$ are integers. We will do this using a recursive construction involving the corrupted product and row cycle switching. Let $(M, s) \in \mathcal{X}$ and let $\zeta \in \{8, 9\}$. Condition (iii) together with Property 2 is used to ensure that we will have a row cycle $\mathcal{D}$ of length 3 available to switch to destroy $\mathbb{T}_M$, the unique proper subsquare in the corrupted product $\mathbb{P} = (A^\zeta, B^\zeta) *_s M$. The difference between the symbols in (r_1, c_1, σ) and $(r_2, c_3, \sigma + s)$ from (4.8) accounts for the shift by s that is applied to the M-coordinate of each symbol in the principal M-block of $\mathbb{P}$. Great care is needed to ensure that we do not create new subsquares when we switch on $\mathcal{D}$. Several of the properties of (A^ζ, B^ζ) have been designed with this in mind. Also, Condition (iii) includes subconditions to ensure that we do not create intercalates. Condition (ii) is needed for the recursive step to ensure that the N_∞ Latin square that we construct satisfies Condition (iii).

4.2.1 Base cases

In this subsection, we create suitable base cases for our recursive construction of N_∞ Latin squares. We will show that

$$\{12, 16, 18, 24, 32, 36, 48, 54, 64, 72\} \subseteq N(\mathcal{X}). \tag{4.9}$$

Each base case that we construct will have strong allowable shift $s = 1$. Suppose that some pair $(L, 1)$ satisfies Condition (iii) with some rows r_1 and r_2, columns c_1, c_2, and c_3, and symbol σ. We will simply say that L satisfies Condition (iii) with rows r_1, r_2 and symbol σ, since the columns c_1, c_2, and c_3 are uniquely determined by this information. Similarly, if $(L, 1)$ satisfies Condition (ii) with row cycle $\rho(i, j, c)$, then we will simply say that L satisfies Condition (ii) with row cycle $\rho(i, j, c)$. Furthermore, we will always choose i, j, and c, respectively, to play the roles of x_1, x_2, and y_3 in Condition (ii). We will not explicitly say that each of our base cases satisfies Condition (i), this is something that can easily be checked.

Let L^{12} denote the N_∞ Latin square

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

of order 12 constructed by Gibbons and Mendelsohn [52]. Then L^{12} satisfies Condition (ii) with row cycle $\rho(2, 11, 11)$ and satisfies Condition (iii) with rows 3, 8 and symbol 10. Let L^{18} denote the N_∞ Latin square

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

of order 18 constructed by Elliott and Gibbons [47]. Then L^{18} satisfies Condition (ii) with row cycle $\rho(4, 5, 9)$ and satisfies Condition (iii) with rows 2, 11 and symbol 10.

We next give a construction of Latin squares that will show that $\{16, 32, 64\} \subseteq N(\mathcal{X})$. Let $n \geqslant 4$ be a positive integer satisfying $\gcd(n, 6) = 2$ and let J be a Latin square of order 3. Let $\mathcal{C}$ denote the Latin square of order $n - 3$ defined by $\mathcal{C}_{i,j} = i + j$. For $k \in \{-1, 0, 1\}$, define the

following set of entries of $\mathcal{C}$.

$$\mathcal{E}_k = \{(2j - 3k, j, 3j - 3k) : j \in [n - 3]\}.$$

It is simple to see that the sets $\mathcal{E}_{-1}$, $\mathcal{E}_0$, and $\mathcal{E}_1$ are pairwise disjoint. A Latin square $Y = Y(n, J)$ can then be defined as follows. If (i, j, ℓ) is an entry of $\mathcal{C}$ that is not contained in any set $\mathcal{E}_k$, then $Y_{i,j} = \ell$. If $(i, j, \ell) \in \mathcal{E}_k$, then $Y_{i,j} = n + 2 + k$ and $Y_{i,n+2+k} = Y_{n+2-k,j} = \ell$. Finally, $Y_{n-3+i,n-3+j} = n + J_{i,j}$ for each $\{i, j\} \subseteq \{1, 2, 3\}$. For our purposes, we will take

$$J = \begin{bmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \\ 2 & 1 & 3 \end{bmatrix}.$$

The squares $Y(n, J)$ were first constructed by Kotzig and Turgeon [75]. In [117], it was shown that when $n - 3$ is prime, the only proper subsquare of $Y = Y(n, J)$ is the subsquare $Y[\{n - 2, n - 1, n\}, \{n - 2, n - 1, n\}]$, which is isotopic to J.

Let $n \in \{16, 32, 64\}$ and let L^n be the Latin square obtained from $Y(n, J)$ by switching on $\eta(n, 1, n/2 - 1)$ then switching the resulting square on $\eta(4, n - 1, n - 2)$. Then L^n satisfies Condition (ii) with row cycle $\rho(2, 8, n/2 + 4)$ and satisfies Condition (iii) with rows 2, 3 and symbol $n - 2$.

To show that $\{24, 36, 48, 54\} \subseteq N(\mathcal{X})$, we will use a new construction. Let e be a positive even integer and let E be an N_∞ square of order e. Let (x, y) be a cell in E and let

$$Z = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

Define a Latin square $\mathbb{L} = \mathbb{L}(E, (x, y))$ as follows. First, form the Latin square of order $3e$ with row indices, column indices, and symbols $\{1, 2, 3\} \times [e]$ where cell $((i, j), (k, \ell))$ is occupied by symbol

$$\begin{cases} (2, E_{x,y}) & \text{if } (i, k) \in \{(1, 1), (2, 3), (3, 2)\} \text{ and } (j, \ell) = (x, y), \\ (1, E_{x,y}) & \text{if } (i, k) \in \{(1, 2), (2, 1), (3, 3)\} \text{ and } (j, \ell) = (x, y), \\ (Z_{i,k}, E_{j,\ell} + e/2) & \text{if } (i, k) = (2, 2), \\ (Z_{i,k}, E_{j,\ell}) & \text{otherwise.} \end{cases}$$

Then rename the rows indices, column indices, and symbols of this square using $\prec_1$ to obtain $\mathbb{L}$. Intuitively, we are obtaining $\mathbb{L}$ from the direct product $Z \times E$ as follows. Add $e/2$ to the E-coordinate of each symbol in the E-block of $Z \times E$ in position $(2, 2)$. Then, switch the resulting square on a symbol cycle of length 3 involving symbols $(1, E_{x,y})$ and $(2, E_{x,y})$.

Henceforth, we fix E to be the Latin square in (4.2), which is N_∞. Let L^{24} denote the Latin square obtained from $\mathbb{L}(E, (1, 2))$ by switching on $\eta(6, 14, 18)$. Then L^{24} satisfies Condition (ii) with row cycle $\rho(2, 7, 16)$ and satisfies Condition (iii) with rows 2, 5 and symbol 3. Let L^{36} denote the Latin square obtained from $\mathbb{L}(L^{12}, (2, 3))$ by switching on $\eta(1, 21, 30)$. Then L^{36} satisfies Condition (ii) with row cycle $\rho(2, 11, 35)$ and satisfies Condition (iii) with rows 2, 3 and symbol 15. Let L^{48} denote the Latin square obtained from $\mathbb{L}(L^{16}, (16, 8))$ by switching on

$\eta(1,17,41)$. Then L^{48} satisfies Condition (ii) with row cycle $\rho(2,8,12)$ and satisfies Condition (iii) with rows 2, 3 and symbol 14. Let L^{54} denote the Latin square obtained from $\mathbb{L}(L^{18},(7,7))$ by switching on $\eta(1,19,52)$. Then L^{54} satisfies Condition (ii) with row cycle $\rho(2,10,29)$ and satisfies Condition (iii) with rows 2, 8 and symbol 34.

Finally, we show that $72 \in N(\mathcal{X})$. Let L^{72} be obtained from the corrupted product $(A^9,B^9)*_5 E$ by renaming the row indices, column indices, and symbols using $\prec_1$ and then switching on $\rho(2,11,3)$. Then L^{72} satisfies Condition (ii) with row cycle $\rho(2,7,48)$ and satisfies Condition (iii) with rows 2, 5 and symbol 19. We have shown (4.9).

4.2.2 The recursive step

In this subsection, we prove the following theorem by combining Lemma 4.2.12, Lemma 4.2.15, and Lemma 4.2.16 below. This will then allow us to prove Theorem 4.2.1.

Theorem 4.2.7. *If $\mu \in N(\mathcal{X})$, then $\{8\mu, 9\mu\} \subseteq N(\mathcal{X})$.*

The following definitions and notation will be fixed throughout this subsection. Let $\zeta \in \{8,9\}$, let $A = A^\zeta$, and let $B = B^\zeta$. Let $(M,s) \in \mathcal{X}$ and let μ be the order of M. Let $\mathbb{P} = (A,B)*_s M$. Since $(M,s) \in \mathcal{X}$, we know that M satisfies Condition (iii) with some rows r_1 and r_2, columns c_1, c_2, and c_3, and symbol σ. Combining this with Property 2 and the fact that $\mathbb{P}_{(1,r_1),(1,c_1)} = (d_1, \sigma+s)$, we see that the row cycle $\rho((1,r_1),(2,r_2),(3,c_3))$ of $\mathbb{P}$ has length 3. Let $\mathbb{Q}$ be obtained from $\mathbb{P}$ by switching on this row cycle. Then the row cycle $\rho((1,r_1),(2,r_2),(3,c_3))$ of $\mathbb{Q}$, which we will denote by $\mathcal{D}$, has length 3. Define $\mathbb{Q}_1$ to be the Latin square obtained from $\mathbb{Q}$ by using $\prec_1$ to relabel the row indices, column indices, and symbols of $\mathbb{Q}$ to be the set $[\zeta\mu]$. Formally, we relabel by using the map $\phi : [\zeta] \times [\mu] \to [\zeta\mu]$ defined by $\phi(i,j) = \mu(i-1)+j$. In order to prove Theorem 4.2.7, we will show that $(\mathbb{Q}_1,\mu) \in \mathcal{X}$. For each cell (ϵ,δ) of $\mathbb{Q}$, define $\mathbb{Q}'\langle\epsilon,\delta\rangle = (\mathbb{Q}_{\epsilon,\delta}+(1,0)) \hookrightarrow \mathbb{Q}_{\epsilon,\delta}$ and note that $\phi(\epsilon+1,\delta) = \phi(\epsilon,\delta)+\mu$. Hence, to show that μ is a strong allowable shift with respect to $\mathbb{Q}_1$, it suffices to show, for every cell (ϵ,δ) of $\mathbb{Q}$, that $\mathbb{Q}'\langle\epsilon,\delta\rangle$ contains no proper subsquare of order ζ.

Notice that $\mathbb{Q}$ is a 6-near copy of $\mathbb{P}$ and every $\mathbb{Q}'\langle\epsilon,\delta\rangle$ is a near copy of $\mathbb{Q}$. The following lemma exhibits strong restrictions on the intersection between a subsquare and a block in such matrices.

Lemma 4.2.8. *Let $\mathbb{P}'$ be an ℓ-near copy of $\mathbb{P}$ for some non-negative integer $\ell \leqslant 7$. Suppose that $\mathbb{P}'$ is a near copy of a Latin square $\mathbb{P}''$ and let π be the alien entry of $\mathbb{P}'$ with respect to $\mathbb{P}''$. Suppose that $\mathcal{D} \cup \{\pi\}$ contains all the alien entries of $\mathbb{P}'$ with respect to $\mathbb{P}$. Let T be a block of $\mathbb{P}'$ in some position (u,v) and assume that $\pi \notin T$. Let $\mathcal{S}$ be a subsquare of $\mathbb{P}'$ containing π. Suppose that $\mathcal{S}$ contains more than one entry from T. Let $V = \mathcal{S} \cap T$, let R be the set of rows of V, and let C be the set of columns of V. Then,*

- *(i) If T is an M-block that contains no alien entries with respect to $\mathbb{P}$, then T is not the principal M-block and one of the following is true:*
  - *(1) $R = \{(u,1)\}$, $C = \{(v,1),(v,c)\}$ for some $c \in [\mu]$, and π is in column $(v,1)$ and has symbol $\mathbb{P}'_{(u,1),(v,c)}$,*
  - *(2) $R = \{(u,1),(u,r)\}$ for some $r \in [\mu]$, $C = \{(v,1)\}$, and π is in row $(u,1)$ and has symbol $\mathbb{P}'_{(u,r),(v,1)}$,*

(3) $R = \{(u, r)\}$ *for some* $r \in [\mu]\setminus\{1\}$, $C = \{(v, 1), (v, c)\}$ *for some* $c \in [\mu]$, *and* π *occurs in column* (v, c) *and has symbol* $\mathbb{P}'_{(u,r),(v,1)}$. *Furthermore,* $\mathbb{P}'_{(u,r),(v,c)} = (A_{u,v}, M_{1,1})$,

(4) $R = \{(u, 1), (u, r)\}$ *for some* $r \in [\mu]$, $C = \{(v, c)\}$ *for some* $c \in [\mu] \setminus \{1\}$, *and* π *occurs in row* (u, r) *and has symbol* $\mathbb{P}'_{(u,1),(v,c)}$. *Furthermore,* $\mathbb{P}'_{(u,r),(v,c)} = (A_{u,v}, M_{1,1})$.

(*ii*) *If* T *is an* A*-block that contains no alien entries with respect to* $\mathbb{P}$, *then one of the following is true:*

(1) $R = \{(1, u)\}$, $C = \{(1, v), (c, v)\}$ *for some* $c \in [\zeta]$, *and* π *is in column* $(1, v)$ *and has symbol* $\mathbb{P}'_{(1,u),(c,v)}$,

(2) $R = \{(1, u), (r, u)\}$ *for some* $r \in [\zeta]$, $C = \{(1, v)\}$, *and* π *is in row* $(1, u)$ *and has symbol* $\mathbb{P}'_{(r,u),(1,v)}$,

(3) $R = \{(r, u)\}$ *for some* $r \in [\zeta]\setminus\{1\}$, $C = \{(1, v), (c, v)\}$ *for some* $c \in [\zeta]$, *and* π *occurs in column* (c, v) *and has symbol* $\mathbb{P}'_{(r,u),(1,v)}$. *Furthermore,* $\mathbb{P}'_{(r,u),(c,v)} = (A_{1,1}, M_{u,v})$,

(4) $R = \{(1, u), (r, u)\}$ *for some* $r \in [\zeta]$, $C = \{(c, v)\}$ *for some* $c \in [\zeta] \setminus \{1\}$, *and* π *occurs in row* (r, u) *and has symbol* $\mathbb{P}'_{(1,u),(c,v)}$. *Furthermore,* $\mathbb{P}'_{(r,u),(c,v)} = (A_{1,1}, M_{u,v})$.

(*iii*) *If* T *contains an alien entry with respect to* $\mathbb{P}$, *then* $|R| \leqslant 3$ *and* $|C| \leqslant 3$. *Furthermore,* $\min\{|R|, |C|\} < 3$.

Proof. Since T is a block of $\mathbb{P}'$ not containing π, it follows that $\Phi_j(T)$ is a k-near copy of N for some $j \in \{1, 2\}$, $k \in \{0, 1, 2\}$, and $N \in \{A, B, M, \Phi_j(\mathbb{T}_M)\}$. We will first prove that $\mathcal{S}$ cannot contain T. We will prove this claim for the case where T is an M-block. The proof when T is an A-block is similar. Suppose, for a contradiction, that $\mathcal{S}$ contains T. Since $\pi \in \mathcal{S} \setminus T$, we know that $\mathcal{S} \neq T$. Hence, $\mathcal{S}$ contains a whole row of some M-block $U \neq T$ and a whole column of some M-block $U' \notin \{T, U\}$. Lemma 4.2.3 implies that $\mathcal{S}$ contains U unless $\pi \in U$. If $\pi \in U$, then Lemma 4.2.3 implies that $\mathcal{S}$ contains U'. Either way, $\mathcal{S}$ contains two M-blocks of $\mathbb{P}'$, which we will call T and T'.

Let $\mathcal{A}$ be the set of A-blocks of $\mathbb{P}'$ that do not contain an alien entry of $\mathbb{P}'$ with respect to $\mathbb{P}$ or $\mathbb{P}''$. Each A-block in $\mathcal{A}$ hits both T and T'. Suppose that π is in row (x, x') and column (y, y'). Lemma 4.2.3 implies that $\mathcal{S}$ contains every A-block in $\mathcal{A}$ that row (x, x') and column (y, y') do not intersect. Since $\mu \geqslant 10$ and $\mathcal{D} \cup \{\pi\}$ contains all the alien entries of $\mathbb{P}'$ with respect to $\mathbb{P}$ or $\mathbb{P}''$, we know that for each $i \in [\mu] \setminus \{x'\}$, there is some $k \in [\mu]$ such that $\mathcal{S}$ contains the A-block of $\mathbb{P}'$ in position (i, k). It follows that R contains all rows not of the form (r, x') with $r \in [\zeta]$. Hence, the order of $\mathcal{S}$ must be at least $(\mu - 1)/\mu$ times the order of $\mathbb{P}'$. Since $\mu \geqslant 10$, this is a contradiction of Lemma 4.1.3, proving that $\mathcal{S}$ does not contain T.

Suppose that T contains no alien entry with respect to $\mathbb{P}$. Then the only possible hole in $\Phi_j(T)$ with respect to N is the principal entry. By Lemma 4.2.3, we infer that $k = 1$ and that either part (*i*) or part (*ii*) of the present Lemma holds.

Now suppose that T contains an alien entry π' with respect to $\mathbb{P}$. Note that in this case $k = 2$. It suffices to assume that Lemma 4.2.3(*iii*)(3) holds. If T is an M-block, then π' does not occur in the same row or column as the principal entry of T, since $1 \notin \{r_1, r_2, c_1, c_2, c_3\}$. Hence, T must be an A-block and π' must have cell in the set $\{((1, r_1), (2, c_2)), ((1, r_1), (3, c_3)), ((2, r_2), (1, c_1))\}$. Thus, there is some matrix A' in (4.7) such that the shadow of V in A' is a subsquare. Property 7 then implies that $|R| = |C| = 2$, completing the proof. □

An idea that we will use repeatedly is to consider the projection of a hypothetical subsquare onto one of A, B, or M. Our next lemma shows one circumstance where we know that this projection is a Latin square.

Lemma 4.2.9. *Let F be any matrix whose row indices, column indices, and symbol set are $[\zeta] \times [\mu]$ and let $\mathcal{S}$ be a subsquare of F of order t. Suppose, for some $i \in \{1,2\}$, that the projection Φ_i is injective on the rows and columns of $\mathcal{S}$ and that there is some Latin square L such that the shadow of $\Phi_i(\mathcal{S})$ in L agrees with L in all but $\ell < t$ entries. Then $\Phi_i(\mathcal{S})$ is a Latin square.*

Proof. Since the projection of $\mathcal{S}$ onto L is injective, it follows that $\Phi_i(\mathcal{S})$ is a $t \times t$ matrix. As $\mathcal{S}$ is a Latin square, it follows that every symbol in $\Phi_i(\mathcal{S})$ occurs some multiple of t times. Since $\Phi_i(\mathcal{S})$ agrees with its shadow in L in all but $\ell < t$ places, it follows that Φ_i is injective on the set of symbols that occur in $\mathcal{S}$ and hence $\Phi_i(\mathcal{S})$ is a Latin square. □

Our next task is to show that $\mathbb{Q}$ is N_∞, which we do with the following three lemmas.

Lemma 4.2.10. *Any proper subsquare of $\mathbb{Q}$ must contain exactly one entry from $\mathcal{D}$.*

Proof. Suppose that $\mathcal{S}$ is a proper subsquare of $\mathbb{Q}$. Let R be the set of rows of $\mathcal{S}$ and let C be the set of columns of $\mathcal{S}$. First, suppose that $\mathcal{S}$ does not contain an entry from $\mathcal{D}$. Then $\mathbb{P}[R,C]$ is a proper subsquare of $\mathbb{P}$, which can only be $\mathbb{T}_M$ by Theorem 4.1.7. But $\mathbb{P}[R,C] \neq \mathbb{T}_M$ since otherwise $\mathcal{S}$ would contain an entry from $\mathcal{D}$. Now suppose that $\mathcal{S}$ contains at least two entries from $\mathcal{D}$. Then Lemma 4.2.4 implies that $\mathcal{S}$ contains every entry from $\mathcal{D}$. It follows that $\mathbb{P}[R,C]$ is a proper subsquare of $\mathbb{P}$ that contains every entry from $\rho((1,r_1),(2,r_2),(3,c_3))$. However, Theorem 4.1.7 implies that $\mathbb{P}$ has no such subsquare. Thus, $\mathcal{S}$ must contain exactly one entry from $\mathcal{D}$. □

Lemma 4.2.11. *Any proper subsquare of $\mathbb{Q}$ hits every M-block of $\mathbb{Q}$ at most once and hits the principal A-block of $\mathbb{Q}$ at most once.*

Proof. Suppose that $\mathcal{S}$ is a proper subsquare of $\mathbb{Q}$. Let R be the set of rows of $\mathcal{S}$ and let C be the set of columns of $\mathcal{S}$. Lemma 4.2.10 tells us that $\mathcal{S}$ contains exactly one entry from $\mathcal{D}$. Let this entry be in cell $((i',j'),(x,y))$ for some $i' \in \{1,2\}$, $x \in \{1,2,3\}$, and $\{j',y\} \subseteq [\mu] \setminus \{1\}$. So $\mathbb{Q}_{(i',j'),(x,y)} = \mathbb{P}_{(i,j),(x,y)}$ for $i \in \{1,2\} \setminus \{i'\}$ and some $j \in [\mu] \setminus \{1\}$. Let $\mathbb{P}'$ denote the matrix $\mathbb{P}_{(i,j),(x,y)} \hookrightarrow \mathbb{P}_{(i',j'),(x,y)}$ and let $\pi = ((i',j'),(x,y),\mathbb{P}_{(i,j),(x,y)})$ be the alien entry of $\mathbb{P}'$ with respect to $\mathbb{P}$. Then $\mathcal{S}' = \mathbb{P}'[R,C]$ is a proper subsquare of $\mathbb{P}'$.

We will first show that $\mathcal{S}'$ contains at most one entry from every M-block of $\mathbb{P}'$. Denote the M-block of $\mathbb{P}'$ that contains π by T. Let $T' \neq T$ be an M-block of $\mathbb{P}'$, so that T' has no alien entries with respect to $\mathbb{P}$. Let the position of T' be (u,v) and suppose that $\mathcal{S}'$ contains at least two entries from T'. Since $1 \notin \{j',y\}$, we know that Lemma 4.2.8$(i)(1)$ and Lemma 4.2.8$(i)(2)$ do not arise. So we may assume that Lemma 4.2.8$(i)(3)$ occurs (the argument for when Lemma 4.2.8$(i)(4)$ occurs is similar). Explicitly, we are assuming that $(u,v) \neq (1,1)$ and that $\mathcal{S}' \cap T'$ has only row (u,r) and columns $(v,1)$ and (v,c) for some $r \in [\mu] \setminus \{1\}$ and where $(v,c) = (x,y)$. Furthermore, $w_1 = \mathbb{P}'_{(u,r),(v,1)} = \mathbb{P}_{(i,j),(x,y)}$ is the symbol in π and $w_2 = \mathbb{P}'_{(u,r),(v,c)} = (A_{u,v}, M_{1,1})$. Since $\Phi_1(w_1) = A_{u,x}$, it follows that $u = i \in \{1,2\}$. Let $u' \in [\zeta]$ be such that $B_{u',v} = A_{u,v}$. Note that Property 4 implies that $u' > 2$. Since $\mathcal{S}'$ must contain symbol w_2 in column $(v,1)$, it follows that $\mathcal{S}'$ contains the entry $((u',1),(v,1),(B_{u',v},M_{1,1}))$.

Let T'' be the M-block of $\mathbb{P}'$ in position (u', v). Since π occurs in an M-block whose position is in the set $\{1,2\} \times \{1,2,3\}$, it follows that $\pi \notin T''$. Now running the above argument with T'' in place of T' we obtain the contradiction that $u' \in \{1,2\}$.

Next, we show that $|\mathcal{S}' \cap T| = 1$. The position of T is (i', x). Suppose that $|\mathcal{S}' \cap T| \geqslant 2$ and that $\mathcal{S}'$ hits two rows that intersect T. If $\mathcal{S}'$ has a column (c, c') where $c \neq x$, then $\mathcal{S}'$ contains more than one entry from the M-block of $\mathbb{P}'$ in position (i', c), which is false. Hence every column of $\mathcal{S}'$ hits T. Then by similar reasoning, every row of $\mathcal{S}'$ hits T, meaning that $\mathcal{S}'$ is contained within T. We reach the same conclusion if we start with the assumption that $\mathcal{S}'$ hits two columns that intersect T. So $\mathcal{S}' \subseteq T$. All symbols in T other than those in π and the principal entry have A-coordinate $A_{i',x}$. However, the symbol in π has A-coordinate $A_{i,x} \neq A_{i',x}$ and it must occur in every row of $\mathcal{S}'$. The only way that this might happen is if the principal entry of T has the same symbol as π. But that would require that $B_{i',x} = A_{i,x}$, which contradicts Property 4. Hence, $\mathcal{S}'$ must intersect every M-block of $\mathbb{P}'$ at most once.

Finally, we suppose that $\mathcal{S}'$ contains more than one entry from the principal A-block of $\mathbb{P}'$. Lemma 4.2.8 implies that π occurs in row $(r, 1)$ for some $r \in [\zeta]$ or in column $(c, 1)$ for some $c \in [\zeta]$. However, this contradicts the fact that $1 \notin \{j', y\}$. □

Lemma 4.2.12. *The Latin square $\mathbb{Q}$ is N_∞.*

Proof. Suppose that $\mathcal{S}$ is a proper subsquare of $\mathbb{Q}$. Let R be the set of rows of $\mathcal{S}$, let C be the set of columns of $\mathcal{S}$, and let $t = |R|$. Lemma 4.2.11 tells us that $\mathcal{S}$ hits every M-block of $\mathbb{Q}$ at most once and hits the principal A-block of $\mathbb{Q}$ at most once. Lemma 4.2.10 says that $\mathcal{S}$ contains exactly one entry from $\mathcal{D}$. Let this entry be $\pi = ((i', j'), (x, y), \mathbb{P}_{(i,j),(x,y)})$ where $\{i, i'\} = \{1,2\}$, $x \in \{1,2,3\}$, and $\{j, j', y\} \subseteq [\mu] \setminus \{1\}$. Denote the matrix $\mathbb{P}_{(i,j),(x,y)} \hookrightarrow \mathbb{P}_{(i',j'),(x,y)}$ by $\mathbb{P}'$. Then $\mathcal{S}' = \mathbb{P}'[R, C]$ is a proper subsquare of $\mathbb{P}'$ that hits every M-block of $\mathbb{P}'$ at most once. It follows that Φ_1 is injective on R and C. So $\Phi_1(\mathcal{S}')$ is a $t \times t$ matrix that agrees with its shadow in A in all but $v \in \{1,2\}$ entries. Indeed, $v = 1$ unless $\mathcal{S}'$ contains the principal entry of some M-block of $\mathbb{P}'$ other than the principal M-block. Lemma 4.2.9 implies that $\Phi_1(\mathcal{S}')$ is a Latin square unless $t = v = 2$ and $\Phi_1(\mathcal{S}')$ contains only one symbol.

Suppose first that $v = 1$. Then $\Phi_1(\mathcal{S}')$ is a subsquare of one of the matrices in the set (4.5). Property 5 implies that $\mathcal{S}'$ is an intercalate, $i' = 1$, $i = 2$, $x = 3$, $j' = r_1$, $j = r_2$, and $y = c_3$. We can write $R = \{(1, r_1), (r, r')\}$ and $C = \{(3, c_3), (c, c')\}$ for some $\{r, c\} \subseteq [\zeta]$ and $\{r', c'\} \subseteq [\mu]$. Since the symbols in cells $(1,1)$ and $(1,3)$ of the matrix $\mathscr{A}_1 \hookrightarrow A_{1,3}$ agree, we know that $\Phi_1(\mathcal{S}')$ does not contain the entry $(1, 1, \mathscr{A}_1)$. It follows that $c \neq 1$. As $\mathcal{S}'$ is an intercalate, we must have $M_{r_2,c_3} = M_{r',c'}$ and $M_{r_1,c'} = M_{r',c_3}$. Since $r_1 \neq r_2$, it follows that the matrix $M_{r_2,c_3} \hookrightarrow M_{r_1,c_3}$ must contain an intercalate, which contradicts Condition (iii).

Now suppose that $v = 2$. So $\Phi_1(\mathcal{S}')$ is a Latin square or a 2×2 matrix with only one symbol. Also, $\Phi_1(\mathcal{S}')$, which is a submatrix of one of the matrices in the set (4.6), contains two alien entries with respect to A. Property 6 then tells us that $\Phi_1(\mathcal{S}')$ is an intercalate, which implies that $\mathcal{S}'$ is an intercalate. Additionally, from $1 \notin \{y, j'\}$ we know that the two alien entries of $\mathcal{S}'$ with respect to $\mathbb{P}$ occur in different rows and columns. Since $\mathcal{S}'$ is an intercalate, we need the symbols in its two alien entries to match. But that requires $M_{1,1} \in \{\tau(\sigma), \tau^2(\sigma), \sigma + s\}$ where τ is the row permutation τ_{r_1,r_2} of M. But this contradicts Condition (iii). Thus, $\mathcal{S}$ cannot exist. □

We now work on showing that $\mathbb{Q}'\langle\epsilon, \delta\rangle$ has no subsquare of order ζ for every cell (ϵ, δ) of $\mathbb{Q}$. For the rest of this subsection, let (ϵ, δ) be a cell of $\mathbb{Q}$ and let $\mathbb{Q}' = \mathbb{Q}'\langle\epsilon, \delta\rangle = (\mathbb{Q}_{\epsilon,\delta} + (1,0)) \hookrightarrow$

$\mathbb{Q}_{\epsilon,\delta}$. Let π be the alien entry of $\mathbb{Q}'$ with respect to $\mathbb{Q}$ and let $\mathcal{D}'$ denote the set of entries of $\mathbb{Q}'$ that share a cell with some entry in $\mathcal{D}$. By definition, $\mathcal{D}' \subseteq (\mathcal{D} \cup \{\pi\})$. Lemma 4.2.12 implies that any proper subsquare of $\mathbb{Q}'$ must contain π. On several occasions we will use the fact that Φ_2 cannot distinguish between π and the entry of $\mathbb{Q}$ in cell (ϵ, δ).

Lemma 4.2.13. *Let W be a block of $\mathbb{Q}'$ containing π. No subsquare of $\mathbb{Q}'$ of order ζ hits W in at least three rows or in at least three columns.*

Proof. Let $\mathcal{S}$ be a subsquare of $\mathbb{Q}'$ of order ζ that hits W in at least three rows or at least three columns. Our first goal is to show that $\mathcal{S}$ is contained within W. We will give the argument assuming that W is an M-block. Analogous arguments can be used to prove the same claim if W is an A-block. Let the position of W be (u, v).

Suppose that $\mathcal{S}$ hits W in at least three columns and suppose, for a contradiction, that there is a row (r, r') of $\mathcal{S}$ that does not hit W. Let T be the M-block of $\mathbb{Q}'$ in position (r, v). Then $\mathcal{S}$ hits T in three distinct columns. Lemma 4.2.8 implies that T must contain an alien entry with respect to $\mathbb{P}$, hence $(r, v) \in \{1, 2\} \times \{1, 2, 3\}$. It also implies that $\mathcal{S}$ hits T in at most two rows and exactly three columns. Hence, $\mathcal{S}$ can contain at most four rows that do not hit W. Since $\zeta \geqslant 8$, there are at least four rows of $\mathcal{S}$ that hit W. However only three columns of $\mathcal{S}$ hit W and therefore there is a column (c, c') of $\mathcal{S}$ that does not hit W. Then $\mathcal{S}$ hits the M-block of $\mathbb{Q}'$ in position (u, c) in at least four rows, contradicting Lemma 4.2.8. This contradiction implies that all rows of $\mathcal{S}$ must hit W. But then $\mathcal{S}$ must be contained within W, as otherwise $\mathcal{S}$ would hit an M-block of $\mathbb{Q}'$ in at least eight rows, again contradicting Lemma 4.2.8.

Now suppose that $\mathcal{S}$ hits W in at least three rows and is not contained within W. First, we claim that $u \in \{1, 2\}$. If not, then since at most two columns of $\mathcal{S}$ hit W, it follows that $\mathcal{S}$ has a column (c, c') that does not hit W. The M-block of $\mathbb{Q}'$ in position (u, c) has no alien entries with respect to $\mathbb{P}$ and is hit by $\mathcal{S}$ in at least three rows, which contradicts Lemma 4.2.8. So $u \in \{1, 2\}$. If $\mathcal{S}$ has a column (c, c') with $c > 3$ that does not hit W, then $\mathcal{S}$ must hit an M-block of $\mathbb{Q}'$ that has no alien entries with respect to $\mathbb{P}$ in at least three rows, contradicting Lemma 4.2.8. Hence, every column of $\mathcal{S}$ either hits W or is of the form (c, c') with $c \in \{1, 2, 3\}$. Lemma 4.2.8 combined with the fact that at least three rows of $\mathcal{S}$ hit W implies that for each $i \in \{1, 2, 3\}$, $\mathcal{S}$ has at most two columns of the form (i, i'). The only possibility is that $\zeta = 8$, $v > 3$, exactly two columns of $\mathcal{S}$ hit W, and for each $i \in \{1, 2, 3\}$, $\mathcal{S}$ has exactly two columns of the form (i, i'). In this case, Lemma 4.2.8 implies that $\mathcal{S}$ has at most three rows of the form $(1, u')$ and at most three rows of the form $(2, u'')$. It follows that there is a row (r, r') of $\mathcal{S}$ with $r > 2$. Let T be the M-block of $\mathbb{Q}'$ in position $(r, 1)$. We know that $\mathcal{S}$ hits T in two distinct columns and so Lemma 4.2.8 implies that $v = 1$, which is false because $v > 3$. This contradiction implies that $\mathcal{S}$ must be contained within W.

It remains to show that $\mathcal{S}$ cannot be contained within W. Suppose first that W is an M-block. Let $\mathcal{F}$ be the set of entries e in $\mathcal{S}$ that satisfy (i) $e = \pi$, (ii) e is the principal entry of W, and/or (iii) $e \in \mathcal{D}'$. Since $\mathcal{S}$ is a Latin square, it follows that each symbol in $\Phi_1(\mathcal{S})$ occurs some multiple of ζ times. Also, all symbols in $W \setminus \mathcal{F}$ have the same A-coordinate. Since $\zeta > 3$, it follows that every symbol in W must have the same A-coordinate. Now suppose that there is an entry e that satisfies (iii). If e is an entry of $\mathcal{D}$, then its symbol has the wrong A-coordinate to match with symbols in $W \setminus \mathcal{F}$. Thus $e = \pi \in \mathcal{D}'$, but then e still has the wrong A-coordinate to match with symbols in $W \setminus \mathcal{F}$ by Property 2. So no entry in $\mathcal{F}$ satisfies (iii). Hence, the symbol of any entry in $\mathcal{F}$ has the same M-coordinate as the symbol in the corresponding entry

in $\mathbb{P}$. If W is not the principal M-block of $\mathbb{Q}'$, then $\Phi_2(\mathcal{S})$ is a Latin square of order ζ that agrees with its shadow in M. However, M is N_∞ of order $\mu > \zeta$, so this is impossible. We reach a similar contradiction if W is the principal M-block of $\mathbb{Q}'$ because then $\Phi_2(\mathcal{S})$ is a Latin square of order ζ that agrees with its shadow in the matrix M' defined by $M'_{i,j} = M_{i,j} + s$.

We now consider the case where W is an A-block of $\mathbb{Q}'$. Note that $\mathcal{S} = W$ because they have the same order. Define $\mathcal{F}$ as we did above. Using the same arguments as when W was an M-block, we find that every symbol in W has the same M-coordinate. Therefore, the entry of W that satisfies (ii) must also satisfy (iii). Also, Lemma 4.2.9 implies that $\Phi_1(\mathcal{S})$ is a Latin square and from Lemma 4.1.4, it is equal to B if W is the principal A-block of $\mathbb{Q}'$ and it is equal to A otherwise. Hence, the A-coordinate of the symbol in the principal entry of W must be equal to $A_{1,1}$. This necessitates that the entry e satisfying (ii) and (iii) is π. But the symbol of π is not $A_{1,1}$, by Property 2. □

Lemma 4.2.14. *Any subsquare of $\mathbb{Q}'$ of order ζ hits every block of $\mathbb{Q}'$ at most once.*

Proof. We give the argument for M-blocks. The argument for A-blocks is similar. Let W be the M-block containing $\pi = ((x_1, x_2), (y_1, y_2), z) \in ([\zeta] \times [\mu])^3$. We first prove that $\mathcal{S}$ hits no block in at least three rows. Suppose, for a contradiction, that $\mathcal{S}$ hits an M-block T in at least three rows. Lemma 4.2.13 implies that $T \neq W$. Let the position of T be (u, v). Lemma 4.2.8 implies that $(u, v) \in \{1, 2\} \times \{1, 2, 3\}$ and for each $i \in \{1, 2, 3\}$, $\mathcal{S}$ has at most two columns of the form (i, i'). Thus, there is a column (c, c') of $\mathcal{S}$ with $c > 3$. So $\mathcal{S}$ hits the M-block T' in position (u, c) in at least three rows. Lemma 4.2.8 implies that $T' = W$, but this contradicts Lemma 4.2.13. Thus, $\mathcal{S}$ hits every M-block in at most two rows and so there are at least two rows (r_1, r'_1) and (r_2, r'_2) of $\mathcal{S}$ that do not hit W and satisfy $2 < r_1 \leqslant r_2$.

Suppose that $\mathcal{S}$ hits some M-block in two columns, say (c, c') and (c, c''). Without loss of generality, $(y_1, y_2) \neq (c, c')$. Lemma 4.2.8 implies that $r_1 < r_2$ and $\mathbb{Q}_{(r_1,r'_1),(c,c')} = z = \mathbb{Q}_{(r_2,r'_2),(c,c')}$, which violates the fact that $\mathbb{Q}$ is a Latin square. So $\mathcal{S}$ hits every M-block in at most one column. We thus know that $\mathcal{S}$ hits two columns (c_1, c'_1) and (c_2, c'_2) that do not intersect W and satisfy $3 < c_1 < c_2$. Employing a similar argument, we can deduce that no M-block can be hit by two rows of $\mathcal{S}$, which proves the lemma. □

Lemma 4.2.15. *The integer μ is a strong allowable shift with respect to $(A, \mathbb{Q}_1)$.*

Proof. It suffices to show that $\mathbb{Q}'$ has no subsquare of order ζ. Suppose that $\mathcal{S}$ is a subsquare of $\mathbb{Q}'$ of order ζ that contains u elements from $\mathcal{D}'$. By Lemma 4.2.5 and Lemma 4.2.6, we know that $u \in \{0, 1, 2, 6\}$ and that if $u = 6$, then $\pi \notin \mathcal{D}'$. Let R be the set of rows of $\mathcal{S}$ and let C be the set of columns of $\mathcal{S}$. By Lemma 4.2.14, we know that $\mathcal{S}$ hits every block of $\mathbb{Q}'$ at most once and so Φ_1 and Φ_2 are injective on R and C.

First suppose that $u \in \{0, 6\}$. Let $\mathbb{P}' = (\mathbb{P}_{\epsilon,\delta} + (1, 0)) \hookrightarrow \mathbb{P}_{\epsilon,\delta}$ and let $\mathcal{S}' = \mathbb{P}'[R, C]$. Then $\mathcal{S}'$ is a subsquare of $\mathbb{P}'$ that hits every block of $\mathbb{P}'$ at most once. Since the M-coordinate of the symbol of π is equal to $\Phi_2(\mathbb{P}_{\epsilon,\delta})$, it follows that $\Phi_2(\mathcal{S}')$ is a $\zeta \times \zeta$ matrix that agrees with its shadow in M in all but at most one entry. Lemma 4.2.9 implies that $\Phi_2(\mathcal{S}')$ is a Latin square. If $\mathcal{S}'$ contains an entry from the principal M-block of $\mathbb{P}'$, then $\Phi_2(\mathcal{S}')$ is a subsquare of the matrix $(M_{i,j} + s) \hookrightarrow M_{i,j}$ for some $\{i, j\} \subseteq [\mu]$, which contradicts the fact that s is a strong allowable shift with respect to (A, M). If $\mathcal{S}'$ does not hit the principal M-block of $\mathbb{P}'$, then $\Phi_2(\mathcal{S}')$ is a proper subsquare of M, which is a contradiction because M is N_∞.

It remains to consider the case where $u \in \{1, 2\}$. Define $\mathcal{F}$ to be the set of entries e in $\mathcal{S}$ that satisfy (i) $e = \pi$, (ii) e is the principal entry of some M-block of $\mathbb{Q}'$, and/or (iii) $e \in \mathcal{D}'$.

By Lemma 4.2.14 and $u \leqslant 2$, we know that $|\mathcal{F}| \leqslant 4$. Since $\Phi_1(\mathcal{S})$ is a $\zeta \times \zeta$ matrix that agrees with its shadow in A except possibly on the entries coming from $\mathcal{F}$, Lemma 4.2.9 implies that $\Phi_1(\mathcal{S})$ is a Latin square. Furthermore, by Lemma 4.1.4 and the fact that A is N_∞, it follows that $\Phi_1(\mathcal{S}) = A$. Since $u \geqslant 1$, there exists an entry e of $\mathcal{S}$ that satisfies (iii). Note that e cannot satisfy (ii), because $1 \notin \{r_1, r_2\}$. If $e \in \mathcal{D}$, then $\Phi_1(e)$ does not match its shadow in A. So we must have $e = \pi$, but then $\Phi_1(e)$ still does not match its shadow in A by Property 2, a contradiction. □

Lemma 4.2.15 takes care of Condition (i) in our recursive step. Next, we deal with the other two required conditions and thereby complete the proof of Theorem 4.2.7.

Lemma 4.2.16. *The pair $(\mathbb{Q}_1, \mu)$ satisfies Condition (ii) and Condition (iii).*

Proof. Let τ denote the row permutation τ_{r_1,r_2} of M. Also let $\phi : [\zeta] \times [\mu] \to [\zeta\mu]$ be the map defined by $\phi(i,j) = \mu(i-1) + j$. We know that $\mathbb{Q}$ contains the row cycle $\mathcal{D} = \rho((1,r_1),(2,r_2),(3,c_3))$ and $r_1 \neq 1$. Also, the columns involved in $\mathcal{D}$ are $(1,c_1)$, $(2,c_2)$, and $(3,c_3)$ with $c_1 \neq 1$. Since M satisfies Condition (iii),

$$\Phi_2\big(\mathbb{Q}_{(1,1),(1,1)} + (1,0)\big) = M_{1,1} + s \notin \big\{\sigma + s, \tau(\sigma), \tau^2(\sigma)\big\}.$$

So $(\mathbb{Q}_{(1,1),(1,1)} + (1,0)) \notin \{(\mathscr{A}_1, \sigma + s), (\mathscr{A}_2, \tau(\sigma)), (\mathscr{A}_3, \tau^2(\sigma))\}$, which is the set of symbols of $\mathcal{D}$. Next, we show that the matrix $\mathbb{Q}'' = \mathbb{Q}_{(2,r_2),(3,c_3)} \hookrightarrow \mathbb{Q}_{(1,r_1),(3,c_3)}$ does not contain an intercalate. Suppose, for a contradiction, that $\mathbb{Q}''$ does contain an intercalate. Denote this intercalate by I and let the set of rows and columns of I be R and C, respectively. By Lemma 4.2.12, we know that $(1,r_1) \in R$ and $(3,c_3) \in C$. Also, $(2,r_2) \notin R$ and $(2,c_2) \notin C$, since $\mathbb{Q}''_{(1,r_1),(2,c_2)} = \mathbb{Q}''_{(1,r_1),(3,c_3)} = \mathbb{Q}''_{(2,r_2),(3,c_3)}$. If $(1,c_1) \notin C$, then $\mathbb{P}[R,C]$ is an intercalate in $\mathbb{P}$, which contradicts Theorem 4.1.7. Thus, $C = \{(1,c_1),(3,c_3)\}$. Let $(r,r') \in R \setminus \{(1,r_1)\}$. If $r = 1$, then since I is an intercalate we must have $(\mathscr{A}_3, \tau^2(\sigma)) = \mathbb{Q}'_{(1,r_1),(3,c_3)} = \mathbb{Q}'_{(r,r'),(1,c_1)} = (\mathscr{A}_1, M_{r',c_1} + s)$, which is false. Thus, $r > 1$. Also, since $1 \notin \{c_1, c_3\}$, it follows that $\mathbb{Q}_{(x_1,x_2),(y_1,y_2)} = (A_{x_1,y_1}, M_{x_2,y_2})$ whenever $((x_1,x_2),(y_1,y_2)) \neq ((1,r_1),(1,c_1))$ is a cell of I. Thus, $\mathscr{A}_2 = A_{r,3}$ and $\mathscr{A}_3 = A_{r,1}$ and so the matrix $\mathscr{A}_2 \hookrightarrow A_{1,1}$ must contain an intercalate. However, this contradicts Property 5. Thus, $\mathbb{Q}''$ does not contain an intercalate. It follows that $(\mathbb{Q}_1, \mu)$ satisfies Condition (ii) with the row cycle $\rho(\phi(1,r_1), \phi(2,r_2), \phi(3,c_3))$

Since $(M,s) \in \mathcal{X}$, we know that M satisfies Condition (ii) with some row cycle involving rows x_1 and x_2, columns y_1, y_2, and y_3, and symbols z_1, z_2, and z_3 where $1 \notin \{x_1, x_2, y_1, y_2, y_3\}$. Without loss of generality, $z_f = M_{x_1,y_f}$ for each $f \in \{1,2,3\}$. Also, A satisfies Property 3, so there is a row permutation $\tau_{i,j}$ of A with $3 \leqslant i < j$ and symbol k such that $\tau^3_{i,j}(k) = k+1$. For $f \in \{1,2,3\}$, let ℓ_f be such that $A_{j,\ell_f} = \tau^f_{i,j}(k)$. It follows that $\mathbb{Q}$ contains the entries

$$\begin{array}{lll} \big((i,x_1),(\ell_1,y_1),(k,z_1)\big), & \big((i,x_1),(\ell_2,y_2),(\tau_{i,j}(k),z_2)\big), & \big((i,x_1),(\ell_3,y_3),(\tau^2_{i,j}(k),z_3)\big), \\ \big((j,x_2),(\ell_1,y_1),(\tau_{i,j}(k),z_2)\big), & \big((j,x_2),(\ell_2,y_2),(\tau^2_{i,j}(k),z_3)\big), & \big((j,x_2),(\ell_3,y_3),(k+1,z_1)\big). \end{array} \tag{4.10}$$

Next, we show that the matrix $\mathbb{Q}'' = \mathbb{Q}_{(j,x_2),(\ell_3,y_3)} \hookrightarrow \mathbb{Q}_{(i,x_1),(\ell_3,y_3)}$ contains no intercalates. Suppose, for a contradiction, that $\mathbb{Q}''$ does contain an intercalate, say I. Lemma 4.2.12 implies that I must contain the entry of $\mathbb{Q}''$ in cell $((i,x_1),(\ell_3,y_3))$. Let the row and columns of I be $\{(i,x_1),(r,r')\}$ and $\{(\ell_3,y_3),(c,c')\}$, respectively, for some $\{r,c\} \subseteq [\zeta]$ and $\{r',c'\} \subseteq [\mu]$. Property 3 tells us that $k+1 \notin \{\mathscr{A}_1, \mathscr{A}_2, \mathscr{A}_3\}$, which implies that $(r,c) \neq (1,1)$ and I contains no

entry from $\mathcal{D}$. It follows that $M_{x_2,y_3} = M_{r',c'}$ and $M_{x_1,c'} = M_{r',y_3}$. Since $x_1 \neq x_2$, this implies that $M_{x_2,y_3} \hookrightarrow M_{x_1,y_3}$ contains an intercalate, contradicting Condition (ii). By Condition (ii), we know that $M_{1,1} + s \notin \{z_1, z_2, z_3\}$. Thus, neither $\mathbb{Q}_{(1,1),(1,1)}$ nor $\mathbb{Q}_{(1,1),(1,1)} + (1,0)$ are elements of $\{(\tau_{i,j}(k), z_2), (\tau_{i,j}^2(k), z_3), (k+1, z_1)\}$. Therefore, $(\mathbb{Q}_1, \mu)$ satisfies Condition (iii) with rows $\phi(i, x_1)$ and $\phi(j, x_2)$, columns $\phi(\ell_1, y_1)$, $\phi(\ell_2, y_2)$, and $\phi(\ell_3, y_3)$, and symbol $\phi(k, z_1)$, as illustrated in (4.10). Note that $1 \notin \{x_1, x_2, y_1, y_2, y_3\}$ ensures that

$$1 \notin \{\phi(i, x_1),\ \phi(j, x_2),\ \phi(\ell_1, y_1),\ \phi(\ell_2, y_2),\ \phi(\ell_3, y_3)\}. \qquad \square$$

We are now ready to prove our main result for this section.

Proof of Theorem 4.2.1. By Theorem 2.2.14, it suffices to show that there exists an N_∞ Latin square of order n for all $n \geqslant 12$ of the form $2^a 3^b$ where $a \geqslant 1$ and $b \geqslant 0$ are integers. Let n be such an integer. Write $n = 2^{3i+j} 3^{2k+\ell}$ for some $\{i, j, k, \ell\} \subseteq \mathbb{N}$ with $j \in \{0, 1, 2\}$ and $\ell \in \{0, 1\}$. Consider the following table.

	$\ell = 0$		$\ell = 1$	
$j = 0$	$i \geqslant 2$	$n = 8^{i-2}9^k 64$	$n = 8^{i-1}9^k 24$	
	$i = 1$ and $k \geqslant 1$	$n = 9^{k-1}72$		
$j = 1$	$i \geqslant 1$	$n = 8^{i-1}9^k 16$	$i \geqslant 1$	$n = 8^{i-1}9^k 48$
	$i = 0$ and $k \geqslant 1$	$n = 9^{k-1}18$	$i = 0$ and $k \geqslant 1$	$n = 9^{k-1}54$
$j = 2$	$i \geqslant 1$	$n = 8^{i-1}9^k 32$	$n = 8^i 9^k 12$	
	$i = 0$ and $k \geqslant 1$	$n = 9^{k-1}36$		

This table together with the base cases in (4.9) tells us that we can always write n in the form $8^{i'}9^{k'}n'$ for some non-negative integers i' and k' and some $n' \in N(\mathcal{X})$. We can then repeatedly apply Theorem 4.2.7 to show that $n \in N(\mathcal{X})$. $\square$

4.3 Latin hypercubes without proper subhypercubes

In this section, we prove Theorem 4.0.3. First, we give a method of boosting the dimension of a Latin hypercube. Let $H : [n]^d \to [n]$ be a d-dimensional Latin hypercube of order n. Let $d' \geqslant d$ be an integer. We can define an array $\mathcal{H}_{d'}(H) : [n]^{d'} \to [n]$ by,

$$\mathcal{H}_{d'}(H)(x_1, x_2, \ldots, x_{d'}) = H(x_1, x_2, \ldots, x_d) + \sum_{i=d+1}^{d'} x_i.$$

The following lemma is easy to verify.

Lemma 4.3.1. *Let $H : [n]^d \to [n]$ be a d-dimensional Latin hypercube of order n and let $d' \geqslant d$ be an integer. Then $\mathcal{H}_{d'}(H)$ is a Latin hypercube.*

The following lemma proves that our method of boosting the dimension of a Latin hypercube preserves the N_∞ property.

Lemma 4.3.2. *Let $H : [n]^d \to [n]$ be a d-dimensional N_∞ Latin hypercube of order n and let $d' \geqslant d$ be an integer. The Latin hypercube $\mathcal{H}_{d'}(H)$ is N_∞.*

Proof. Suppose, for a contradiction, that $\mathcal{H}_{d'}(H)$ has a proper subhypercube $\mathcal{S} = H|_{S_1 \times S_2 \times \cdots \times S_{d'}}$ where $S_i \subseteq [n]$ for each $i \in [d']$. Let the symbol set of $\mathcal{S}$ be $\Xi \subseteq [n]$ and let k be the cardinality of Ξ. Fix $s_i \in S_i$ for each $i \in [d'] \setminus [d]$ and define $s = \sum_{i=d+1}^{d'} s_i$. Let $\Xi + s$ denote the set $\{j + s : j \in \Xi\} \subseteq [n]$ and define $H' : S_1 \times S_2 \times \cdots \times S_d \to (\Xi + s)$ by $H'(x_1, x_2, \ldots, x_d) = \mathcal{S}(x_1, x_2, \ldots, x_d, s_{d+1}, \ldots, s_{d'}) = H(x_1, x_2, \ldots, x_d) + s$. It is easy to see that H' is a subhypercube of the Latin hypercube $H'' : [n]^d \to [n]$ defined by $H''(x_1, x_2, \ldots, x_d) = H(x_1, x_2, \ldots, x_d) + s$. This implies that H also has a proper subhypercube, which is a contradiction. □

Let $H : [n]^3 \to [n]$ be a Latin cube of order n. For each $x \in [n]$, the restriction $H|_{[n]\times[n]\times\{x\}}$ induces a Latin square L^x defined by $L^x_{i,j} = H(i, j, x)$. We can specify H by listing the Latin squares L^x in order for each $x \in [n]$. McKay and Wanless [91] enumerated Latin hypercubes of small orders and dimensions and some of their data can be found at [87]. The Latin cube specified by (4.11) below is an N_∞ Latin cube of order 4. There are five species of Latin cubes of order 4 and only one of them contains an N_∞ Latin cube. The Latin cube specified by (4.12) below is also N_∞ and has order 6. There are 264248 species of Latin cubes of order 6 and 17946 of them contain an N_∞ Latin cube.

$$\left[\begin{array}{cccc|cccc|cccc|cccc}
1 & 2 & 3 & 4 & 2 & 1 & 4 & 3 & 3 & 4 & 2 & 1 & 4 & 3 & 1 & 2 \\
2 & 3 & 4 & 1 & 1 & 4 & 3 & 2 & 4 & 2 & 1 & 3 & 3 & 1 & 2 & 4 \\
3 & 4 & 1 & 2 & 4 & 3 & 2 & 1 & 2 & 1 & 3 & 4 & 1 & 2 & 4 & 3 \\
4 & 1 & 2 & 3 & 3 & 2 & 1 & 4 & 1 & 3 & 4 & 2 & 2 & 4 & 3 & 1
\end{array}\right] \tag{4.11}$$

$$\left[\begin{array}{cccccc|cccccc|cccccc}
1 & 2 & 3 & 4 & 5 & 6 & 2 & 1 & 4 & 3 & 6 & 5 & 3 & 4 & 5 & 6 & 1 & 2 \\
2 & 1 & 4 & 3 & 6 & 5 & 1 & 3 & 2 & 6 & 5 & 4 & 4 & 2 & 6 & 5 & 3 & 1 \\
3 & 4 & 6 & 5 & 1 & 2 & 6 & 2 & 5 & 4 & 3 & 1 & 5 & 6 & 3 & 1 & 2 & 4 \\
4 & 3 & 5 & 6 & 2 & 1 & 3 & 4 & 6 & 5 & 1 & 2 & 6 & 5 & 1 & 2 & 4 & 3 \\
5 & 6 & 1 & 2 & 4 & 3 & 4 & 5 & 3 & 1 & 2 & 6 & 1 & 3 & 2 & 4 & 6 & 5 \\
6 & 5 & 2 & 1 & 3 & 4 & 5 & 6 & 1 & 2 & 4 & 3 & 2 & 1 & 4 & 3 & 5 & 6
\end{array}\right.$$
$$\left.\begin{array}{cccccc|cccccc|cccccc}
4 & 3 & 6 & 5 & 2 & 1 & 5 & 6 & 1 & 2 & 3 & 4 & 6 & 5 & 2 & 1 & 4 & 3 \\
3 & 5 & 1 & 2 & 4 & 6 & 6 & 4 & 5 & 1 & 2 & 3 & 5 & 6 & 3 & 4 & 1 & 2 \\
2 & 1 & 4 & 6 & 5 & 3 & 1 & 5 & 2 & 3 & 4 & 6 & 4 & 3 & 1 & 2 & 6 & 5 \\
5 & 6 & 2 & 1 & 3 & 4 & 2 & 1 & 3 & 4 & 6 & 5 & 1 & 2 & 4 & 3 & 5 & 6 \\
6 & 4 & 5 & 3 & 1 & 2 & 3 & 2 & 4 & 6 & 5 & 1 & 2 & 1 & 6 & 5 & 3 & 4 \\
1 & 2 & 3 & 4 & 6 & 5 & 4 & 3 & 6 & 5 & 1 & 2 & 3 & 4 & 5 & 6 & 2 & 1
\end{array}\right] \tag{4.12}$$

Theorem 4.0.3 now follows by combining Theorem 4.2.1, (4.11), and (4.12) with Lemma 4.3.2.

Chapter 5

Perfect 1-factorisations of $K_{11,11}$

The main purpose of this chapter is to report the results of a computer enumeration of the perfect 1-factorisations of $K_{11,11}$.

Theorem 5.0.1. *There are* 687 121 *perfect* 1*-factorisations of* $K_{11,11}$ *up to isomorphism. Of these,* 2657 *have a non-trivial automorphism group.*

Recall from §2.3.1 that there is an equivalence between ordered 1-factorisations of complete bipartite graphs and Latin squares. Thus, the catalogue behind Theorem 5.0.1 allows us to enumerate several interesting classes of Latin squares of order 11.

Theorem 5.0.2.

- *There are* 687 115 *species containing row-Hamiltonian Latin squares of order* 11*. Of these,* 2660 *have a non-trivial autoparatopism group,* 687 096 *have* $\nu = 2$*,* 12 *have* $\nu = 4$*, and* 7 *have* $\nu = 6$*.*
- *There are* 1 374 132 *isotopism classes containing row-Hamiltonian Latin squares of order* 11*. Of these,* 5104 *have a non-trivial autotopism group.*

Recall from §2.3.2 the three known infinite families of perfect 1-factorisations of complete graphs. Let p be an odd prime and let V be the vertex set of K_{p+1}. When $\mathcal{F} \in \{GK_{p+1}, GB_{p+1}\}$, the value $\nu(\mathscr{L}(\mathcal{F}, v))$ is known for any $v \in V$ and the number of species that contain a Latin square $\mathscr{L}(\mathcal{F}, v)$ with $v \in V$ is known. However, these facts are not known when $\mathcal{F} = GA_{2p}$. We tie up this loose end by proving the following theorem.

Theorem 5.0.3. *Let* p *be an odd prime, let* V *be the vertex set of* K_{2p}*, and let* $\{u, v\} \subseteq V$*. The squares* $\mathscr{L}(GA_{2p}, v)$ *and* $\mathscr{L}(GA_{2p}, u)$ *are paratopic and*

$$\nu(\mathscr{L}(GA_{2p}, v)) = \begin{cases} 6 & \text{if } p = 3, \\ 2 & \text{otherwise.} \end{cases}$$

The structure of this chapter is as follows. In §5.1, we discuss our enumeration algorithm for proving Theorem 5.0.1. In §5.2, we discuss Theorem 5.0.2 and the catalogue of row-Hamiltonian Latin squares of order 11. In §5.3, we discuss how useful various invariants are for distinguishing our enumerated objects. Finally, in §5.4, we prove Theorem 5.0.3.

To reduce the risk of programming errors, all computations described in this chapter were performed independently by the author and Ian Wanless, then crosschecked. The combined computation time was under two CPU years.

5.1 The algorithm

In this section, we describe an algorithm to generate the perfect 1-factorisations of any complete bipartite graph, which we used to generated the perfect 1-factorisations of $K_{11,11}$. The algorithm is similar to the algorithm used in [54] to generate the perfect 1-factorisations of K_{16}.

Definition 5.1.1. An *ordered partial* 1*-factorisation of* $K_{n,n}$ is an ordered 1-factorisation of a subgraph of $K_{n,n}$.

Let $\mathcal{P} = [f_1, f_2, \ldots, f_a]$ be an ordered partial 1-factorisation of $K_{n,n}$. We use $\mathcal{P} \| f_{a+1}$ to denote $[f_1, f_2, \ldots, f_a, f_{a+1}]$, the ordered partial 1-factorisation obtained by appending f_{a+1} to $\mathcal{P}$. We use $|\mathcal{P}|$ to denote the number of 1-factors in $\mathcal{P}$.

The following definitions and notation will be fixed throughout this section. Let n be a positive integer, let $U = \{u_1, u_2, \ldots, u_n\}$, and let $W = \{w_1, w_2, \ldots, w_n\}$. Let the vertex set of $K_{n,n}$ be $U \cup W$ with bipartition (U, W). Designate U to be the first part of $K_{n,n}$. Endow U with the total order defined by $u_i \leqslant u_j$ if $i \leqslant j$. Endow W with the analogous total order.

We now define a partial order $\prec_2$ on the set of ordered partial 1-factorisations of $K_{n,n}$. For brevity, we will write the edge $\{u_i, w_j\}$ of $K_{n,n}$ as $u_i w_j$. We will adopt a similar convention for edges of other graphs throughout this chapter. Let $\mathcal{P} = [f_1, f_2, \ldots, f_a]$ and $\mathcal{P}' = [f'_1, f'_2, \ldots, f'_b]$ be two distinct ordered partial 1-factorisations of $K_{n,n}$. If $f_i = f'_i$ for all $i \in [\min\{a, b\}]$, then $\mathcal{P}$ and $\mathcal{P}'$ are incomparable. Otherwise, let j be minimal such that $f_j \neq f'_j$. If $j > 3$, then we deem $\mathcal{P}$ and $\mathcal{P}'$ incomparable. So suppose that $j \leqslant 3$. The edges in f_j can be written as $u_1x_1, u_2x_2, \ldots, u_nx_n$ where $\{x_1, \ldots, x_n\} = \{w_1, \ldots, w_n\}$. Similarly the edges in f'_j can be written as $u_1y_1, u_2y_2, \ldots, u_ny_n$ where $\{y_1, \ldots, y_n\} = \{w_1, \ldots, w_n\}$. Let ℓ be minimal such that $x_\ell \neq y_\ell$. We say that $\mathcal{P} \prec_2 \mathcal{P}'$ if $x_\ell < y_\ell$. If $x_\ell > y_\ell$, we say that $\mathcal{P}' \prec_2 \mathcal{P}$. Let $\preccurlyeq_2$ denote the reflexive closure of $\prec_2$.

Let $\mathcal{P} = [f_1, f_2, \ldots, f_a]$ be an ordered partial 1-factorisation of $K_{n,n}$ with $a \geqslant 3$. For $i \in [a]$, denote by $\mathcal{P}^i$ the ordered partial 1-factorisation $[f_1, f_2, \ldots, f_i]$.

Definition 5.1.2. Let $\mathcal{P} = [f_1, f_2, \ldots, f_a]$ be an ordered partial 1-factorisation of $K_{n,n}$ with $a \geqslant 3$. Say that $\mathcal{P}$ is *minimal* if $\mathcal{P}^3 \preccurlyeq_2 (\mathcal{P}')^3$ for every ordered partial 1-factorisation $\mathcal{P}'$ of $K_{n,n}$ that is isomorphic to $\mathcal{P}$.

Note that if $\mathcal{P} = [f_1, f_2, \ldots, f_a]$ is a minimal ordered partial perfect 1-factorisation of $K_{n,n}$, then

$$f_1 = \{u_1w_1, u_2w_2, \ldots, u_{n-1}w_{n-1}, u_nw_n\} \text{ and}$$
$$f_2 = \{u_1w_2, u_2w_3, \ldots, u_{n-1}w_n, u_nw_1\}.$$

The software nauty [89] is a practical algorithm for testing whether there is a colour preserving graph isomorphism between two vertex coloured graphs. Isomorphism testing for 1-factorisations of bipartite graphs can be converted into an isomorphism problem on vertex coloured graphs as follows. Let Γ be a subgraph of $K_{n,n}$ and let $\mathcal{F} = \{f_1, f_2, \ldots, f_a\}$ be a 1-factorisation of Γ. Construct a coloured graph $C(\mathcal{F})$ containing

- green vertices $f_1, f_2, \ldots, f_a$, each joined to a blue vertex F,
- green vertices $u_1, u_2, \ldots, u_n$, each joined to a red vertex U,
- green vertices $w_1, w_2, \ldots, w_n$, each joined to a red vertex V,

- one black vertex for each edge in Γ, which is joined to one green vertex in each of the previous three categories to indicate the end points of the edge and the 1-factor that contains the edge.

It is routine to check that two 1-factorisations $\mathcal{F}$ and $\mathcal{F}'$ of Γ are isomorphic if and only if there is a colour preserving graph isomorphism from $C(\mathcal{F})$ to $C(\mathcal{F}')$. Also, $\mathrm{Aut}(\mathcal{F})$ is isomorphic to the group of colour preserving automorphisms of $C(\mathcal{F})$, which nauty determines. The same method can be used to determine when two ordered partial 1-factorisations of $K_{n,n}$ are isomorphic. Also, we can vary the procedure in an obvious way to solve the isomorphism problem for non-bipartite graphs.

Our algorithm for generating the perfect 1-factorisations of $K_{n,n}$ is described in Procedure 2 and its subroutine `AddFactor` described in Procedure 1. Steps 2 and 7 of Procedure 2 can be handled in a straightforward manner using nauty as discussed above and represent a negligible fraction of the computation time.

AddFactor: Recursively add 1-factors to an ordered partial perfect 1-factorisation

input: An odd integer $n \geqslant 5$
An ordered partial perfect 1-factorisation $\mathcal{P}$ of $K_{n,n}$
A set $\mathcal{T}$ of 1-factors t for which $\mathcal{P}\|t$ is an ordered partial perfect 1-factorisation

1 **Procedure** `AddFactor`$(n, \mathcal{P}, \mathcal{T})$
2 **if** $|\mathcal{P}| = n$ **then**
3 Output $\mathcal{P}$
4 **else**
5 Let e be an edge of $K_{n,n} \setminus \bigcup \mathcal{P}$ that minimises the number of 1-factors in $\mathcal{T}$ that it is contained in
6 **for** $t \in \mathcal{T}$ *containing* e **do**
7 Let $\mathcal{T}^*$ be the set of 1-factors $t^* \in \mathcal{T}$ such that $K_{n,n}[t, t^*]$ is a Hamiltonian cycle
8 `AddFactor`$(n, \mathcal{P}\|t, \mathcal{T}^*)$
9 **end**
10 **end**
11 **end**

GenP1Fs: Generate the perfect 1-factorisations of $K_{n,n}$

input: An odd integer $n \geqslant 5$

1 **Procedure** `GenP1Fs`(n)
2 Generate a set $\mathscr{S}$ of minimal isomorphism class representatives of ordered partial perfect 1-factorisations of $K_{n,n}$ containing exactly four 1-factors
3 **for** $\mathcal{P} \in \mathscr{S}$ **do**
4 Let $\mathcal{T} = \{$1-factors t of $K_{n,n}$ such that $\mathcal{P}\|t$ is a minimal ordered partial perfect 1-factorisation of $K_{n,n}\}$
5 `AddFactor`$(n, \mathcal{P}, \mathcal{T})$
6 **end**
7 Screen the ordered 1-factorisations of $K_{n,n}$ output by `AddFactor` for isomorphism
8 **end**

We next show that our algorithm performs the desired enumeration.

Lemma 5.1.3. *The set of ordered perfect 1-factorisations of $K_{n,n}$ returned by* `GenP1Fs`(n) *contains a representative from each isomorphism class of ordered perfect 1-factorisations of $K_{n,n}$.*

Proof. Let $\mathcal{M}$ be an isomorphism class of ordered perfect 1-factorisations of $K_{n,n}$ and let $\mathcal{F} \in \mathcal{M}$. By induction on $k \in \{4, 5, \ldots, n\}$, we will prove that `GenP1Fs` makes a call to `AddFactor` with input $\mathcal{P} = \mathcal{E}^k$ where $\mathcal{E} = \mathcal{F}\langle\theta, \psi\rangle$ for some $\theta \in \mathrm{Sym}(U \cup W)$ and $\psi \in \mathrm{Sym}([n])$.

First, consider when $k = 4$. Let $\mathscr{S}$ be as in line 2 of `GenP1Fs`. Since $\mathcal{F}^4$ is an ordered partial perfect 1-factorisation of $K_{n,n}$ of cardinality 4, there is some $\mathcal{E}_1 \in \mathscr{S}$ that is isomorphic to $\mathcal{F}^4$. Let (θ_1, ψ_1) be an isomorphism from $\mathcal{F}^4$ to $\mathcal{E}_1$. Extend ψ_1 to a permutation of $[n]$ by defining

$$\psi_2(x) = \begin{cases} \psi_1(x) & \text{if } x \in \{1, 2, 3, 4\}, \\ x & \text{otherwise.} \end{cases}$$

Let $\mathcal{E} = \mathcal{F}\langle\theta_1, \psi_2\rangle$. Then $\mathcal{E}^4 = \mathcal{E}_1$ and there is a call to `AddFactor` with input $\mathcal{P} = \mathcal{E}^4$.

Now suppose that $k \geqslant 5$ and assume that there is a call `AddFactor`$(n, \mathcal{E}^{k-1}, \mathcal{T})$ where $\mathcal{E} = \mathcal{F}\langle\theta, \psi\rangle$ for some $\theta \in \mathrm{Sym}(U \cup W)$ and $\psi \in \mathrm{Sym}([n])$. Let $[e_1, e_2, \ldots, e_n] = \mathcal{E}$ and let $\mathcal{U} = \{e_k, e_{k+1}, \ldots, e_n\}$. Since $\mathcal{E}$ is ordered isomorphic to $\mathcal{F}$ and $\mathcal{F}$ is perfect, it follows that $\mathcal{E}$ is also perfect and thus $\mathcal{U} \subseteq \mathcal{T}$. Let e be defined as in line 5 of `AddFactor`. Since e must appear in some 1-factor in $\mathcal{E}$, it follows that there is some $t' \in \mathcal{U} \subseteq \mathcal{T}$ containing e. Thus, in the **for** loop of `AddFactor`, there will be a call of `AddFactor` with argument $\mathcal{E}^{k-1} \| t'$. Note that $\mathcal{E}^{k-1} \| t'$ can be written as $\mathcal{E}^k$ where $\mathcal{E} = \mathcal{F}\langle\theta, \psi'\rangle$ for some $\psi' \in \mathrm{Sym}([n])$. Thus, the claim follows by induction.

We have proven that some call of `AddFactor` will output an ordered 1-factorisation of $K_{n,n}$ that is isomorphic to $\mathcal{F}$. The result follows. □

Both the author's and Ian Wanless' implementations of `GenP1Fs` were used to generate the perfect 1-factorisations of $K_{n,n}$ for $n \in \{5, 7, 9, 11\}$. Results of both programs agreed with each other and for $n \in \{5, 7, 9\}$, agreed with previously computed values [116]. For $n = 11$, we found that the set $\mathscr{S}$ in line 2 of `GenP1Fs` had cardinality 13 727 482. Table 5.1 shows the 687 121 perfect 1-factorisations of $K_{11,11}$ up to isomorphism categorised by how much symmetry they have. The second column of the table lists the number of part-preserving automorphisms of each 1-factorisation and the third column lists the total number of automorphisms. The first column gives the number of 1-factorisations that attain the attributes listed in the row in question. The number of part-preserving automorphisms of a 1-factorisation $\mathcal{F}$ can be counted using nauty as described above, except that we change the colour of the vertex V to yellow so that it can no longer be interchanged with U in any colour preserving automorphism of $C(\mathcal{F})$.

5.2 Row-Hamiltonian Latin squares of order 11

From the set of representatives of isomorphism classes of perfect 1-factorisations of $K_{11,11}$ that we generated, it is a simple task to obtain a representative of each species that contains a row-Hamiltonian Latin square of order 11. This can be achieved by using nauty as described in §5.1, except that we change the colour of the vertex F to red. We then use nauty to determine the autoparatopism group of each species representative, which allows us to deduce Theorem 5.0.2.

Count	Part-preserving automorphisms	Automorphisms
684464	1	1
100	1	2
2531	2	2
6	5	5
5	5	10
7	10	10
3	10	20
1	22	22
2	55	55
1	55	110
1	1210	2420

Table 5.1: Symmetries of perfect 1-factorisations of $K_{11,11}$

Table 5.2 shows the 687 115 species of row-Hamiltonian Latin squares of order 11 classified according to their ν values and how much symmetry they have. In that table, the second and third column gives the order of the autotopism group and the autoparatopism group, respectively, the fourth column gives the value of ν, and the first column reports how many species attain the attributes listed in the row in question.

We next discuss the row-Hamiltonian Latin squares of order 11 with high symmetry.

Lemma 5.2.1. *Let n be a positive integer and let L be a Latin square of order n that is isotopic to its transpose. For a 1-line permutation Ψ of $\{1,2,3\}$, let L^Ψ denote the Ψ-conjugate of L and let $\mathcal{F}_\Psi = \mathscr{F}(L^\Psi)$. Then $\mathcal{F}_{(1,2,3)}$, $\mathcal{F}_{(1,3,2)}$, $\mathcal{F}_{(2,1,3)}$, and $\mathcal{F}_{(2,3,1)}$ are all isomorphic. Hence, if L is row-Hamiltonian, then $\nu(L) \in \{4,6\}$ and if the $(3,2,1)$-conjugate of L is row-Hamiltonian, then $\nu(L) \in \{2,6\}$.*

Proof. The proof is similar to that of [116, Lemma 5]. Theorem 2.3.5 implies that $\mathcal{F}_{(1,2,3)}$ is isomorphic to $\mathcal{F}_{(1,3,2)}$ and that $\mathcal{F}_{(2,1,3)}$ is isomorphic to $\mathcal{F}_{(2,3,1)}$, even if L was not isotopic to its transpose. Combining the fact that L is isotopic to its transpose with Theorem 2.3.5 shows that $\mathcal{F}_{(1,2,3)}$ is isomorphic to $\mathcal{F}_{(2,1,3)}$. Hence, $\mathcal{F}_{(1,2,3)}$, $\mathcal{F}_{(1,3,2)}$, $\mathcal{F}_{(2,1,3)}$, and $\mathcal{F}_{(2,3,1)}$ are all isomorphic. Thus, the following four statements are equivalent:

- L is row-Hamiltonian,
- The row-inverse of L is row-Hamiltonian,
- The transpose of L is row-Hamiltonian,
- The $(2,3,1)$-conjugate of L is row-Hamiltonian.

The lemma follows. □

Wanless [116] observed that 11 is the smallest order for which a Latin square with $\nu = 4$ exists. Theorem 5.0.2 tells us that there are 12 species of Latin squares of order 11 with

Count	Autotopisms	Autoparatopisms	ν
684455	1	1	2
99	1	2	2
8	1	2	4
1	1	2	6
2531	2	2	2
5	5	5	2
4	5	10	2
1	5	10	6
1	10	10	2
1	10	10	4
2	10	20	4
2	10	20	6
1	22	22	2
1	10	60	6
1	55	110	4
1	55	110	6
1	1210	7260	6

Table 5.2: Symmetries and ν values of species containing row-Hamiltonian Latin squares of order 11

$\nu = 4$, which we now catalogue. Let $m \geqslant 1$ and $b \geqslant 0$ be integers. Define $\mathbb{Z}_{m,b} = \mathbb{Z}_m \cup \{\infty_1, \infty_2, \ldots, \infty_b\}$ and for $x \in \mathbb{Z}_{m,b}$ define

$$x^+ = \begin{cases} x+1 & \text{if } x \in \mathbb{Z}_m, \\ x & \text{otherwise.} \end{cases}$$

A *bordered diagonally cyclic Latin square* (BDCLS) of order $m+b$ is a Latin square L with row indices, column indices, and symbols $\mathbb{Z}_{m,b}$ such that if $(i,j,k) \in L$, then $(i^+, j^+, k^+) \in L$. If $b = 0$, then L is a *diagonally cyclic Latin square* (DCLS). The map $x \mapsto x^+$ is an automorphism of L, which we call its *diagonally cyclic symmetry*. If $b \in \{0,1\}$, then L is uniquely determined by its first row [119].

There are four species with $\nu = 4$ that contain a BDCLS of order 11. The first row of a BDCLS representative for each such species is given below.

$$(0, 10, 4, 8, 7, 6, 1, 3, 5, 2, 9), \tag{5.1}$$
$$(0, 2, 6, 8, 7, \infty_1, 3, 5, 4, 1, 9), \tag{5.2}$$
$$(0, 3, 7, 9, 8, \infty_1, 4, 6, 5, 2, 1), \text{ and} \tag{5.3}$$
$$(\infty_1, 1, 9, 7, 5, 3, 8, 6, 4, 2, 0). \tag{5.4}$$

The DCLS whose first row is (5.1) comes from the only known infinite family of Latin squares with $\nu = 4$ constructed in [5]. The BDCLS with first row (5.1), (5.2), or (5.3) is symmetric and so, by Lemma 5.2.1, the species that it belongs to gives rise to a single isomorphism class

of perfect 1-factorisations of $K_{11,11}$. In contrast, the species containing the BDCLS with first row (5.4) gives rise to two isomorphism classes of perfect 1-factorisations. The remaining eight species all contain symmetric Latin squares. Figure 5.1 provides a symmetric representative of each of these species. Lemma 5.2.1 implies that they also each give rise to a single isomorphism class of perfect 1-factorisations.

The seven species containing atomic Latin squares of order 11 were catalogued in [86]. From that study, it can be inferred that they give rise to 12 isomorphism classes of perfect 1-factorisations of $K_{11,11}$. Of course, any species with $\nu = 2$ gives rise to a single isomorphism class of perfect 1-factorisations. This accounts for the $687\,121 = 687\,096 + 13 + 12$ perfect 1-factorisations of $K_{11,11}$ up to isomorphism. One representative from each species containing a row-Hamiltonian Latin square of order 11 can be found at [114].

Up to paratopism, there are nine row-Hamiltonian Latin squares of order 11 that have trivial autotopism group but non-trivial autoparatopism group and which give rise to perfect 1-factorisations of $K_{11,11}$ with trivial automorphism group. They are the eight squares given in Figure 5.1 and a symmetric atomic Latin square in the species $\mathcal{A}_{11}^5$ from [86]. There are two isomorphism classes of perfect 1-factorisations which arise from $\mathcal{A}_{11}^5$. One of these has trivial automorphism group and the other has automorphism group of order 2.

We have already given details for the Latin squares reported in Table 5.2 with $\nu \in \{4, 6\}$. The most symmetric species from Table 5.2 with $\nu = 2$ is represented by the DCLS with first row $(0, 2, 8, 5, 7, 1, 10, 4, 6, 3, 9)$. Denote this DCLS by L. Then $\mathrm{Atp}(L)$ is of order 22 and is generated by the diagonally cyclic symmetry and the automorphism $(0, 10)(1, 9)(2, 8)(3, 7)(4, 6) \in \mathrm{Sym}(\mathbb{Z}_{11})$ of L. The next most symmetric species from Table 5.2 with $\nu = 2$ is represented by

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

Its autotopism group is isomorphic to the dihedral group of order 10.

5.3 Invariants

Let $\mathcal{B}$ be the set of row-Hamiltonian Latin squares of order 11 and let $\mathcal{R}(\mathcal{B})$ be the set of species representatives of $\mathcal{B}$ that we generated. Similarly, let $\mathcal{D}$ be the set of perfect 1-factorisations of $K_{11,11}$ and let $\mathcal{R}(\mathcal{D})$ be the set of isomorphism class representatives of $\mathcal{D}$ that we generated. In this section, we discuss some old and new invariants and examine how useful they are for distinguishing elements of $\mathcal{R}(\mathcal{B})$ and elements of $\mathcal{R}(\mathcal{D})$. A *complete species invariant on* $\mathcal{B}$ is a

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

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

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

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

Figure 5.1: A symmetric representative from each of the eight species of Latin squares of order 11 with $\nu = 4$ that do not contain a BDCLS.

function $\mathcal{I}$ on $\mathcal{B}$ such that $\mathcal{I}(L_1) = \mathcal{I}(L_2)$ if and only if Latin squares L_1 and L_2 are paratopic. A *complete isomorphism class invariant on* $\mathcal{D}$ can be defined similarly.

Let L be a Latin square of order n. A *transversal* of L is a selection of n of its entries such that no two entries share a row, column, or symbol. Let $N(L)$ denote the number of transversals of L. Then N is a species invariant.

Let L be a Latin square with row indices R, column indices C, and symbols S. Define $G = G(L)$ to be the digraph with vertex set $R \times C \times S$ such that each vertex (a, b, c) has a unique outgoing arc, which goes to the triple (x, y, z) where $\{(a, b, z), (a, y, c), (x, b, c)\} \subseteq L$. The graph G is called the *train* of L and the isomorphism class of G is a species invariant [120]. Thus, the indegree sequence of G, which is the sorted list of the indegrees of the vertices of G, is also a species invariant. Denote the indegree sequence of G by $I(L)$.

For a Latin square L, let $\mathcal{C}(L)$ be a sorted list of the lengths of its row, column, and symbol cycles. Then $\mathcal{C}$ is a species invariant. Also define $M(L)$ to be a multiset consisting of three sorted lists, one giving the lengths of its row cycles, one giving the lengths of its column cycles, and one giving the lengths of its symbol cycles. Then M is also a species invariant.

We determined how well the above invariants, and combinations of them, distinguish squares in $\mathcal{R}(\mathcal{B})$ and obtained the following results. When applied to every square in $\mathcal{R}(\mathcal{B})$:

- N took 630 distinct values,
- I took 283 518 distinct values,
- $\mathcal{C}$ took 151 412 distinct values,
- M took 675 110 distinct values,
- $(I, \mathcal{C})$ took 687 069 distinct values,
- $(N, I, \mathcal{C})$ took 687 115 distinct values, thus is a complete invariant on $\mathcal{B}$, and
- (I, M) took 687 115 distinct values, thus is a complete invariant on $\mathcal{B}$.

Let n be a positive integer and let $\mathcal{F}$ and $\mathcal{F}'$ be non-isomorphic perfect 1-factorisations of $K_{n,n}$ such that $\mathscr{L}(\mathcal{F})$ is paratopic to $\mathscr{L}(\mathcal{F}')$. Since each of N, I, $\mathcal{C}$, and M are species invariants, they cannot possibly distinguish between $\mathcal{F}$ and $\mathcal{F}'$. So we now define a new invariant, which is useful for distinguishing such perfect 1-factorisations.

Let n be a positive integer and let $\mathcal{F} = \{f_1, f_2, \ldots, f_n\}$ be a perfect 1-factorisation of $K_{n,n}$. Let $\{i, j, k\} \subseteq [n]$ with $i < j$ and $k \notin \{i, j\}$. Since $\mathcal{F}$ is perfect, $K_{n,n}[f_i \cup f_j]$ forms a Hamiltonian cycle in $K_{n,n}$. For each edge $e \in f_k$, define $q_{i,j,k,e}$ to be the distance between the endpoints of e in $K_{n,n}[f_i \cup f_j]$. Define

$$\mathcal{P}(\mathcal{F}) = \sum_{i<j} \sum_{k \notin \{i,j\}} \prod_{e \in f_k} q_{i,j,k,e}.$$

Then $\mathcal{P}$ is invariant on isomorphism classes of perfect 1-factorisations of $K_{n,n}$.

When applied to every element of $\mathcal{R}(\mathcal{D})$, $\mathcal{P}$ took 687 115 distinct values. The six pairs of elements in $\mathcal{R}(\mathcal{D})$ on which $\mathcal{P}$ coincide can be found at [114]. For any invariant $\mathcal{I} \in \{N, \mathcal{C}, I, M\}$, the pair $(\mathcal{P}, \mathcal{I})$ (when applying $\mathcal{P}$ to $\mathcal{F} \in \mathcal{R}(\mathcal{D})$ and $\mathcal{I}$ to $\mathscr{L}(\mathcal{F})$) forms a complete invariant on $\mathcal{D}$.

5.4 The classical families of perfect 1-factorisations

In this section, we tie up a loose end in the literature by proving Theorem 5.0.3.

Let n be an odd integer, let $V = V(K_{n+1})$, let $v \in V$, and let $\mathcal{F}$ be an ordered 1-factorisation of K_{n+1}. In §2.3.2, we associated a Latin square $\mathscr{L}(\mathcal{F}, v)$ to the rooted 1-factorisation $(\mathcal{F}, v)$. Now, we associate a different, but related, Latin square to $(\mathcal{F}, v)$. For distinct x and y in $V \setminus \{v\}$, let $h_{x,y}$ denote the unique 1-factor in $\mathcal{F}$ containing the edge xy. Define a Latin square $\mathscr{L} = \mathscr{L}^*(\mathcal{F}, v)$ with row indices, column indices, and symbols $V \setminus \{v\}$ by

$$\mathscr{L}_{i,j} = \begin{cases} i & \text{if } j = i, \\ k & \text{if } j \neq i \text{ where } k \in V \setminus \{v\} \text{ is such that } kv \in h_{i,j}. \end{cases} \tag{5.5}$$

It is immediate from (5.5) that $\mathscr{L}$ is symmetric. Furthermore, if $\mathcal{F}$ is perfect, then $\mathscr{L}$ is symbol-Hamiltonian, meaning that the $(3, 2, 1)$-conjugate of $\mathscr{L}$ is row-Hamiltonian [22]. In fact, after any necessary relabelling of row indices, column indices, and symbols, the $(1, 3, 2)$-conjugate of $\mathscr{L}$ is isotopic to $\mathscr{L}(\mathcal{F}, v)$. Hence, $\nu(\mathscr{L}(\mathcal{F}, v)) = \nu(\mathscr{L})$ and Lemma 5.2.1 implies that $\nu(\mathscr{L}) \in \{2, 6\}$.

Let p be an odd prime. Our next task is to define the 1-factorisation GA_{2p} of K_{2p}. Let the vertex set of K_{2p} be $\mathbb{Z}_p \times \{1, 2\}$. For $i \in \mathbb{Z}_p$, define

$$f_i = \left\{(i + j, 1)(i - j, 1), (i + j, 2)(i - j, 2) : j \in \mathbb{Z}_p \setminus \{0\}\right\} \cup \{(i, 1)(i, 2)\}.$$

For $i \in \mathbb{Z}_p \setminus \{0\}$, define

$$g_i = \left\{(j, 1)(i + j, 2) : j \in \mathbb{Z}_p\right\}.$$

Then

$$GA_{2p} = \left\{f_i : i \in \mathbb{Z}_p\right\} \cup \left\{g_i : i \in \mathbb{Z}_p \setminus \{0\}\right\}$$

is a perfect 1-factorisation of K_{2p}. See Figure 5.2 for an example of a 1-factor f_i and a 1-factor g_j in GA_{2p}. From Definition 2.3.14, in order to form a rooted 1-factorisation using GA_{2p}, we need to specify a total order on the vertex set of K_{2p} and a total order on the 1-factors in GA_{2p}. We will order the vertices of K_{2p} by their second coordinate and use the first to break ties and we will use the total order

$$f_0 < f_1 < \ldots < f_{p-1} < g_1 < g_2 < \ldots < g_{p-1}$$

on the 1-factors in GA_{2p}. Of course, the results proved in this section do not depend on these total orders.

Anderson [13] showed that if $\{u, v\} \subseteq \mathbb{Z}_p \times \{1, 2\}$, then there is an automorphism of GA_{2p} that maps u to v. Combining this fact with Theorem 2.3.19 proves the first claim of Theorem 5.0.3. Next, we want to determine $\nu(\mathscr{L}(GA_{2p}, v))$ for $v \in V(K_{2p})$. Since this value does not depend on v, we will choose to work with the root vertex $v = (-1, 2)$. Define $\mathscr{L}_p = \mathscr{L}^*(GA_{2p}, v)$. Since $\nu(\mathscr{L}_p) = \nu(\mathscr{L}(GA_{2p}, v))$, we can focus on determining $\nu(\mathscr{L}_p)$. The following is an explicit definition of $\mathscr{L}_p$.

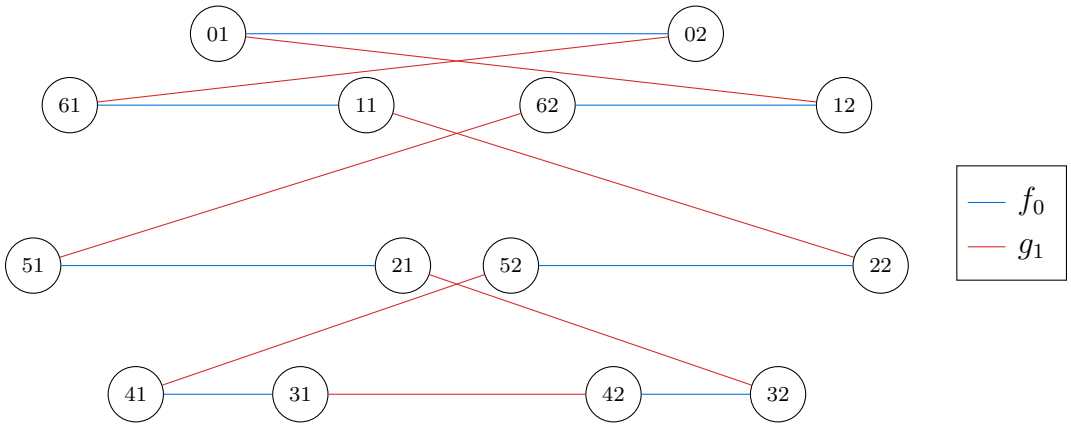

Figure 5.2: The 1-factors f_0 and g_1 of GA_{10}, where the vertex (x, y) of K_{10} is instead labelled xy.

Lemma 5.4.1. *The Latin square $\mathscr{L} = \mathscr{L}_p$ is defined by*

$$\mathscr{L}_{(x,z),(y,w)} = \begin{cases} (x,z) & \text{if } (x,z) = (y,w), \\ (x+y+1,2) & \text{if } z = w \text{ and } x+y+2 \neq 0, \\ (-1,1) & \text{if } z = w \text{ and } x+y+2 = 0, \\ (2x+1,2) & \text{if } z \neq w \text{ and } x = y, \\ (x-y-1,1) & \text{if } z = 1, w = 2, \text{ and } x \neq y, \\ (y-x-1,1) & \text{if } z = 2, w = 1, \text{ and } x \neq y. \end{cases}$$

Proof. Let $((x,z),(y,w)) \in (\mathbb{Z}_p \times \{1,2\})^2$ with $(x,z) \neq (y,w)$. First, suppose that $z = 1 = w$. Let $i = 2^{-1}(x+y) \in \mathbb{Z}_p$ and note that $(x,z)(y,w) \in f_i$. If $x+y+2 = 0$, then $i = -1$ and so $(-1,1)(-1,2) \in f_i$. Hence, $\mathscr{L}_{(x,z),(y,w)} = (-1,1)$. Now suppose that $x+y+2 \neq 0$. Let j be such that $i-j = -1$. Then $j = i+1$ and so $i+j = 2i+1 = x+y+1$. Thus, $(x+y+1,2)(-1,2) \in f_i$ and so $\mathscr{L}_{(x,z),(y,w)} = (x+y+1,2)$. Similar arguments can be used to prove that the claimed value of $\mathscr{L}_{(x,z),(y,w)}$ is correct when $z = 2 = w$.

Now assume that $z = 1$ and $w = 2$. We must distinguish two cases depending on whether or not $x = y$. First, suppose that $x \neq y$. Let $i = y - x$ and note that $(x,z)(y,w) \in g_i$. Setting $i + j = -1$ we obtain $j = -i - 1 = x - y - 1$. So $(x-y-1,1)(-1,2) \in g_i$ and thus $\mathscr{L}_{(x,z),(y,w)} = (x-y-1,1)$. Now suppose that $y = x$. Then $(x,z)(y,w) \in f_x$. Setting $x-j = -1$ yields $j = x+1$. Thus $(2x+1,2)(-1,2) \in f_x$ and so $\mathscr{L}_{(x,z),(y,w)} = (2x+1,2)$. Similar arguments can be used to prove that the claimed value of $\mathscr{L}_{(x,z),(y,w)}$ is correct when $z = 2$ and $w = 1$. □

To prove the second claim of Theorem 5.0.3, we will prove that $\mathscr{L}_p$ is not atomic by proving that it contains a row cycle of length 5. Figure 5.3 shows a row cycle of length 5 in the Latin square $\mathscr{L}_5$.

Proof of Theorem 5.0.3. The first claim of the theorem follows from the discussion before Lemma 5.4.1, so it remains to prove the second claim. Since $\nu(\mathscr{L}(GA_{2p}, v)) = \nu(\mathscr{L}_p)$, it suffices to prove that $\nu(\mathscr{L}_p) = 6$ if $p = 3$ and $\nu(\mathscr{L}_p) = 2$ otherwise.

Table 2.3 and Table 2.5 together tell us that any Latin square of order 5 that has $\nu \neq 0$ is atomic, so $\nu(\mathscr{L}_3) = 6$. Now assume that $p \geqslant 5$. Using Lemma 5.4.1, it is easy to verify that

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

Figure 5.3: The Latin square $\mathscr{L}_5$ and a highlighted row cycle of length 5.

the following ten triples are entries of $\mathscr{L}_p$:

$$\begin{aligned}
&((0,1),(0,1),(0,1)), && ((0,2),(0,1),(1,2)),\\
&((0,1),(0,2),(1,2)), && ((0,2),(0,2),(0,2)),\\
&((0,1),(-1,1),(0,2)), && ((0,2),(-1,1),(-2,1)),\\
&((0,1),(1,2),(-2,1)), && ((0,2),(1,2),(2,2)),\\
&((0,1),(1,1),(2,2)), && ((0,2),(1,1),(0,1)).
\end{aligned}$$

These entries form a row cycle of length 5 in $\mathscr{L}_p$ and so $\mathscr{L}_p$ is not atomic. Since $\nu(\mathscr{L}_p) \in \{2,6\}$ by Lemma 5.2.1, the theorem follows. □

Chapter 6

Quadratic Latin squares

In this chapter, we study a variety of problems regarding subrectangles of quadratic Latin squares. Throughout this chapter, p will be an odd prime, d will be a positive integer, and $q = p^d$ will be an odd prime power. Unless otherwise stated, all asymptotics will be as $q \to \infty$. We will use standard terminology of permutation groups, which can be found, for example, in [40].

Our first main result counts the number of intercalates in quadratic Latin squares.

Theorem 6.0.1. *Let $\mathcal{L} = \mathcal{L}[a, b]$ be a quadratic Latin square of order q and let N denote the number of intercalates that $\mathcal{L}$ contains.*

- *If $b \notin \{-a, 2-a, a/(2a-1)\}$ and*

$$(2ab - a - b)(a + b)(a - 1) \in \mathcal{R}_q \text{ and } \{2(a + b - 2)(a - 1), 2a(a + b)\} \subseteq \mathcal{N}_q, \tag{6.1}$$

  then $N = q(q-1)$.

- *If $b \notin \{-a, 2-a, a/(2a-1)\}$ and (6.1) is not satisfied, then $N = 0$.*

- *If $b \in \{-a, 2-a, a/(2a-1)\}$, then $q \equiv 1 \bmod 4$ and $N \neq 0$. Furthermore,*

$$\frac{q(q-1)(q - 11q^{1/2} - 38)}{32} \leqslant N \leqslant \frac{q(q-1)(q + 11q^{1/2} + 70)}{32}.$$

Theorem 6.0.1 yields the following two corollaries, the first of which gives a characterisation of when a quadratic Latin square is N_2 and second of which counts the number of N_2 quadratic Latin squares.

Corollary 6.0.2. *The Latin square $\mathcal{L}[a, b]$ of order q contains an intercalate if and only if (6.1) is satisfied or $b \in \{-a, 2-a, a/(2a-1)\}$. In the latter case, $q \equiv 1 \bmod 4$.*

Corollary 6.0.3. *The number of N_2 quadratic Latin squares of order q is $7q^2/32 + O(q^{3/2})$.*

Let n be a positive integer. The maximum number of intercalates in a Latin square of order n is $n^2(n-1)/4$ and there is a Latin square of order n that achieves this bound if and only if n is a power of 2 (see, e.g., [61]). On the other hand, there is a Latin square of order n with at least $(n-1)(n-3)(n-15)/8$ intercalates [19]. By Theorem 6.0.1, a Latin square $\mathcal{L}[a, b]$ of order q with $b \in \{-a, 2-a, a/(2a-1)\}$ has at least $q(q-1)(q - 11q^{1/2} - 38)/32 = \Theta(q^3)$

intercalates, which is within a constant factor of the maximum number of intercalates that a Latin square of order q can contain. It will be justified at the end of §6.2 that a square $\mathcal{L}[a,b]$ of order q with $b \in \{-a, 2-a, a/(2a-1)\}$ exists whenever $9 \leqslant q \equiv 1 \bmod 4$.

Our next main result gives a partial answer to the question of when a quadratic Latin square is row-Hamiltonian. We prove that for each prime p, there are only finitely many positive integers d for which a row-Hamiltonian quadratic Latin square of order p^d might exist.

Theorem 6.0.4. *Let P denote the set of all odd primes. There exists a function $f : P \to \mathbb{N}$ such that if $d \geqslant f(p)$ and $\mathcal{L} = \mathcal{L}[a,b]$ is a quadratic Latin square of order $q = p^d$, then $\mathcal{L}$ contains a row cycle of length at most p and it contains a row cycle of length exactly p if $\{a,b\} \not\subseteq \mathbb{F}_p \cap \mathcal{N}_q$.*

We will prove Theorem 6.0.4 by constructing a suitable function f where $f(p) = (1 + o(1))p\log(16)/\log p$ as $p \to \infty$. We note that this function f is not the minimal function satisfying the conditions in Theorem 6.0.4.

The *cycle structure* of a permutation is a sorted list of the lengths of its cycles. Let $\mathcal{L} = \mathcal{L}[a,b]$ be a quadratic Latin square. The cycle structure of any row permutation of $\mathcal{L}$ is equal to the cycle structure of the row permutation $\tau_{0,1}$ of $\mathcal{L}$ or the row permutation $\tau_{0,1}$ of $\mathcal{L}[b,a]$ (see Lemma 6.1.1). Combining this with Lemma 2.3.8 makes it tempting to consider quadratic Latin squares when searching for perfect 1-factorisations or $x^>$-cycle free 1-factorisations of complete bipartite graphs. However, Theorem 6.0.4 tells us that quadratic Latin squares of order p^d will not be useful for constructing perfect 1-factorisations if d is too large. It also tells us that if x is an even integer satisfying $4 \leqslant x < 2p$, then quadratic Latin squares of order p^d are not useful for constructing $x^>$-cycle free 1-factorisations if d is too large, with the possible exceptions of the squares $\mathcal{L}[a,b]$ where $\{a,b\} \subseteq \mathbb{F}_p \cap \mathcal{N}_q$. Note that such squares can only exist when d is odd.

Our next main result resolves the existence problem for anti-perfect 1-factorisations of complete graphs.

Theorem 6.0.5. *There exists an anti-perfect 1-factorisation of K_n for all even integers $n \geqslant 8$.*

We note that all 1-factorisations of K_2, K_4, and K_6 are perfect. As noted in §2.3.3, our contribution to Theorem 6.0.5 is little more than an observation that the construction of $x^>$-cycle free 1-factorisations of complete graphs by Dukes and Ling [46] can be used to construct anti-perfect 1-factorisations of complete graphs of almost all orders. By combining Theorem 6.0.5 with Theorem 2.3.24, we can state the complete existence result of x-cycle free 1-factorisations of complete graphs.

Theorem 6.0.6. *Let n be an even integer and let x be an even integer satisfying $4 \leqslant x \leqslant n$. There exists an x-cycle free 1-factorisation of K_n unless $(n,x) \in \{(2,2),(4,4),(6,6)\}$.*

Next, we strengthen [97, Theorem 5] by resolving the existence problem for anti-atomic Latin squares.

Theorem 6.0.7. *An anti-atomic Latin square of order n exists for all positive integers $n \notin \{2,3,5\}$.*

Theorem 6.0.4 suggests that we might be able to build anti-perfect 1-factorisations and anti-atomic Latin squares using quadratic Latin squares.

Theorem 6.0.8. *Let $n \notin \{1, 3, 5, 15\}$ be an odd positive integer. There exists an anti-atomic Latin square of order n that is the direct product of quadratic Latin squares. If n contains a prime power divisor $m \neq 3$ such that m is not prime or $m \equiv 3 \bmod 4$, then there exists an idempotent, involutory Latin square L of order n that is the direct product of quadratic Latin squares such that the 1-factorisation $\mathscr{G}(L)$ of K_{n+1} is anti-perfect.*

If n is a positive integer and L is an anti-atomic Latin square of order n, then $\mathscr{F}(L)$ is an anti-perfect 1-factorisation of $K_{n,n}$. Thus, Theorem 6.0.8 also implies that we can construct anti-perfect 1-factorisations of complete bipartite graphs using quadratic Latin squares.

Let $(Q, *)$ be a quasigroup. In this chapter, we will use the natural analogs of Definition 2.1.5, Definition 2.1.6, and Definition 2.1.7 for quasigroups. In particular, an automorphism of Q is a map $\theta \in \mathrm{Sym}(Q)$ such that $\theta(x * x) = \theta(x) * \theta(x)$ for all $x \in Q$. We will also refer to a triple $(\theta, \theta, \theta) \in \mathrm{Atp}(Q)$ as an automorphism of Q.

Drápal and Wanless [43] determined the automorphism groups of quadratic quasigroups and also determined exactly when two quadratic quasigroups are isomorphic. Before stating their results, we need to give some definitions.

Let X be a set. Let $\mathrm{Alt}(X) \leqslant \mathrm{Sym}(X)$ be the group of even permutations of X. For $\{h, g\} \subseteq \mathrm{Sym}(X)$, let $h \circ g$ denote the function $x \mapsto h(g(x))$.

Let $\mathbb{S}$ be a subfield of $\mathbb{F}_q$. A permutation $\psi \in \mathrm{Sym}(\mathbb{F}_q)$ is *additive* if $\psi(x+y) = \psi(x)+\psi(y)$ for all $\{x, y\} \subseteq \mathbb{F}_q$ and ψ is $\mathbb{S}$-*linear* if ψ is additive and $\psi(kx) = k\psi(x)$ for all $k \in \mathbb{S}$ and $x \in \mathbb{F}_q$. For $c \in \mathbb{F}_q$, let $\kappa_c : \mathbb{F}_q \to \mathbb{F}_q$ be defined by $x \mapsto x + c$ and let $\lambda_c : \mathbb{F}_q \to \mathbb{F}_q$ be defined by $x \mapsto cx$. Define $\mathcal{T}_q = \{\kappa_c : c \in \mathbb{F}_q\}$. We can identify the general linear group $\mathrm{GL}_d(p)$ with the set of additive permutations in $\mathrm{Sym}(\mathbb{F}_q)$ and we can identify the affine general linear group $\mathrm{AGL}_d(p)$ with the set of permutations in $\mathrm{Sym}(\mathbb{F}_q)$ of the form $\kappa_c \circ \sigma$ where $\sigma \in \mathrm{GL}_d(p)$ and $c \in \mathbb{F}_q$.

Denote the automorphism group of $\mathbb{F}_q$ by $\mathrm{Aut}(\mathbb{F}_q)$ and denote the group of automorphisms of $\mathbb{F}_q$ which fix a subfield $\mathbb{S}$ of $\mathbb{F}_q$ pointwise by $\mathrm{Gal}(\mathbb{F}_q|\mathbb{S})$. Define $\mathrm{A\Gamma^2L_1}(\mathbb{F}_q|\mathbb{S})$ to be the group of all mappings of the form $x \mapsto v\theta(x)+u$ for some $v \in \mathcal{R}_q$, $u \in \mathbb{F}_q$, and $\theta \in \mathrm{Gal}(\mathbb{F}_q|\mathbb{S})$. Suppose that $\mathbb{M}$ is a subfield of $\mathbb{S}$ of order ζ such that $[\mathbb{S} : \mathbb{M}] = 2$. Define $\mathrm{A\Gamma L_1^{tw}}(\mathbb{F}_q|\mathbb{S})$ to be the group consisting of all mappings in $\mathrm{A\Gamma^2L_1}(\mathbb{F}_q|\mathbb{S})$ along with all mappings $x \mapsto v\theta(x^\zeta) + u$ for some $v \in \mathcal{N}_q$, $u \in \mathbb{F}_q$, and $\theta \in \mathrm{Gal}(\mathbb{F}_q|\mathbb{S})$.

The following two theorems were shown in [43].

Theorem 6.0.9. *Quadratic quasigroups $\mathcal{Q}_{a,b}$ and $\mathcal{Q}_{a',b'}$ of order q are isomorphic if and only if there exists some $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ such that $\{a, b\} = \{\theta(a'), \theta(b')\}$.*

Theorem 6.0.10. *Let $\mathcal{Q} = \mathcal{Q}_{a,b}$ be a quadratic quasigroup of order q and let $\mathbb{S}$ be the subfield of $\mathbb{F}_q$ generated by a and b. Then $\mathrm{Aut}(\mathcal{Q}) = \mathrm{A\Gamma^2L_1}(\mathbb{F}_q|\mathbb{S})$ up to these exceptions:*

- *If $a = b$, then $\mathrm{Aut}(\mathcal{Q}) \cong \mathrm{AGL}_k(|\mathbb{S}|)$ where $k = [\mathbb{F}_q : \mathbb{S}]$. The automorphisms of $\mathcal{Q}$ are the maps $\kappa_u \circ \sigma$ where $u \in \mathbb{F}_q$ and $\sigma \in \mathrm{Sym}(\mathbb{F}_q)$ is an $\mathbb{S}$-linear map.*
- *If $|\mathbb{S}| = \zeta^2$ for some integer ζ and $b = a^\zeta$, then $\mathrm{Aut}(\mathcal{Q}) = \mathrm{A\Gamma L_1^{tw}}(\mathbb{F}_q|\mathbb{S})$.*
- *If $q = 7$ and $\{a, b\} = \{3, 5\}$, then $\mathrm{Aut}(\mathcal{Q}) \cong \mathrm{PSL}_2(7)$.*

We prove the analogous result to Theorem 6.0.9 for isotopisms and to Theorem 6.0.10 for autotopisms.

Theorem 6.0.11. *Quadratic quasigroups $\mathcal{Q}_{a,b}$ and $\mathcal{Q}_{a',b'}$ of order q are isotopic if and only if there exists some $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ such that $\{a,b\} = \{\theta(a'), \theta(b')\}$ or both $a = b$ and $a' = b'$.*

Theorem 6.0.12. *Let $\mathcal{Q} = \mathcal{Q}_{a,b}$ be a quadratic quasigroup of order q.*

- *If $a = b$, then $\mathrm{Atp}(\mathcal{Q})$ is isomorphic to the semi-direct product $\mathcal{T}_q^2 \rtimes \mathrm{GL}_d(p)$ with multiplication defined by*
$$((\kappa_u, \kappa_v), \theta) \cdot ((\kappa_w, \kappa_z), \phi) = ((\kappa_{\phi^{-1}(u)+w}, \kappa_{\phi^{-1}(v)+z}), \theta \circ \phi).$$
Every autotopism of $\mathcal{Q}$ is of the form
$$(\lambda_{1-a}^{-1} \circ \theta \circ \kappa_u \circ \lambda_{1-a}, \lambda_a^{-1} \circ \theta \circ \kappa_v \circ \lambda_a, \theta \circ \kappa_{u+v})$$
for some $\theta \in \mathrm{GL}_d(p)$ and $\{u, v\} \subseteq \mathbb{F}_q$.
- *If $a \neq b$, then every autotopism of $\mathcal{Q}$ is an automorphism of $\mathcal{Q}$ and so $\mathrm{Atp}(\mathcal{Q}) \cong \mathrm{Aut}(\mathcal{Q})$.*

Let $\mathcal{Q} = \mathcal{Q}_{a,b}$ and $\mathcal{Q}' = \mathcal{Q}_{a',b'}$ be quadratic quasigroups with $a \neq b$ and $a' \neq b'$. Theorem 6.0.11 tells us that $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic if and only if they are isomorphic. This statement was predicted in [5] in the case where $\mathcal{Q}$ and $\mathcal{Q}'$ are of prime order.

Every parastrophe of a quadratic quasigroup is also a quadratic quasigroup and a result of Wanless [120] allows us to determine these parastrophes. Combining Wanless' result with Theorem 6.0.12 allows us to determine $\mathrm{Apar}(\mathcal{Q})$ for any quadratic quasigroup $\mathcal{Q}$.

Corollary 6.0.3 gives us an estimate of the number of N_2 quadratic Latin squares of order q. Since the N_2 property of a Latin square is a species invariant, it would be useful to know the number of species that contain an N_2 quadratic Latin square of order q. Theorem 6.0.11 allows us to deduce that there are at least $\Omega(q^2/\log q)$ species containing an N_2 quadratic Latin square of order q. Counting problems such as this (see also [5]) partly motivated the study of when quadratic quasigroups are isotopic.

The structure of this chapter is as follows. In §6.1, we develop a general method to study row cycles of quadratic Latin squares. We will then apply these methods in §6.2 to study quadratic Latin squares that contain a row cycle of length 2. This will allow us to prove Theorem 6.0.1 and its corollaries. In §6.3, we will prove Theorem 6.0.4. In §6.4, we prove Theorem 6.0.5, Theorem 6.0.7, and Theorem 6.0.8, our results regarding anti-perfect 1-factorisations and anti-atomic Latin squares. Finally, in §6.5 we investigate autotopisms and isotopisms of quadratic quasigroups and prove Theorem 6.0.11 and Theorem 6.0.12.

6.1 Row cycles of quadratic Latin squares

In this section, we develop a method to investigate row cycles of quadratic Latin squares. Recall from §3.1 that a cycle of length ℓ in a row permutation $\tau_{i,j}$ of a Latin square L corresponds to a row cycle of length ℓ in L hitting rows i and j. Thus, we can understand row cycles of quadratic Latin squares by understanding the cycles in their row permutations.

Let χ denote the extended quadratic character on $\mathbb{F}_q$. Explicitly,

$$\chi(x) = \begin{cases} -1 & \text{if } x \in \mathcal{N}_q, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x \in \mathcal{R}_q. \end{cases}$$

The following result will be used frequently and it is one of our primary motivators for studying quadratic Latin squares.

Lemma 6.1.1. *Let $\mathcal{L} = \mathcal{L}[a,b]$ be a quadratic Latin square of order q and let i and j be distinct elements of $\mathbb{F}_q$.*

(i) If $q \equiv 3 \bmod 4$, then the row permutation $\tau_{i,j}$ of $\mathcal{L}$ has the same cycle structure as the row permutation $\tau_{0,1}$ of $\mathcal{L}$.

(ii) If $q \equiv 1 \bmod 4$, then the row permutation $\tau_{i,j}$ of $\mathcal{L}$ has the same cycle structure as the row permutation $\tau_{0,1}$ of $\mathcal{L}$ if $\chi(j-i) = 1$ and it has the same cycle structure as the row permutation $\tau_{0,1}$ of $\mathcal{L}[b,a]$ if $\chi(j-i) = -1$.

The proof of Lemma 6.1.1 is contained in [120]. Explicitly, it can be proven by combining the arguments used in the proof of [120, Lemma 10] with the fact that the map λ_c is an isomorphism from $\mathcal{L}[a,b]$ to $\mathcal{L}[b,a]$ for any $c \in \mathcal{N}_q$ [120, Lemma 7].

Lemma 6.1.1 tells us that to investigate the lengths of row cycles in quadratic Latin squares, it suffices to investigate the row permutations of quadratic Latin squares mapping row 0 to row 1. Denote the row permutation $\tau_{0,1}$ of a quadratic Latin square $\mathcal{L}[a,b]$ by $\omega[a,b]$ and define the set

$$\Lambda = \left\{ \omega[a,b] : (a,b) \in \mathbb{F}_q^2 \text{ is valid} \right\}.$$

Let $(a,b) \in \mathbb{F}_q^2$ be valid and recall from (2.2) the definition of the quadratic orthomorphism $\varphi[a,b]$. Let $\omega = \omega[a,b] \in \Lambda$ and let $\varphi = \varphi[a,b]$. For distinct i and j in $\mathbb{F}_q$, the row permutation $\tau_{i,j}$ of $\mathcal{L}[a,b]$ satisfies

$$\tau_{i,j} = \kappa_j \circ \varphi \circ \kappa_{i-j} \circ \varphi^{-1} \circ \kappa_{-i}. \tag{6.2}$$

In particular, ω is defined by

$$\omega(x) = \varphi(\varphi^{-1}(x) - 1) + 1. \tag{6.3}$$

A straightforward computation shows that $\varphi^{-1} = \varphi[a^{-1}, b^{-1}]$ if $a \in \mathcal{R}_q$ and $\varphi^{-1} = \varphi[b^{-1}, a^{-1}]$ if $a \in \mathcal{N}_q$.

We now introduce some tools that can be used to investigate the cycles of permutations in Λ. Throughout this section, let $c \in [q] \setminus \{1\}$. Let $\omega \in \Lambda$. We will call a cycle of length c in ω a c-cycle. For a sequence z, we denote the i-th element of z by z_i, starting from z_0. For a cycle μ of ω and element j in the cycle μ, we will write $j \in \mu$.

Definition 6.1.2. Let $z \in \{-1,0,1\}^{2c}$, let $\omega = \omega[a,b] \in \Lambda$, and let $\varphi = \varphi[a,b]$. Suppose that there is a c-cycle μ of ω and element $j \in \mu$ such that $z_{2k} = \chi(\omega^k(j))$ and $z_{2k+1} = \chi(\varphi^{-1}(\omega^k(j)) - 1)$ for each $k \in \{0,1,\ldots,c-1\}$. Then we say that ω *satisfies* z with cycle μ and element $j \in \mu$.

If the conditions of Definition 6.1.2 are satisfied, then we will sometimes simply say that ω satisfies z or that ω satisfies z with element $j \in \mathbb{F}_q$.

Let $\omega = \omega[a,b] \in \Lambda$ and let $\varphi = \varphi[a,b]$. Suppose that ω satisfies a sequence $z \in \{-1,0,1\}^{2c}$ with $z_k = 0$ for some $k \in \{0,1,\ldots,2c-1\}$. Then either $\omega^m(j) = 0$ or $\varphi^{-1}(\omega^m(j)) - 1 = 0$ for some $m \in \{0,1,\ldots,c-1\}$. The former case implies that $0 \in \mu$ and the latter implies that μ contains $\omega^m(j) = \varphi(1) = a$. We will let the cycles of ω containing 0 and a be denoted by ω_0 and ω_a, respectively. These cycles of ω will be treated separately. Thus, we will largely focus on cycles of permutations in Λ that satisfy a sequence in $\{-1,1\}^{2c}$.

For $i \in \{0, 1, \ldots, 2c-1\}$ and $z \in \{-1, 1\}^{2c}$, let z^i denote the sequence defined by $z^i_k = z_{(k+i) \bmod 2c}$. The sequence z^i can be obtained from z by cyclically shifting each of its entries by i positions. We note the following simple observation.

Lemma 6.1.3. *Let $\omega \in \Lambda$ and let $i \in \{0, 1, \ldots, c-1\}$. If ω satisfies $z \in \{-1, 1\}^{2c}$ with element $j \in \mathbb{F}_q$, then ω satisfies z^{2i} with element $\omega^i(j) \in \mathbb{F}_q$.*

We will need the following notation to deal with sequences $z \in \{-1, 1\}^{2c}$.

Definition 6.1.4. Let $\{i, j\} \subseteq \{0, 1, \ldots, 2c-1\}$ with $i \leqslant j$. For a sequence $z \in \{-1, 1\}^{2c}$ define

$$\begin{aligned}
e^+(i,j) &= |\{k \in \{i, i+1, \ldots, j\} : k \text{ is even and } z_k = 1\}|,\\
o^+(i,j) &= |\{k \in \{i, i+1, \ldots, j\} : k \text{ is odd and } z_k = 1\}|,\\
e^-(i,j) &= |\{k \in \{i, i+1, \ldots, j\} : k \text{ is even and } z_k = -1\}|,\\
o^-(i,j) &= |\{k \in \{i, i+1, \ldots, j\} : k \text{ is odd and } z_k = -1\}|.
\end{aligned}$$

Also define

$$\begin{aligned}
u^+(i,j) &= o^+(i,j) - e^+(i,j),\\
u^-(i,j) &= o^-(i,j) - e^-(i,j),\\
v^+(i,j) &= o^+(i,j) - e^-(i,j),\\
v^-(i,j) &= o^-(i,j) - e^+(i,j).
\end{aligned}$$

We note that the values of u^+, u^-, v^+ and v^- implicitly depend on the choice of sequence $z \in \{-1, 1\}^{2c}$. If $\{i, j\} \subseteq \{0, 1, \ldots, 2c-1\}$ with $i > j$, then we set $u^+(i,j) = u^-(i,j) = v^+(i,j) = v^-(i,j) = 0$, regardless of the sequence z.

We now prove a result concerning how permutations in Λ act on elements of $\mathbb{F}_q$. We will need to consider the cases $a \in \mathcal{R}_q$ and $a \in \mathcal{N}_q$ separately. We will repeatedly use the simple property that $u^+(i,j) + u^+(j+1,k) = u^+(i,k)$ for any $\{i, j, k\} \subseteq \{0, 1, \ldots, 2c-1\}$ such that $i \leqslant j \leqslant k$, regardless of the sequence z. The same holds when replacing u^+ by u^-, v^+ or v^-.

Lemma 6.1.5. *Let $\omega = \omega[a, b] \in \Lambda$ with $a \in \mathcal{R}_q$, let $\varphi = \varphi[a, b]$, and let $z \in \{-1, 1\}^{2c}$. Suppose that ω satisfies z with element $j \in \mathbb{F}_q$. Then for all $m \in \{0, 1, \ldots, c\}$,*

$$\omega^m(j) = a^{u^+(0,2m-1)} b^{u^-(0,2m-1)} j + \sum_{k=1}^{2m} (-1)^k a^{u^+(k,2m-1)} b^{u^-(k,2m-1)} \tag{6.4}$$

and

$$\varphi^{-1}(\omega^m(j)) - 1 = a^{u^+(0,2m)} b^{u^-(0,2m)} j + \sum_{k=1}^{2m+1} (-1)^k a^{u^+(k,2m)} b^{u^-(k,2m)}. \tag{6.5}$$

Proof. We will prove the claim by induction on m. If $m = 0$, then (6.4) simply states that $\omega^m(j) = j$, which is trivially true. Since ω satisfies z, we know that $\chi(j) = z_0$. Hence, $\varphi^{-1}(j) - 1 = a^{-e^+(0,0)} b^{-e^-(0,0)} j - 1$, which agrees with (6.5). Now suppose that (6.4) and (6.5)

hold for some $m \in \{0, 1, \ldots, c-1\}$. Then,

$$\begin{aligned}
\omega^{m+1}(j) &= \varphi(\varphi^{-1}(\omega^m(j)) - 1) + 1 \\
&= a^{o^+(2m+1,2m+1)} b^{o^-(2m+1,2m+1)} (\varphi^{-1}(\omega^m(j)) - 1) + 1 \\
&= a^{u^+(2m+1,2m+1)} b^{u^-(2m+1,2m+1)} \left(a^{u^+(0,2m)} b^{u^-(0,2m)} j + \right. \\
&\quad \left. \sum_{k=1}^{2m+1} (-1)^k a^{u^+(k,2m)} b^{u^-(k,2m)} \right) + 1 \\
&= a^{u^+(0,2m+1)} b^{u^-(0,2m+1)} j + \left(\sum_{k=1}^{2m+1} (-1)^k a^{u^+(k,2m+1)} b^{u^-(k,2m+1)} \right) + 1 \\
&= a^{u^+(0,2m+1)} b^{u^-(0,2m+1)} j + \sum_{k=1}^{2m+2} (-1)^k a^{u^+(k,2m+1)} b^{u^-(k,2m+1)},
\end{aligned}$$

which agrees with (6.4). Thus,

$$\begin{aligned}
\varphi^{-1}(\omega^{m+1}(j)) - 1 &= a^{-e^+(2m+2,2m+2)} b^{-e^-(2m+2,2m+2)} \omega^{m+1}(j) - 1 \\
&= a^{u^+(2m+2,2m+2)} b^{u^-(2m+2,2m+2)} \left(a^{u^+(0,2m+1)} b^{u^-(0,2m+1)} j + \right. \\
&\quad \left. \sum_{k=1}^{2m+2} (-1)^k a^{u^+(k,2m+1)} b^{u^-(k,2m+1)} \right) - 1 \\
&= a^{u^+(0,2m+2)} b^{u^-(0,2m+2)} j + \left(\sum_{k=1}^{2m+2} (-1)^k a^{u^+(k,2m+2)} b^{u^-(k,2m+2)} \right) - 1 \\
&= a^{u^+(0,2m+2)} b^{u^-(0,2m+2)} j + \sum_{k=1}^{2m+3} (-1)^k a^{u^+(k,2m+2)} b^{u^-(k,2m+2)},
\end{aligned}$$

which agrees with (6.5). The lemma follows by induction. □

Using analogous arguments as in the proof of Lemma 6.1.5, we can prove the following result.

Lemma 6.1.6. *Let $\omega = \omega[a, b] \in \Lambda$ with $a \in \mathcal{N}_q$, let $\varphi = \varphi[a, b]$, and let $z \in \{-1, 1\}^{2c}$. Suppose that ω satisfies z with element $j \in \mathbb{F}_q$. Then for all $m \in \{0, 1, \ldots, c\}$,*

$$\omega^m(j) = a^{v^+(0,2m-1)} b^{v^-(0,2m-1)} j + \sum_{k=1}^{2m} (-1)^k a^{v^+(k,2m-1)} b^{v^-(k,2m-1)}$$

and

$$\varphi^{-1}(\omega^m(j)) - 1 = a^{v^+(0,2m)} b^{v^-(0,2m)} j + \sum_{k=1}^{2m+1} (-1)^k a^{v^+(k,2m)} b^{v^-(k,2m)}.$$

Let $\omega = \omega[a, b] \in \Lambda$ with $a \in \mathcal{R}_q$ and consider Lemma 6.1.5. Setting $m = c$ in (6.4) we see

that

$$j = a^{u^+(0,2c-1)}b^{u^-(0,2c-1)}j + \sum_{k=1}^{2c}(-1)^k a^{u^+(k,2c-1)}b^{u^-(k,2c-1)}. \tag{6.6}$$

In order to investigate (6.6), we will distinguish two cases, depending on whether or not $a^{u^+(0,2c-1)}b^{u^-(0,2c-1)}$ is equal to 1. We also need to make the analogous case distinction when $a \in \mathcal{N}_q$.

Recall that, for an integer $m \in [q-1]$, an m-th root of unity in $\mathbb{F}_q$ is an element $x \in \mathbb{F}_q$ such that $x^m = 1$. We will say that all non-zero elements of $\mathbb{F}_q$ are 0-th roots of unity. If $m \in \{1-q, 2-q, \dots, -1\}$, then we will say that x is an m-th root of unity if x^{-1} is a $(-m)$-th root of unity. Let $\omega = \omega[a,b] \in \Lambda$ and let $z \in \{-1,1\}^{2c}$. Define

$$t(z,\omega) = \begin{cases} u^+(0,2c-1) & \text{if } a \in \mathcal{R}_q, \\ v^+(0,2c-1) & \text{if } a \in \mathcal{N}_q. \end{cases}$$

It is immediate from Definition 6.1.4 that $e^-(0,2c-1) = c - e^+(0,2c-1)$ and $o^-(0,2c-1) = c - o^+(0,2c-1)$. Hence,

$$u^-(0,2c-1) = c - o^+(0,2c-1) - (c - e^+(0,2c-1)) = e^+(0,2c-1) - o^+(0,2c-1) = -u^+(0,2c-1).$$

Similarly, $v^-(0,2c-1) = -v^+(0,2c-1)$. Thus, $a^{u^+(0,2c-1)}b^{u^-(0,2c-1)} = (ab^{-1})^{t(z,\omega)}$ if $a \in \mathcal{R}_q$ and $a^{v^+(0,2c-1)}b^{v^-(0,2c-1)} = (ab^{-1})^{t(z,\omega)}$ if $a \in \mathcal{N}_q$. We therefore make the following definition.

Definition 6.1.7. Let $\omega = \omega[a,b] \in \Lambda$ and let $z \in \{-1,1\}^{2c}$. We say that the pair (z,ω) is of *Type One* if ab^{-1} is not a $t(z,\omega)$-th root of unity in $\mathbb{F}_q$. Otherwise, we say that (z,ω) is of *Type Two*.

Fix a permutation $\omega = \omega[a,b] \in \Lambda$ and let $z' \in \{-1,1\}^{2c}$. We will say that z' is a Type One sequence or Type Two sequence according to whether the pair (z',ω) is of Type One or Type Two. Of course, the type of z' is not an intrinsic property of z', since it depends on ω. Let $\mu \notin \{\omega_0, \omega_a\}$ be a c-cycle of ω and let $j \in \mu$. Using Definition 6.1.2, we can associate a sequence $z \in \{-1,1\}^{2c}$ to the pair (μ, j). Furthermore, by Lemma 6.1.3 we know that changing the element j of μ simply changes z to z^{2i} for some $i \in \{0,1,\dots,c-1\}$. It is easy to verify that (z,ω) is of Type One if and only if (z^{2i},ω) is of Type One for every $i \in \{0,1,\dots,c-1\}$. Thus, we define μ to be a Type One cycle if (z,ω) is of Type One and we define μ to be a Type Two cycle otherwise.

Our goal in this section is to develop a method to investigate the cycles of a permutation $\omega \in \Lambda$. To do this, we will study Type One cycles, Type Two cycles, and the cycles ω_0 and ω_a separately.

6.1.1 Type One cycles

In this subsection, we prove a characterisation of when a permutation in Λ contains a Type One cycle of length c.

Let k be a positive integer and let $x \in \{-1,1\}^k$. For a positive integer m, we denote by

$\bigoplus_{\ell=1}^{m} x$ the sequence obtained by concatenating m copies of x. Explicitly,

$$\left(\bigoplus_{\ell=1}^{m} x\right)_i = x_{i \bmod k}.$$

Definition 6.1.8. Let k be a positive integer and let $z \in \{-1,1\}^{2k}$. We call z *even periodic with period* r if we can write $z = \bigoplus_{\ell=1}^{k/r} y$ for some divisor r of k and $y \in \{-1,1\}^{2r}$. If z is even periodic with period r for some proper divisor r of k, then z is *even periodic*. If r is the smallest divisor of k such that z is even periodic with period r, then z has *least period* r.

Let r be a divisor of c and suppose that $z \in \{-1,1\}^{2c}$ is even periodic with period r. It is simple to verify that

$$u^+(k, 2c-1) = \left(\frac{c}{r} - \left\lceil \frac{k+1}{2r} \right\rceil\right) u^+(0, 2r-1) + u^+(k \bmod 2r, 2r-1) \tag{6.7}$$

for all $k \in \{0, 1, \ldots, 2c-1\}$. In particular, $u^+(0, 2c-1) = (c/r)u^+(0, 2r-1)$. If we replace u^+ by v^+, then (6.7) still holds for any $k \in \{0, 1, \ldots, 2c-1\}$. We will now show that a permutation in Λ cannot satisfy an even periodic sequence of Type One.

Lemma 6.1.9. *Let $\omega \in \Lambda$ and let $z \in \{-1,1\}^{2c}$ be an even periodic sequence. If ω satisfies z, then (z, ω) is of Type Two.*

Proof. Let $(a, b) \in \mathbb{F}_q^2$ be such that $\omega = \omega[a, b]$, let r be a proper divisor of c so that z is even periodic with period r, let $j \in \mathbb{F}_q$ be such that ω satisfies z with j, and let μ be the cycle of ω such that $j \in \mu$. We will prove the lemma for the case where $a \in \mathcal{R}_q$. The case where $a \in \mathcal{N}_q$ can be handled using analogous arguments. From Lemma 6.1.5 we know that

$$\begin{aligned}
\omega^c(j) &= a^{u^+(0,2c-1)} b^{u^-(0,2c-1)} j + \sum_{k=1}^{2c} (-1)^k a^{u^+(k,2c-1)} b^{u^-(k,2c-1)} \\
&= (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^{c/r} j + \\
&\quad \sum_{k=1}^{2c} (-1)^k \left((a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^{c/r - \lceil (k+1)/(2r) \rceil} a^{u^+(k \bmod 2r, 2r-1)} b^{u^-(k \bmod 2r, 2r-1)} \right) \\
&= (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^{c/r} j + \sum_{k=1}^{2r} (-1)^k \sum_{i=0}^{c/r-1} (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^i a^{u^+(k,2r-1)} b^{u^-(k,2r-1)} \\
&= (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^{c/r} j + \sum_{i=0}^{c/r-1} (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^i \sum_{k=1}^{2r} (-1)^k a^{u^+(k,2r-1)} b^{u^-(k,2r-1)}.
\end{aligned} \tag{6.8}$$

Suppose, for a contradiction, that z is a Type One sequence. So $a^{u^+(0,2c-1)} b^{u^-(0,2c-1)} \neq 1$, hence $a^{u^+(0,2r-1)} b^{u^-(0,2r-1)} \neq 1$ also. Thus we can write

$$\sum_{i=0}^{c/r-1} (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^i = \frac{1 - (a^{u^+(0,2r-1)} b^{u^-(0,2r-1)})^{c/r}}{1 - a^{u^+(0,2r-1)} b^{u^-(0,2r-1)}}. \tag{6.9}$$

Combining (6.8) and (6.9) we obtain

$$\omega^c(j) = (a^{u^+(0,2r-1)}b^{u^-(0,2r-1)})^{c/r}j + \frac{1-(a^{u^+(0,2r-1)}b^{u^-(0,2r-1)})^{c/r}}{1-a^{u^+(0,2r-1)}b^{u^-(0,2r-1)}}\sum_{k=1}^{2r}(-1)^k a^{u^+(k,2r-1)}b^{u^-(k,2r-1)}.$$

Since $\omega^c(j) = j$, it follows that

$$j = \frac{1}{1-a^{u^+(0,2r-1)}b^{u^-(0,2r-1)}}\sum_{k=1}^{2r}(-1)^k a^{u^+(k,2r-1)}b^{u^-(k,2r-1)}.$$

By clearing the denominator we obtain

$$j = a^{u^+(0,2r-1)}b^{u^-(0,2r-1)}j + \sum_{k=1}^{2r}(-1)^k a^{u^+(k,2r-1)}b^{u^-(k,2r-1)} = \omega^r(j)$$

by Lemma 6.1.5. This contradicts the fact that μ is a c-cycle. □

Let $\omega \in \Lambda$ and define

$$X_{c,\omega} = \left\{z \in \{-1,1\}^{2c} : z \text{ is not even periodic and } (z,\omega) \text{ is of Type One}\right\}.$$

Define a relation $\sim$ on $\{-1,1\}^{2c}$ by $z \sim y$ if and only if $z = y^{2i}$ for some $i \in \{0,1,\ldots,c-1\}$. It is simple to verify that $\sim$ forms an equivalence relation on $X_{c,\omega}$. For notational convenience, we will identify an equivalence class of $X_{c,\omega}/\sim$ with an element of that equivalence class.

By combining Lemma 6.1.3 and Lemma 6.1.9 we have the following result.

Lemma 6.1.10. *A permutation $\omega \in \Lambda$ contains a Type One c-cycle if and only if it satisfies a sequence in $X_{c,\omega}/\sim$.*

We can strengthen Lemma 6.1.10 to determine the number of Type One c-cycles in a permutation $\omega \in \Lambda$ in terms of the number of sequences in $X_{c,\omega}/\sim$ that it satisfies.

Lemma 6.1.11. *The number of Type One c-cycles in a permutation $\omega \in \Lambda$ is equal to the number of sequences in $X_{c,\omega}/\sim$ that it satisfies.*

Proof. Let $\omega \in \Lambda$ and suppose that μ is a Type One c-cycle in ω. We can associate to each $j \in \mu$ a sequence $z(j) \in \{-1,1\}^{2c}$ using Definition 6.1.2. By definition, ω satisfies $z(j)$ for each $j \in \mu$. Furthermore, by Lemma 6.1.3 and the definition of $\sim$, we know that there is a unique $j \in \mu$ such that $z(j) \in X_{c,\omega}/\sim$. Let $z = z(j)$ for this particular j. Lemma 6.1.3 and the definition of $\sim$ imply that ω does not satisfy any $z' \in (X_{c,\omega}/\sim) \setminus \{z\}$ with any element $j' \in \mu$. Thus, we can naturally define a map ϕ from the set of Type One c-cycles in ω to the set of sequences in $X_{c,\omega}/\sim$ that ω satisfies. Explicitly, if μ' is a Type One c-cycle in ω, then $\phi(\mu')$ is the unique sequence $z' \in X_{c,\omega}/\sim$ such that ω satisfies z' with some element $j' \in \mu'$. It is immediate from Definition 6.1.2 that ϕ is surjective. Lemma 6.1.5 and Lemma 6.1.6 together imply that if ω satisfies some $z' \in X_{c,\omega}/\sim$, then there is a unique $j \in \mathbb{F}_q$ such that ω satisfies z' with j. Therefore, ϕ is a bijection. The lemma follows. □

For a positive integer m, let Λ_m be the subset of Λ consisting of the permutations $\omega[a,b]$ where ab^{-1} is not a k-th root of unity for any $k \in [m]$. If $\omega \in \Lambda_c$, then the set $X_{c,\omega}$ depends only

on whether $a \in \mathcal{R}_q$ or $a \in \mathcal{N}_q$. Hence, we use $X_{c,1}$ to denote the set $X_{c,\omega}$ for $\omega = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{R}_q$ and we use $X_{c,2}$ to denote the set $X_{c,\omega}$ for $\omega = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{N}_q$. The cardinalities of $X_{c,1}/\sim$ and $X_{c,2}/\sim$ are related to the number of Lyndon words of length c over an alphabet of size 4.

We next work on characterising when a permutation $\omega \in \Lambda$ satisfies a sequence in $X_{c,\omega}/\sim$. Let $z \in \{-1,1\}^{2c}$. Define the bivariate Laurent polynomial $F_{0,z}$ over $\mathbb{F}_q$ by

$$F_{0,z}(x,y) = (1-(xy^{-1})^{u^+(0,2c-1)}) \sum_{k=1}^{2c} (-1)^k x^{u^+(k,2c-1)} y^{u^-(k,2c-1)}.$$

For $i \in [2c-1]$, define

$$F_{i,z}(x,y) = x^{u^+(0,i-1)} y^{u^-(0,i-1)} F_{0,z}(x,y) + (1-(xy^{-1})^{u^+(0,2c-1)})^2 \sum_{k=1}^{i} (-1)^k x^{u^+(k,i-1)} y^{u^-(k,i-1)}.$$

Also define

$$G_{0,z}(x,y) = (1-(xy^{-1})^{v^+(0,2c-1)}) \sum_{k=1}^{2c} (-1)^k x^{v^+(k,2c-1)} y^{v^-(k,2c-1)}$$

and for $i \in [2c-1]$, define

$$G_{i,z}(x,y) = x^{v^+(0,i-1)} y^{v^-(0,i-1)} G_{0,z}(x,y) + (1-(xy^{-1})^{v^+(0,2c-1)})^2 \sum_{k=1}^{i} (-1)^k x^{v^+(k,i-1)} y^{v^-(k,i-1)}.$$

Lemma 6.1.12. *Let $\omega = \omega[a,b] \in \Lambda$ and let $z \in X_{c,\omega}/\sim$. If $a \in \mathcal{R}_q$, then ω satisfies z if and only if $\chi(F_{i,z}(a,b)) = z_i$ for all $i \in \{0,1,\ldots,2c-1\}$. If $a \in \mathcal{N}_q$, then ω satisfies z if and only if $\chi(G_{i,z}(a,b)) = z_i$ for all $i \in \{0,1,\ldots,2c-1\}$.*

Proof. We will prove the lemma in the case where $a \in \mathcal{R}_q$. The case where $a \in \mathcal{N}_q$ can be handled using analogous arguments. Suppose that ω satisfies z with $j \in \mathbb{F}_q$. It follows from Lemma 6.1.5 that $F_{2i,z}(a,b) = (1-(ab^{-1})^{u^+(0,2c-1)})^2 \omega^i(j)$ and $F_{2i+1,z}(a,b) = (1-(ab^{-1})^{u^+(0,2c-1)})^2(\varphi^{-1}(\omega^i(j))-1)$ for all $i \in \{0,1,\ldots,c-1\}$. Since ω satisfies z, it follows that $\chi(F_{i,z}(a,b)) = \chi((1-(ab^{-1})^{u^+(0,2c-1)})^2 F_{i,z}(a,b)) = z_i$ for all $i \in \{0,1,\ldots,2c-1\}$.

Now suppose that $\chi(F_{i,z}(a,b)) = z_i$ for all $i \in \{0,1,\ldots,2c-1\}$. Let $j = F_{0,z}(a,b)/(1-(ab^{-1})^{u^+(0,2c-1)})^2$. It is a simple task to use Lemma 6.1.5 to verify that $\omega^c(j) = j$ and that $\omega^i(j) = F_{2i,z}(a,b)/(1-(ab^{-1})^{u^+(0,2c-1)})^2$ and $\varphi^{-1}(\omega^i(j))-1 = F_{2i+1,z}(a,b)/(1-(ab^{-1})^{u^+(0,2c-1)})^2$ for every $i \in \{0,1,\ldots,c-1\}$. Thus, ω satisfies z with j. □

By combining Lemma 6.1.10 and Lemma 6.1.12, we can characterise when a permutation in Λ contains a Type One cycle of length c. In §6.2, we will see how to use these conditions to bound the number of permutations in Λ_c that contain a Type One c-cycle.

6.1.2 Type Two cycles

In this subsection, we prove necessary conditions for a permutation in Λ to contain a Type Two c-cycle. We also describe how to use these conditions to bound the number of permutations in Λ_c that contain a Type Two cycle of length c.

For a permutation $\omega \in \Lambda$, define $Y_{c,\omega}$ to be the set of sequences $z \in \{-1,1\}^{2c}$ such that (z,ω) is of Type Two. If $\omega = \omega[a,b] \in \Lambda_c$, then $Y_{c,\omega}$ depends only on whether $a \in \mathcal{R}_q$ or $a \in \mathcal{N}_q$. Therefore, we will use $Y_{c,1}$ to denote $Y_{c,\omega'}$ for $\omega' = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{R}_q$ and we will use $Y_{c,2}$ to denote $Y_{c,\omega'}$ for $\omega' = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{N}_q$.

The following is an immediate consequence of Lemma 6.1.3.

Lemma 6.1.13. *A permutation $\omega \in \Lambda$ contains a Type Two c-cycle if and only if it satisfies a sequence in $Y_{c,\omega}/\sim$.*

Next, we want to prove a lemma that relates the number of Type Two c-cycles in a permutation $\omega \in \Lambda$ to the sequences in $Y_{c,\omega}/\sim$ that it satisfies, analogous to Lemma 6.1.11. Let $\omega \in \Lambda$. For a divisor r of c, let $Y^r_{c,\omega}$ be the subset of $Y_{c,\omega}$ consisting of the sequences with least period r. Also, for a sequence $z \in \{-1,1\}^{2c}$, let $s(\omega,z)$ denote the number of $j \in \mathbb{F}_q$ such that ω satisfies z with j.

Lemma 6.1.14. *The number of Type Two c-cycles in a permutation $\omega \in \Lambda$ is*

$$\sum_{r|c} \sum_{z \in Y^r_{c,\omega}/\sim} \frac{r}{c} s(\omega,z).$$

Proof. Let $\omega \in \Lambda$ and let μ be a Type Two c-cycle of ω. Arguing in a similar fashion as in the proof of Lemma 6.1.11, we can associate to μ a sequence $z \in Y_{c,\omega}/\sim$. We say that μ has least period r where r is such that z has least period r.

Let r be a divisor of c. For a c-cycle μ of ω and $j \in \mu$, let $z(j) \in \{-1,1\}^{2c}$ denote the sequence associated to j using Definition 6.1.2. Let A be the set of Type Two c-cycles in ω with least period r and let B be the set of pairs (z,j) where $z \in Y^r_{c,\omega}/\sim$ and ω satisfies z with j. Define a relation between A and B by saying that $\mu \in A$ is related to $(z,j) \in B$ if $j \in \mu$ and $z = z(j)$. Let $\mu \in A$. By Lemma 6.1.3 and the definition of $\sim$, there is a unique $z \in Y^r_{c,\omega}/\sim$ such that ω satisfies z with some $j \in \mu$. Since μ has least period r, it follows that $z(j) = z(\omega^r(j))$ for all $j \in \mu$. Furthermore, if $\{j,j'\} \subseteq \mu$, then $z(j) = z(j')$ if and only if $j' = \omega^{ir}(j)$ for some integer $i \in \{0,1,\ldots,c/r-1\}$. Thus, there are exactly c/r elements $j \in \mathbb{F}_q$ such that ω satisfies z with j. Hence, each $\mu \in A$ is related to exactly c/r elements of B. Conversely, it is immediate from Definition 6.1.2 and the definition of B that each $(z,j) \in B$ is related to exactly one element of A. So $(c/r)|A| = |B|$ and the number of Type Two c-cycles in ω with least period r is exactly

$$\sum_{z \in Y^r_{c,\omega}/\sim} \frac{r}{c} s(\omega,z).$$

The lemma follows. □

Let H be a k-variate Laurent polynomial over $\mathbb{F}_q$ with indeterminates $x_1, x_2, \ldots, x_k$ and let $i \in [k]$. The *total degree of H in x_i*, denoted by $\deg(H, x_i)$, is the difference between the maximum power of x_i in H and the minimum power of x_i in H. If $k = 1$, then we say that H has *total degree* $\deg(H, x_1)$. The *maximum total degree* of H is $\max\{\deg(H, x_i) : i \in [k]\}$.

Lemma 6.1.15. *Let $z \in \{-1,1\}^{2c}$. There is a bivariate Laurent polynomial g over $\mathbb{F}_q$ with maximum total degree at most $2c$ such that if $\omega = \omega[a,b] \in \Lambda$ satisfies z, $a \in \mathcal{R}_q$, and (z,ω) is of Type Two, then (a,b) is a root of g. Similarly, there is a bivariate Laurent polynomial h*

over $\mathbb{F}_q$ with maximum total degree at most $2c$ such that if $\omega = \omega[a,b] \in \Lambda$ satisfies z, $a \in \mathcal{N}_q$, and (z,ω) is of Type Two, then (a,b) is a root of h.

Proof. Let $\omega = \omega[a,b] \in \Lambda$ and suppose that ω satisfies z and that (z,ω) is of Type Two. We will prove the lemma assuming that $a \in \mathcal{R}_q$. Similar arguments can deal with the case where $a \in \mathcal{N}_q$. Since ω satisfies z, it follows from Lemma 6.1.5 that (a,b) is a root of the bivariate Laurent polynomial g defined by

$$g(x,y) = \sum_{k=1}^{2c} (-1)^k x^{u^+(k,2c-1)} y^{u^-(k,2c-1)}.$$

The total degree of g in y is equal to

$$\max\left\{u^-(k,2c-1) : k \in [2c]\right\} - \min\left\{u^-(k,2c-1) : k \in [2c]\right\} \leqslant 2c,$$

because $u^-(k,2c-1) \leqslant c$ for any $k \in \{0,1,\ldots,2c-1\}$. Similarly, $\deg(g,x) \leqslant 2c$. □

For $z \in \{-1,1\}^{2c}$, denote the bivariate Laurent polynomials g and h from Lemma 6.1.15 associated to z by g_z and h_z, respectively. Lemma 6.1.13 and Lemma 6.1.15 can be used together to bound the number of permutations in Λ_c that contain a Type Two c-cycle. The number of roots of a non-zero bivariate Laurent polynomial H over $\mathbb{F}_q$ with indeterminates x and y is at most $q\deg(H,y)$. If a permutation $\omega[a,b] \in \Lambda_c$ with $a \in \mathcal{R}_q$ contains a c-cycle, then Lemma 6.1.15 implies that (a,b) is a root of g_z for some $z \in Y_{c,1}/\!\sim$. Thus, if g_z is not the zero polynomial for any $z \in Y_{c,1}/\!\sim$, then there are at most $2qc|Y_{c,1}/\!\sim|$ permutations $\omega[a,b] \in \Lambda_c$ with $a \in \mathcal{R}_q$ that contain a Type Two c-cycle. Similarly, if h_z is not the zero polynomial for any $z \in Y_{c,2}/\!\sim$, then there are at most $2qc|Y_{c,2}/\!\sim|$ permutations $\omega[a,b] \in \Lambda_c$ with $a \in \mathcal{N}_q$ that contain a Type Two c-cycle. However, if c is equal to the characteristic of $\mathbb{F}_q$, then there do exist sequences $z \in (Y_{c,1}/\!\sim) \cup (Y_{c,2}/\!\sim)$ such that g_z or h_z is the zero polynomial. In this case, we cannot use the described method to obtain any meaningful bound on the number of permutations in Λ_c that contain a Type Two cycle of length c. The fact that there exist sequences $z \in (Y_{c,1}/\!\sim) \cup (Y_{c,2}/\!\sim)$ such that g_z or h_z is the zero polynomial when c is the characteristic of $\mathbb{F}_q$ will be used in §6.3 to prove Theorem 6.0.4.

6.1.3 ω_0 and ω_a

In this subsection, we prove a result that allows us to bound the number of permutations $\omega \in \Lambda$ such that ω_0 or ω_a have length c.

Lemma 6.1.16. *Let $m \in \{0,1,\ldots,q-1\}$. There is a set T_m containing at most 4^m trivariate Laurent polynomials over $\mathbb{F}_q$ that satisfies the following property: For every $\omega = \omega[a,b] \in \Lambda$ and $j \in \mathbb{F}_q$, there is some $t \in T_m$ with with maximum total degree at most m such that $\omega^m(j) = t(a,b,j)$.*

Proof. We will prove the claim by induction on m. When $m = 0$, the set T_0 containing the polynomial t defined by $t(x,y,z) = z$ suffices. Suppose that the claim is true for some $m \in \{0,1,\ldots,q-2\}$. Let $\omega = \omega[a,b] \in \Lambda$. By induction, there is some $t \in T_m$ such that

$\omega^{m+1}(j) = \omega(t(a,b,j))$. If $a \in \mathcal{R}_q$, then

$$\omega^{m+1}(j) = \begin{cases} t(a,b,j) - a + 1 & \text{if } \{t(a,b,j), a^{-1}t(a,b,j) - 1\} \subseteq \mathcal{R}_q, \\ a^{-1}bt(a,b,j) - b + 1 & \text{if } t(a,b,j) \in \mathcal{R}_q \text{ and } a^{-1}t(a,b,j) - 1 \in \mathcal{N}_q, \\ ab^{-1}t(a,b,j) - a + 1 & \text{if } t(a,b,j) \in \mathcal{N}_q \text{ and } b^{-1}t(a,b,j) - 1 \in \mathcal{R}_q, \\ t(a,b,j) - b + 1 & \text{if } \{t(a,b,j), b^{-1}t(a,b,j) - 1\} \subseteq \mathcal{N}_q. \end{cases}$$

Similarly, if $a \in \mathcal{N}_q$, then $\omega^{m+1}(j) \in \{t(a,b,j) - a + 1, a^{-1}bt(a,b,j) - b + 1, ab^{-1}t(a,b,j) - a + 1, t(a,b,j) - b + 1\}$. For $t \in T_m$, define the following trivariate Laurent polynomials:

$$\begin{aligned} H[1,t](x,y,z) &= t(x,y,z) - x + 1, \\ H[2,t](x,y,z) &= x^{-1}yt(x,y,z) - y + 1, \\ H[3,t](x,y,z) &= xy^{-1}t(x,y,z) - x + 1, \\ H[4,t](x,y,z) &= t(x,y,z) - y + 1. \end{aligned}$$

Then define $T_{m+1} = \{H[i,t] : i \in \{1,2,3,4\} \text{ and } t \in T_m\}$. By construction, $\omega^{m+1}(j) = t'(a,b,j)$ for some $t' \in T_{m+1}$. Also, $|T_{m+1}| \leqslant 4|T_m| \leqslant 4^{m+1}$ by induction. Furthermore, if $t \in T_m$, $i \in \{1,2,3,4\}$, and $w \in \{x,y,z\}$, then $|\deg(t,w) - \deg(H[i,t],w)| \leqslant 1$. The lemma follows by induction. □

We can use Lemma 6.1.16 to bound the number of permutations $\omega \in \Lambda$ such that ω_0 or ω_a is a c-cycle. Let T_c be the set of trivariate Laurent polynomials from Lemma 6.1.16. The number of pairs $(a,b) \in \mathbb{F}_q^2$ such that $t(a,b,0) = 0$ for some $t \in T_c$ is at most qc. Since $|T_c| \leqslant 4^c$, it follows that the number of permutations $\omega \in \Lambda$ where ω_0 is a c-cycle is at most $qc4^c$. The same conclusion holds for the number of permutations $\omega \in \Lambda$ such that ω_a is of length c.

6.2 Intercalates in quadratic Latin squares

In this section, we apply the method developed in §6.1 to investigate permutations in Λ that contain cycles of length 2. This will allow us to prove Theorem 6.0.1. A cycle of length 2 in a permutation is also known as a *transposition*.

Fix any two distinct rows i and j of a Latin square L. The number of intercalates of L involving rows i and j is exactly the number of transpositions in the row permutation $\tau_{i,j}$ (or $\tau_{j,i}$) of L. Therefore, in order to count the number of intercalates in a Latin square, it suffices to count the number of transpositions in each of its row permutations. Now let $\mathcal{L} = \mathcal{L}[a,b]$ be a quadratic Latin square of order q. By Lemma 6.1.1, to count the number of transpositions in any row permutation of $\mathcal{L}$, it suffices to count the number of transpositions in the row permutation $\tau_{0,1}$ of $\mathcal{L}$ and if $q \equiv 1 \bmod 4$, also the number of transpositions in the row permutation $\tau_{0,1}$ of $\mathcal{L}[b,a]$. Thus, the main goal in this section is to count the number of transpositions in a permutation in Λ. This will allows us to prove Theorem 6.0.1.

Theorem 6.0.1 is easy to verify in the case where $a = b$, so we will focus on the case where $a \neq b$. Define

$$\Lambda^* = \{\omega[a,b] \in \Lambda : a \neq b\}.$$

We first determine the number of Type One transpositions a permutation $\omega \in \Lambda^*$ contains.

To do this, we construct the sequences in $X_{2,\omega}/\sim$. Then, for each $z \in X_{2,\omega}/\sim$, we apply Lemma 6.1.12 to determine a necessary and sufficient condition for ω to satisfy z. We can take $X_{2,\omega}/\sim$ to be

$$\{(-1,-1,-1,1),(-1,-1,1,-1),(-1,1,1,1),(1,-1,1,1)\}, \tag{6.10}$$

regardless of the choice of $\omega \in \Lambda^*$. Following the described method we obtain Lemma 6.2.1 and Lemma 6.2.2 below.

Lemma 6.2.1. *Let $\omega = \omega[a,b] \in \Lambda^*$ with $a \in \mathcal{R}_q$.*

(i) ω satisfies $(-1,-1,-1,1)$ if and only if $2(b-1)(a-b) \in \mathcal{R}_q$ and $\{(2ab-a-b)(a-b), b(b-1)(a+b)(a-b), b(a+b-2)(a-b)\} \subseteq \mathcal{N}_q$.

(ii) ω satisfies $(-1,-1,1,-1)$ if and only if $2a(1-b)(a-b) \in \mathcal{R}_q$ and $\{(1-b)(a+b)(a-b), b(a+b-2ab)(a-b), (2-a-b)(a-b)\} \subseteq \mathcal{N}_q$.

(iii) ω satisfies $(-1,1,1,1)$ if and only if $\{(a+b-2)(a-b), (a-1)(a+b)(a-b), a(2ab-a-b)(a-b)\} \subseteq \mathcal{R}_q$ and $2b(a-1)(a-b) \in \mathcal{N}_q$.

(iv) ω satisfies $(1,-1,1,1)$ if and only if $\{a(2-a-b)(a-b), (a+b-2ab)(a-b), a(1-a)(a+b)(a-b)\} \subseteq \mathcal{R}_q$ and $2(1-a)(a-b) \in \mathcal{N}_q$.

Lemma 6.2.2. *Let $\omega = \omega[a,b] \in \Lambda^*$ with $a \in \mathcal{N}_q$.*

(i) ω satisfies $(-1,-1,-1,1)$ if and only if $a(1-a)(a+b)(a-b) \in \mathcal{R}_q$ and $\{a(2-a-b)(a-b), 2(1-a)(a-b), (a+b-2ab)(a-b)\} \subseteq \mathcal{N}_q$.

(ii) ω satisfies $(-1,-1,1,-1)$ if and only if $(1-b)(a+b)(a-b) \in \mathcal{R}_q$ and $\{2a(1-b)(a-b), (2-a-b)(a-b), b(a+b-2ab)(a-b)\} \subseteq \mathcal{N}_q$.

(iii) ω satisfies $(-1,1,1,1)$ if and only if $\{a(2ab-a-b)(a-b), 2b(a-1)(a-b), (a+b-2)(a-b)\} \subseteq \mathcal{R}_q$ and $(a-1)(a+b)(a-b) \in \mathcal{N}_q$.

(iv) ω satisfies $(1,-1,1,1)$ if and only if $\{(2ab-a-b)(a-b), b(a+b-2)(a-b), 2(b-1)(a-b)\} \subseteq \mathcal{R}_q$ and $b(b-1)(a+b)(a-b) \in \mathcal{N}_q$.

We can combine the previous two lemmas to count the number of Type One transpositions that a permutation in Λ^* contains.

Lemma 6.2.3. *Let $\omega = \omega[a,b] \in \Lambda^*$.*

- *If (6.1) is not satisfied, then ω contains no Type One transpositions.*
- *If (6.1) is satisfied, then ω contains two Type One transpositions.*

Proof. We distinguish four cases, depending on whether $q \equiv 1 \bmod 4$ or $q \equiv 3 \bmod 4$ and whether $a \in \mathcal{R}_q$ or $a \in \mathcal{N}_q$. There are only minor differences in the arguments for these four cases, so we will only prove the claim in the case where $q \equiv 3 \bmod 4$ and $a \in \mathcal{R}_q$. We know that ω contains a Type One transposition if and only if one of the conditions (i)–(iv) in Lemma 6.2.1 are satisfied. From Lemma 6.2.1, ω satisfies $(-1,-1,-1,1)$ if and only if

$$\{(2ab-a-b)(a-b), b(b-1)(a+b)(a-b), b(a+b-2)(a-b), 2(1-b)(a-b)\} \subseteq \mathcal{N}_q \tag{6.11}$$

and ω satisfies $(1,-1,1,1)$ if and only if

$$\{2(1-a)(a-b), a(a+b-2)(a-b), (2ab-a-b)(a-b), a(a-1)(a+b)(a-b)\} \subseteq \mathcal{N}_q. \tag{6.12}$$

Since $-1 \in \mathcal{N}_q$ and $\{a, b, (a-1)(b-1)\} \subseteq \mathcal{R}_q$, it follows that (6.11) and (6.12) are both equivalent to

$$\{(2ab-a-b)(a-b), (a-1)(a+b)(a-b), (a+b-2)(a-b), 2(1-a)(a-b)\} \subseteq \mathcal{N}_q. \tag{6.13}$$

Thus, the following are all equivalent:

- ω satisfies $(-1,-1,-1,1)$,
- ω satisfies $(1,-1,1,1)$,
- (6.13) is satisfied.

We can use similar arguments to prove that ω satisfies $(-1,-1,1,-1)$ if and only if ω satisfies $(-1,1,1,1)$ if and only if

$$\{(1-a)(a+b)(a-b), (a+b-2ab)(a-b), 2(a-1)(a-b), (2-a-b)(a-b)\} \subseteq \mathcal{N}_q. \tag{6.14}$$

If (6.13) and (6.14) are both true, then $\{(a+b-2)(a-b), (2-a-b)(a-b)\} \subseteq \mathcal{N}_q$, which implies that $-1 \in \mathcal{N}_q$, which is false. Thus, one of the following is true:

- ω satisfies no sequences in (6.10),
- ω satisfies the sequences $(-1,-1,-1,1)$ and $(1,-1,1,1)$ in (6.10) but not $(-1,-1,1,-1)$ or $(-1,1,1,1)$,
- ω satisfies the sequences $(-1,-1,1,-1)$ and $(-1,1,1,1)$ in (6.10) but not $(-1,-1,-1,1)$ or $(1,-1,1,1)$.

Thus, by Lemma 6.1.11, ω contains either zero or two Type One transpositions. Also, ω contains two Type One transpositions if and only if (6.13) or (6.14) is satisfied. It is simple to verify, using the fact that $-1 \in \mathcal{N}_q$, that (6.13) or (6.14) is satisfied if and only if (6.1) is satisfied. □

We next determine how many Type Two transpositions a permutation in Λ^* contains. We know from Lemma 6.1.15 that if $\omega = \omega[a,b] \in \Lambda^*$ satisfies a sequence $z \in Y_{2,\omega}/\sim$, then (a,b) must be a root of the bivariate Laurent polynomial g_z if $a \in \mathcal{R}_q$ and it must be a root of h_z if $a \in \mathcal{N}_q$. If $\omega \in \Lambda_2$ and $a \in \mathcal{R}_q$, then we can take $Y_{2,\omega}/\sim$ to be

$$\{(-1,-1,-1,-1), (-1,-1,1,1), (-1,1,1,-1), (1,1,1,1)\}. \tag{6.15}$$

If $\omega \in \Lambda_2$ and $a \in \mathcal{N}_q$, then we can take $Y_{2,\omega}/\sim$ to be

$$\{(-1,-1,1,1), (-1,1,-1,1), (-1,1,1,-1), (1,-1,1,-1)\}. \tag{6.16}$$

Finally, if $a = -b$, then we can take $Y_{2,\omega}/\sim$ to be

$$\{(-1,-1,-1,-1), (-1,-1,1,1), (-1,1,-1,1), (-1,1,1,-1), (1,-1,1,-1), (1,1,1,1)\}. \tag{6.17}$$

By iterating through the sequences in $Y_{2,\omega}/\sim$, constructing the associated bivariate Laurent polynomials, and checking their roots, we obtain the following lemmas.

Lemma 6.2.4. *Let $\omega = \omega[a, b] \in \Lambda^*$. If ω contains a Type Two transposition, then one of the following is true:*

(i) $b = 2 - a \in \mathcal{R}_q$ *and ω satisfies* $(-1, -1, 1, 1)$ *and no other sequence in* (6.15),

(ii) $b = 2 - a \in \mathcal{N}_q$ *and ω satisfies* $(-1, 1, 1, -1)$ *and no other sequence in* (6.16),

(iii) $b = a/(2a - 1) \in \mathcal{R}_q$ *and ω satisfies* $(-1, 1, 1, -1)$ *and no other sequence in* (6.15),

(iv) $b = a/(2a - 1) \in \mathcal{N}_q$ *and ω satisfies* $(-1, -1, 1, 1)$ *and no other sequence in* (6.16),

(v) $b = -a \in \mathcal{R}_q$ *and ω satisfies* $(-1, 1, -1, 1)$ *or* $(1, -1, 1, -1)$ *and no other sequence in* (6.17),

(vi) $b = -a \in \mathcal{N}_q$ *and ω satisfies* $(-1, -1, -1, -1)$ *or* $(1, 1, 1, 1)$ *and no other sequence in* (6.17).

An immediate corollary of Lemma 6.2.4 is the following.

Corollary 6.2.5. *Let $\omega = \omega[a, b] \in \Lambda^*$ with $b \notin \{-a, 2 - a, a/(2a - 1)\}$. Then ω does not contain a Type Two transposition.*

We note that if $q \equiv 3 \bmod 4$, then there are no permutations $\omega[a, b] \in \Lambda^*$ with $b \in \{-a, 2 - a, a/(2a - 1)\}$. Suppose that $q \equiv 3 \bmod 4$. Since $-1 \in \mathcal{N}_q$, it follows that $-a^2 \in \mathcal{N}_q$, hence $(a, -a)$ is not valid. Since $(2 - a - 1)(a - 1) = -(a - 1)^2 \in \mathcal{N}_q$, the pair $(a, 2 - a)$ is also not valid. Finally, if $(a, a/(2a - 1))$ is a valid pair, then we must have both $a^2/(2a - 1) \in \mathcal{R}_q$ and $-(a - 1)^2/(2a - 1) \in \mathcal{R}_q$ and clearly both cannot be true.

Let $\omega = \omega[a, b] \in \Lambda^*$. Corollary 6.2.5 tells us how many Type Two transpositions ω contains if $b \notin \{-a, 2 - a, a/(2a - 1)\}$. To determine the number of Type Two transpositions in ω if $b \in \{-a, 2 - a, a/(2a - 1)\}$, we will need some tools. If H is a Laurent polynomial over $\mathbb{F}_q$ with a pole at 0, then we will say that $H(0) = \infty$. We will then extend χ to $\mathbb{F}_q \cup \{\infty\}$ by defining $\chi(\infty) = 0$. The following theorem [122] is a version of the Weil bound.

Theorem 6.2.6. *Let H be a monic Laurent polynomial over $\mathbb{F}_q$ of total degree $r > 0$ that is not the square of a Laurent polynomial. For every $e \in \mathbb{F}_q$,*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(eH(x)) \right| \leqslant (r - 1)q^{1/2}. \tag{6.18}$$

In particular, if H is a polynomial over $\mathbb{F}_q$ of degree r that has r distinct roots, then (6.18) *holds.*

In the special case where H is a quadratic polynomial with non-zero discriminant, the following result [82] gives an explicit value for the sum in (6.18).

Theorem 6.2.7. *Let $H \in \mathbb{F}_q[x]$ be a monic, quadratic polynomial with non-zero discriminant. For every $e \in \mathbb{F}_q$,*

$$\sum_{x \in \mathbb{F}_q} \chi(eH(x)) = -\chi(e).$$

We can now count the number of Type Two transpositions in a permutation in Λ^*.

Lemma 6.2.8. *Let $\omega = \omega[a,b] \in \Lambda^*$ and let M denote the number of Type Two transpositions that ω contains. If $b \notin \{-a, 2-a, a/(2a-1)\}$, then $M = 0$. Otherwise,*

$$\frac{q - 11q^{1/2} - 38}{16} \leqslant M \leqslant \frac{q + 11q^{1/2} + 38}{16}.$$

Proof. If $b \notin \{-a, 2-a, a/(2a-1)\}$, then the result is true by Corollary 6.2.5. Now assume that $b \in \{2-a, a/(2a-1)\}$. There are four cases to consider, depending on whether $b = 2-a$ or $b = a/(2a-1)$ and whether $b \in \mathcal{R}_q$ or $b \in \mathcal{N}_q$. There is minimal difference in the arguments used for each case, so we will only consider when $b = 2-a \in \mathcal{R}_q$.

Let $z = (-1,-1,1,1)$. Lemma 6.1.14 and Lemma 6.2.4 together tell us that the number of Type Two transpositions that ω contains is $s(\omega, z)$. Define

$$V = \left\{ j \in \mathbb{F}_q : \{j, (j+a-2)(2-a)^{-1}\} \subseteq \mathcal{N}_q \text{ and } \{j+a-1, a^{-1}(j-1)\} \subseteq \mathcal{R}_q \right\}.$$

Using (6.3) and Definition 6.1.2, it is easy to determine that ω satisfies z with j if and only if $j \in V$. Therefore, $s(\omega, z) = |V|$. Define linear polynomials ℓ_1, ℓ_2, ℓ_3, and ℓ_4 over $\mathbb{F}_q$ by $\ell_1(x) = x$, $\ell_2(x) = (x+a-2)(2-a)^{-1}$, $\ell_3(x) = x+a-1$, and $\ell_4(x) = a^{-1}(x-1)$. Also define the map $W : \mathbb{F}_q \to \mathbb{N}$ by

$$W(x) = (1-\chi(\ell_1(x)))(1-\chi(\ell_2(x)))(1+\chi(\ell_3(x)))(1+\chi(\ell_4(x)))$$

and let

$$S = \sum_{x \in \mathbb{F}_q} W(x).$$

If $x \in V$, then $W(x) = 16$. If $x \in \{0, 2-a, 1-a, 1\}$, then $-8 \leqslant W(x) \leqslant 8$. If $x \in \mathbb{F}_q \setminus (V \cup \{0, 2-a, 1-a, 1\})$, then $W(x) = 0$. Hence,

$$16|V| - 32 \leqslant S \leqslant 16|V| + 32. \tag{6.19}$$

Expanding W and using the fact that χ is a homomorphism on $\mathbb{F}_q^*$, we can write S as a sum consisting of $\binom{4}{k}$ terms of the form $\sum_{x \in \mathbb{F}_q} \chi(\pm J(x))$ where J is the product of k distinct factors in $\{\ell_1, \ell_2, \ell_3, \ell_4\}$ for each $k \in \{0,1,2,3,4\}$. Since (a,b) is valid, it follows that $\{0,1\} \cap \{a,b\} = \varnothing$. So, $|\{0, 2-a, 1-a, 1\}| = 4$. Thus, if J is the product of k distinct factors in $\{\ell_1, \ell_2, \ell_3, \ell_4\}$ for some $k \in \{0,1,2,3,4\}$, then J has k distinct roots. Therefore, we can apply Theorem 6.2.6 or Theorem 6.2.7 to each term of the form $\sum_{x \in \mathbb{F}_q} \chi(\pm J(x))$ with $J \neq 1$. Doing this, we obtain

$$q - 11q^{1/2} - 6 \leqslant S \leqslant q + 11q^{1/2} + 6.$$

Combining this with (6.19) gives the result.

We now deal with the case where $b = -a$. We will assume that $a \in \mathcal{R}_q$, similar arguments can be used to deal with the case where $a \in \mathcal{N}_q$. Let $z' = (-1,1,-1,1)$ and let $z^* = (1,-1,1,-1)$. Lemma 6.1.14 and Lemma 6.2.4 together tell us that the number of Type Two transpositions in ω is $(s(\omega, z') + s(\omega, z^*))/2$. First, consider the sequence z'. The quantity $s(\omega, z')$ is equal to

the cardinality of the set

$$U = \left\{ j \in \mathbb{F}_q : \{j, 1-a-j\} \subseteq \mathcal{N}_q \text{ and } \{-a^{-1}(j+a), a^{-1}(j-1)\} \subseteq \mathcal{R}_q \right\}.$$

Using the same method as above we can determine that

$$\frac{q - 11q^{1/2} - 38}{16} \leqslant |U| \leqslant \frac{q + 11q^{1/2} + 38}{16}.$$

Similarly, we can show that $s(\omega, z^*)$ is between $(q - 11q^{1/2} - 38)/16$ and $(q + 11q^{1/2} + 38)/16$. The lemma follows. □

The way that Theorem 6.2.6 and Theorem 6.2.7 were utilised in the proof of Lemma 6.2.8 is by now a standard technique (see, e.g., [2, 5, 42, 44, 84]). Throughout this chapter, there will be many results whose proofs rely on this technique. For the sake of brevity, we will often not give all the details when we prove such results.

Next, investigate which permutations $\omega \in \Lambda^*$ satisfy $\omega^2(0) = 0$ or $\omega^2(a) = a$.

Lemma 6.2.9. *Let $\omega = \omega[a, b] \in \Lambda^*$ with $b \notin \{-a, 2-a, a/(2a-1)\}$. Then ω_0 is not a transposition.*

Proof. We will distinguish four cases, depending on whether $q \equiv 1 \bmod 4$ or $q \equiv 3 \bmod 4$ and whether $a \in \mathcal{R}_q$ or $a \in \mathcal{N}_q$. We will consider the case where $q \equiv 3 \bmod 4$ and $a \in \mathcal{R}_q$. The other cases can be dealt with using similar arguments. Since $-1 \in \mathcal{N}_q$, it follows that $\omega(0) = \varphi(\varphi^{-1}(0) - 1) + 1 = \varphi(-1) + 1 = 1 - b$. Hence,

$$\omega^2(0) = \begin{cases} 2 - b - a & \text{if } \{1-b, a^{-1} - a^{-1}b - 1\} \subseteq \mathcal{R}_q, \\ a^{-1}b - a^{-1}b^2 - b + 1 & \text{if } 1-b \in \mathcal{R}_q \text{ and } a^{-1} - a^{-1}b - 1 \in \mathcal{N}_q, \\ ab^{-1} - 2a + 1 & \text{if } 1-b \in \mathcal{N}_q \text{ and } b^{-1} - 2 \in \mathcal{R}_q, \\ 2 - 2b & \text{if } \{1-b, b^{-1} - 2\} \subseteq \mathcal{N}_q. \end{cases}$$

Suppose that ω_0 is a transposition. If $\{1-b, a^{-1}-a^{-1}b-1\} \subseteq \mathcal{R}_q$, then $b = 2-a$. If $1-b \in R_q$ and $a^{-1}-a^{-1}b-1 \in \mathcal{N}_q$, then b is a root of the polynomial $a^{-1}x^2+x(1-a^{-1})-1 = a^{-1}(x-1)(x+a)$. Since $b \neq 1$, it follows that $b = -a$. If $1 - b \in \mathcal{N}_q$ and $b^{-1} - 2 \in \mathcal{R}_q$, then $b = a/(2a-1)$. Finally, if $\{1-b, b^{-1}-2\} \subseteq \mathcal{N}_q$, then $b = 1$, which is false. □

Lemma 6.2.10. *Let $\omega = \omega[a, b] \in \Lambda^*$ with $b \notin \{-a, 2-a, a/(2a-1)\}$. Then ω_a is not a transposition.*

Proof. We will first prove the claim assuming that $a \in \mathcal{R}_q$. We have that $\omega(a) = \varphi(\varphi^{-1}(a) - 1) + 1 = \varphi(0) + 1 = 1$. Hence,

$$\omega^2(a) = \varphi(a^{-1} - 1) + 1 = \begin{cases} 2 - a & \text{if } a^{-1} - 1 \in \mathcal{R}_q, \\ a^{-1}b - b + 1 & \text{if } a^{-1} - 1 \in \mathcal{N}_q. \end{cases}$$

If ω_a is a transposition, then $a = 1$ or $b = (a-1)/(a^{-1}-1) = -a$, both of which are false. Using similar arguments, we can show that if $a \in \mathcal{N}_q$ and $\omega^2(a) = a$, then $b \in \{2-a, a/(2a-1)\}$. □

By combining Lemma 6.2.3, Corollary 6.2.5, Lemma 6.2.9, and Lemma 6.2.10, we obtain a complete characterisation of when a permutation $\omega[a,b] \in \Lambda^*$ with $b \notin \{-a, 2-a, a/(2a-1)\}$ contains a transposition. Let $\omega = \omega[a,b] \in \Lambda^*$ with $b \in \{-a, 2-a, a/(2a-1)\}$. Lemma 6.2.8 says that ω contains at least $(q-11q^{1/2}-38)/16$ transpositions. If $q \geqslant 190$, then $(q-11q^{1/2}-38)/16 > 0$, thus ω contains a transposition. If $q < 190$, then we can use a computer to find the permutations $\omega[a,b] \in \Lambda^*$ with $b \in \{-a, 2-a, a/(2a-1)\}$ that contain a transposition. This allows us to complete classify when a permutation in Λ^* contains a transposition.

Lemma 6.2.11. *The permutation $\omega[a,b] \in \Lambda^*$ contains a transposition if and only if one of the following holds:*

1: $(2ab-a-b)(a+b)(a-1) \in \mathcal{R}_q$ *and* $\{2(a+b-2)(a-1), 2a(a+b)\} \subseteq \mathcal{N}_q$,

2: $b = 2-a$ *and* $(q,a) \notin \{(13,3),(13,8),(17,12),(17,15),(37,11),(37,27),(41,13),(41,25)\}$,

3: $b = a/(2a-1)$ *and* $(q,a) \notin \{(13,2),(13,9),(17,5),(17,8),(37,11),(37,27),(41,23),(41,26)\}$,

4: $b = -a$ *and* $(q,a) \notin \{(13,7),(13,11),(17,3),(17,11),(37,10),(37,26),(41,12),(41,17)\}$.

Now that we have characterised when a permutation in Λ^* contains a transposition, we next count the number of transpositions that a permutation in Λ^* contains.

Lemma 6.2.12. *Let $\omega = \omega[a,b] \in \Lambda^*$ and let M denote the number of transpositions that ω contains.*

- *If $b \notin \{-a, 2-a, a/(2a-1)\}$ and (6.1) is satisfied, then $M = 2$.*
- *If $b \notin \{-a, 2-a, a/(2a-1)\}$ and (6.1) is not satisfied, then $M = 0$.*
- *If $b \in \{-a, 2-a, a/(2a-1)\}$, then*

$$\frac{q-11q^{1/2}-38}{16} \leqslant M \leqslant \frac{q+11q^{1/2}+70}{16}.$$

Proof. If $b \notin \{-a, 2-a, a/(2a-1)\}$, then the result follows immediately from the combination of Lemma 6.2.3, Corollary 6.2.5, Lemma 6.2.9, and Lemma 6.2.10. Now suppose that $b \in \{-a, 2-a, a/(2a-1)\}$. Then $0 \in \{a+b, 2ab-a-b, 2-a-b\}$, thus Lemma 6.2.3 implies that ω does not contain a Type One transposition. Therefore, ω contains at most two transpositions that are not of Type Two. The result now follows from Lemma 6.2.8. □

We are now ready to prove Theorem 6.0.1.

Proof of Theorem 6.0.1. First, we deal with the case where $a = b$. Note that $a \notin \{-a, 2-a, a/(2a-1)\}$, since $a \notin \{0,1\}$. It is known [43] that $\mathcal{L}[a,a]$ is isotopic to the Cayley table of the group $(\mathbb{F}_q, +)$. Thus, $\mathcal{L}[a,a]$ does not contain an intercalate. Furthermore, $2(a+a-2)(a-1) = 4(a-1)^2 \in \mathcal{R}_q$, so (6.1) is not satisfied. Hence, the theorem is true when $a = b$.

Now assume that $a \neq b$. Note that $b \in \{-a, 2-a, a/(2a-1)\}$ if and only if $a \in \{-b, 2-b, b/(2b-1)\}$. Let $\omega = \omega[a,b] \in \Lambda^*$. Let M be the number of transpositions in ω and let M' be the number of transpositions in $\omega[b,a]$. By Lemma 6.1.1, if $q \equiv 3 \bmod 4$, then $N = Mq(q-1)/2$ and if $q \equiv 1 \bmod 4$, then $N = (M+M')q(q-1)/4$.

Consider when $b \notin \{-a, 2-a, a/(2a-1)\}$. Corollary 6.2.5, Lemma 6.2.9, Lemma 6.2.10, and Lemma 6.2.12 together imply that any transposition in ω is of Type One and $\{M, M'\} \subseteq \{0, 2\}$. From Lemma 6.2.3, we know that ω contains a transposition if and only if (6.1) is satisfied. Since $\{ab, (a-1)(b-1)\} \subseteq \mathcal{R}_q$, it follows that (6.1) is satisfied if and only if

$$(2ba - b - a)(b + a)(b - 1) \in \mathcal{R}_q \text{ and } \{2(b + a - 2)(b - 1), 2b(b + a)\} \subseteq \mathcal{N}_q,$$

which is true if and only if $\omega[b, a]$ contains a Type One transposition, by Lemma 6.2.3. Thus, $M = M'$ and so $N = 0$ if (6.1) is not satisfied and $N = q(q-1)$ if (6.1) is satisfied.

Now consider when $b \in \{-a, 2-a, a/(2a-1)\}$ and recall that $q \equiv 1 \bmod 4$ in this case. If $\omega[a, b]$ corresponds to an exception in condition 2, 3, or 4 in Lemma 6.2.11, then $\omega[b, a]$ does not correspond to an exception in Lemma 6.2.11. Thus, $\omega[a, b]$ or $\omega[b, a]$ contains a transposition. Also, by Lemma 6.2.12, both M and M' lie between $(q-11q^{1/2}-38)/16$ and $(q+11q^{1/2}+70)/16$, which proves the required bounds on N. □

Corollary 6.0.2 follows immediately from Theorem 6.0.1. We next use Corollary 6.0.2 to prove Corollary 6.0.3.

Proof of Corollary 6.0.3. Fix $a \in \mathbb{F}_q \setminus \{-1, 0, 1, 2\}$ and define

$$V_a = \big\{b \in \mathbb{F}_q : \{ab, (a-1)(b-1), (2ab-a-b)(a+b)(a-1)\} \subseteq \mathcal{R}_q \\ \text{and } \{2(a+b-2)(a-1), 2a(a+b)\} \subseteq \mathcal{N}_q\big\}.$$

If $q \equiv 3 \bmod 4$, then Corollary 6.0.2 implies that $|V_a|$ is the number of quadratic Latin squares of order q of the form $\mathcal{L}[a, b]$ that contain an intercalate. If $q \equiv 1 \bmod 4$, then Corollary 6.0.2 tells us that the number of squares $\mathcal{L}[a, b]$ of order q that contain an intercalate is $|V_a| + m$ for some $m \in \{0, 1, 2, 3\}$. Using Theorem 6.2.6 and Theorem 6.2.7 in an analogous way as in the proof of Lemma 6.2.8, we obtain

$$\frac{1}{32}(q - 58q^{1/2} - 79) \leqslant |V_a| \leqslant \frac{1}{32}(q + 58q^{1/2} + 79).$$

The condition that $a \notin \{-1, 2\}$ is required in order to apply Theorem 6.2.6 and Theorem 6.2.7 to estimate $|V_a|$. Since there are $q-4$ choices for a, it follows that the number of quadratic Latin squares $\mathcal{L}[a', b]$ of order q with $a' \notin \{-1, 2\}$ that contain an intercalate is $q^2/32 + O(q^{3/2})$. From [48], we know that the total number of quadratic Latin squares of order q is $q^2/4 + O(q)$. Clearly, there there are at most $O(q)$ quadratic Latin squares $\mathcal{L}[a', b]$ of order q with $a' \in \{-1, 2\}$. It follows that the number of N_2 quadratic Latin squares of order q is $7q^2/32 + O(q^{3/2})$. □

We have two loose ends to wrap up before concluding this section. Let $c \in \{2, 3, \ldots, q\}$. We first describe how to bound the number of permutations in Λ that contain a cycle of length c. It is easy to find a bound on the number of permutations in $\Lambda \setminus \Lambda_c$. The comments at the end of §6.1.2 and §6.1.3 together describe how to bound the number of permutations in Λ_c that contain a cycle of length c that is not of Type One. As mentioned at the end of §6.1.1, Lemma 6.1.10 and Lemma 6.1.12 together give us a characterisation of permutations in Λ_c that contain a Type One cycle of length c. A plausible method of bounding the number of such permutations is as follows. Construct the sets $X_{c,1}/\!\sim$ and $X_{c,2}/\!\sim$. For each $z \in (X_{c,1}/\!\sim) \cup (X_{c,2}/\!\sim)$, Lemma 6.1.12 provides

a necessary and sufficient condition for a permutation in Λ_c to satisfy z. Use these conditions together with Theorem 6.2.6 and Theorem 6.2.7 to bound the number of permutations in Λ_c that satisfy z. However, to apply Theorem 6.2.6 and Theorem 6.2.7 in the described way, we would need to know when products of functions in the set $\{F_{i,z} : i \in \{0, 1, \ldots, 2c-1\}\}$ and products of functions in $\{G_{i,z} : i \in \{0, 1, \ldots, 2c-1\}\}$ are, up to multiplication by a constant, the square of a bivariate Laurent polynomial. It seems a difficult task to predict when this occurs, unless c is very small.

Finally, as foreshadowed after Theorem 6.0.1, we justify the fact that a quadratic Latin square $\mathcal{L}[a, b]$ of order q with $b \in \{-a, 2-a, a/(2a-1)\}$ exists whenever $9 \leqslant q \equiv 1 \bmod 4$. This fact is easy to prove using Theorem 6.2.6 and Theorem 6.2.7 in a similar way as in the proof of Lemma 6.2.8.

6.3 Row cycles of length p in quadratic Latin squares

In this section, we prove Theorem 6.0.4.

Lemma 6.3.1. *Let $\omega = \omega[a, b] \in \Lambda$ with $a \in \mathcal{R}_q$. If there exists $y \in \mathbb{F}_q$ such that $\{y - ja + j, y - (j+1)a + j : j \in \{0, 1, \ldots, p-1\}\} \subseteq \mathcal{R}_q$, then ω contains a p-cycle.*

Proof. We will prove by induction on $k \in \{0, 1, \ldots, p\}$ that $\omega^k(y) = y - ka + k$. The claim is trivial when $k = 0$. Suppose that $\omega^k(y) = y - ka + k$ for some $k \in \{0, 1, \ldots, p-1\}$. Then $\omega^k(y) \in \mathcal{R}_q$, hence

$$\varphi^{-1}(\omega^k(y)) - 1 = a^{-1}y - (k+1) + ka^{-1} = a^{-1}(y - (k+1)a + k),$$

which is an element of $\mathcal{R}_q$ by assumption. Therefore,

$$\omega^{k+1}(y) = a(a^{-1}(y - (k+1)a + k)) + 1 = y - (k+1)a + (k+1).$$

The lemma follows by induction. □

If the hypotheses of Lemma 6.3.1 hold, then ω satisfies the sequence $z \in \{-1, 1\}^{2p}$ defined by $z_i = 1$ for all $i \in \{0, 1, \ldots, 2p-1\}$. Analogous arguments as those used to prove Lemma 6.3.1 allow us to prove the following.

Lemma 6.3.2. *Let $\omega = \omega[a, b] \in \Lambda$ with $a \in \mathcal{N}_q$. If there exists $y \in \mathbb{F}_q$ such that $\{y - ja + j, y - (j+1)a + j : j \in \{0, 1, \ldots, p-1\}\} \subseteq \mathcal{N}_q$, then ω contains a p-cycle.*

If the hypotheses of Lemma 6.3.2 hold, then ω satisfies the sequence $z \in \{-1, 1\}^{2p}$ defined by $z_i = (-1)^{i+1}$ for all $i \in \{0, 1, \ldots, 2p-1\}$.

We are now ready to prove Theorem 6.0.4.

Proof of Theorem 6.0.4. Let $\omega = \omega[a, b] \in \Lambda$. First, suppose that $\{a, b\} \subseteq \mathbb{F}_p \cap \mathcal{N}_q$. Using Lemma 6.1.6, it is simple to verify that if $j \in \omega_0$, then $j \in \mathbb{F}_p$. Thus, ω has a cycle of length at most p.

Now we deal with the case where $\{a, b\} \not\subseteq \mathbb{F}_p \cap \mathcal{N}_q$. So either $\{a, b\} \subseteq \mathbb{F}_p \cap \mathcal{R}_q$ or $\{a, b\} \not\subseteq \mathbb{F}_p$. We will deal with the latter case first. Recall that $\mathcal{L}[a, b]$ and $\mathcal{L}[b, a]$ are isomorphic [120].

Therefore, by Lemma 2.3.7, it suffices to prove that ω or $\omega[b,a]$ has a cycle of length p. Thus, we may assume that $a \notin \mathbb{F}_p$. We will first consider when $a \in \mathcal{R}_q \setminus \mathbb{F}_p$. Define

$$Y = \left\{y \in \mathbb{F}_q : \{y - ja + j, y - (j+1)a + j\} \subseteq \mathcal{R}_q \text{ for all } j \in \{0, 1, \ldots, p-1\}\right\}. \tag{6.20}$$

By Lemma 6.3.1, if $Y \neq \varnothing$, then ω contains a p-cycle. For $j \in \{0, 1, \ldots, p-1\}$, define linear polynomials ℓ_j and ℓ'_j over $\mathbb{F}_q$ by $\ell_j(y) = y - ja + j$ and $\ell'_j(y) = y - (j+1)a + j$. Also define the map $W : \mathbb{F}_q \to \mathbb{N}$ by

$$W(y) = \prod_{j=0}^{p-1}(1 + \chi(\ell_j(y)))(1 + \chi(\ell'_j(y)))$$

and let

$$S = \sum_{y \in \mathbb{F}_q} W(y).$$

If $y \in Y$, then $W(y) = 4^p$. If $y \in \{ja - j, (j+1)a - j : j \in \{0, 1, \ldots, p-1\}\}$, then $W(y) \leqslant 2^{2p-1}$. In all other cases, $W(y) = 0$. It follows that $S \leqslant 4^p|Y| + p4^p$. Expanding W and using the fact that χ is a homomorphism on $\mathbb{F}_q^*$, we can write S as a sum consisting of $\binom{2p}{k}$ terms of the form $\sum_{x \in \mathbb{F}_q} \chi(\pm J(y))$ where J is the product of k distinct factors in $\{\ell_j, \ell'_j : j \in \{0, 1, \ldots, p-1\}\}$ for each $k \in \{0, 1, \ldots, 2p\}$. Let $\{j, \ell\} \subseteq \{0, 1, \ldots, p-1\}$. If $ja - j = \ell a - \ell$, then $j = \ell$. Similarly, if $(j+1)a - j = (\ell+1)a - \ell$, then $j = \ell$. Suppose that $ja - j = (\ell+1)a - \ell$. Then $j \neq \ell + 1$ and so $a = (j - \ell)/(j - \ell - 1) \in \mathbb{F}_p$, which is a contradiction. It follows that if J is the product of k distinct factors in $\{\ell_j, \ell'_j : j \in \{0, 1, \ldots, p-1\}\}$ for some $k \in \{0, 1, \ldots, 2p\}$, then J has k distinct roots. Thus, Theorem 6.2.6 or Theorem 6.2.7 applies to each such term $J \neq 1$. Using these theorems, we obtain the bound

$$S \geqslant q - \binom{2p}{2} - \sum_{k=3}^{2p} \binom{2p}{k}(k-1)q^{1/2} = q + q^{1/2}(p-1)(1 - 4^p + 2p) + p(1 - 2p). \tag{6.21}$$

Combining (6.21) with the fact that $S \leqslant 4^p|Y| + p4^p$ yields

$$|Y| \geqslant 2^{-2p}(q + q^{1/2}(p-1)(1 - 4^p + 2p) + p(1 - 2p - 4^p)).$$

Therefore, $Y \neq \varnothing$ if

$$q + q^{1/2}(p-1)(1 - 4^p + 2p) + p(1 - 2p - 4^p) > 0. \tag{6.22}$$

The inequality (6.22) will hold if

$$q^{1/2} > \frac{1}{2}\left((1-p)(1 - 4^p + 2p) + \left((p-1)^2(1 - 4^p + 2p)^2 - 4p(1 - 2p - 4^p)\right)^{1/2}\right). \tag{6.23}$$

Since $q = p^d$, (6.23) will hold provided that

$$d > \frac{2}{\log p} \log\left(\frac{1}{2}\left((1-p)(1 - 4^p + 2p) + \left((p-1)^2(1 - 4^p + 2p)^2 - 4p(1 - 2p - 4^p)\right)^{1/2}\right)\right).$$

Define $f : P \to \mathbb{N}$ by

$$f(p) = 1 + \left\lfloor \frac{2}{\log p} \log\left(\frac{1}{2}\left((1-p)(1-4^p+2p) + \left((p-1)^2(1-4^p+2p)^2 - 4p(1-2p-4^p)\right)^{1/2}\right)\right)\right\rfloor.$$

Then we have shown that $\mathcal{L}[a,b]$ contains a row cycle of length p if $d \geqslant f(p)$. We can use analogous arguments in conjunction with Lemma 6.3.2 to reach the same conclusion if $a \in \mathcal{N}_q \setminus \mathbb{F}_p$.

We now deal with the case where $\{a,b\} \subseteq \mathbb{F}_p \cap \mathcal{R}_q$. By Lemma 6.3.1, to show that ω contains a p-cycle, it suffices to show that the set Y defined in (6.20) is non-empty. Note that $y - ja + j = y - (k+1)a + k$ where $k = j + a/(1-a)$. Therefore, we can rewrite

$$Y = \left\{y \in \mathbb{F}_q : y - ja + j \in \mathcal{R}_q \text{ for all } j \in \{0, 1, \ldots, p-1\}\right\}.$$

We can use analogous arguments as used in the case where $a \in \mathcal{R}_q \setminus \mathbb{F}_p$ to show that ω contains a p-cycle if

$$d > \frac{2}{\log p} \log\left(\frac{1}{4}\left((2-p)(1-2^p+p) + \left((p-2)^2(1-2^p+p)^2 - 8p(1-p-2^p)\right)^{1/2}\right)\right). \tag{6.24}$$

Since the right hand side of (6.24) is less than $f(p)$, it follows that $\mathcal{L}[a,b]$ contains a row cycle of length p if $d \geqslant f(p)$. □

The function f constructed in the proof of Theorem 6.0.4 satisfies

$$f(p) = \frac{p\log(16)}{\log p}(1 + o(1))$$

as $p \to \infty$. Furthermore, f is not the minimal function that satisfies the conditions of Theorem 6.0.4. This is evidenced by the fact that $f(3) = 9$, but every quadratic Latin square of order 3^d contains a row cycle of length 3 if $d \geqslant 7$.

6.4 Anti-perfect 1-factorisations and anti-atomic Latin squares

In this section, we prove our main results concerning anti-perfect 1-factorisations and anti-atomic Latin squares. Throughout this section, if L is a Latin square, then its row index set, column index set, and symbol set are all equal. To prove Theorem 6.0.5 and Theorem 6.0.7, we need the following definition.

Definition 6.4.1. Let v be a positive integer and let $T \subseteq \mathbb{N} \setminus \{0,1\}$. A *pairwise balanced design* with parameters v and T is a pair $(X, \mathcal{B})$ where X is a set of cardinality v, whose elements are called points, and $\mathcal{B}$ is a collection of subsets of X, called blocks, such that:

- If $B \in \mathcal{B}$, then $|B| \in T$, and
- If x and y are distinct points in X, then there is a unique $B \in \mathcal{B}$ such that $\{x,y\} \subseteq B$.

We say that $(X, \mathcal{B})$ is a PBD(v, T).

There is a method, known as the 'PBD construction', of building Latin squares from pairwise balanced designs, which we describe now. It is a simple fact that an idempotent Latin square of order n exists for all positive integers $n \neq 2$. Let $(X, \mathcal{B})$ be a PBD(v, T) for some positive integer v and some set $T \subseteq \mathbb{N} \setminus \{0, 1, 2\}$. For each $B \in \mathcal{B}$, let L^B be an idempotent Latin square with symbol set B. We can define an idempotent Latin square L of order v with symbol set X by

$$L_{i,j} = \begin{cases} i & \text{if } i = j, \\ L^B_{i,j} & \text{if } i \neq j, \text{ where } B \text{ is the unique block in } \mathcal{B} \text{ with } \{i, j\} \subseteq B. \end{cases} \tag{6.25}$$

We say that L has been obtained from the pairwise balanced design $(X, \mathcal{B})$. Of course, there may be many Latin squares that can be obtained from $(X, \mathcal{B})$, since there may be many choices for the Latin square L^B for each $B \in \mathcal{B}$.

The PBD construction has previously been used to solve various problems, such as the construction of mutually orthogonal Latin squares (see, e.g., [83]) and the construction of $x^>$-cycle free 1-factorisations [17, 45, 46].

We now give a series of simple lemmas regarding Latin squares built using the PBD construction. The first is a simple observation.

Lemma 6.4.2. *Any conjugate of a Latin square obtained from a pairwise balanced design $(X, \mathcal{B})$ can also be obtained from $(X, \mathcal{B})$.*

The following is a known result [45].

Lemma 6.4.3. *Let L be a Latin square obtained from the pairwise balanced design $(X, \mathcal{B})$. Let $\{i, j\} \subseteq X$ with $i \neq j$ and let $B \in \mathcal{B}$ be the block with $\{i, j\} \subseteq B$. Then $\tau_{i,j}(B) = B$.*

It is a well known fact that an idempotent, involutory Latin square of order n exists if and only if n is an odd integer.

Lemma 6.4.4. *Let $(X, \mathcal{B})$ be a pairwise balanced design such that $|B|$ is odd for each $B \in \mathcal{B}$. For each $B \in \mathcal{B}$, let L^B be an idempotent, involutory Latin square with row indices, column indices, and symbols B. Let L be the Latin square obtained from $(X, \mathcal{B})$ defined by (6.25). Then L is involutory.*

Proof. Let $\{i, j\} \subseteq X$ with $i \neq j$ and let $k = L_{i,j}$. Then $k = L^B_{i,j}$ where $B \in \mathcal{B}$ is the block with $\{i, j\} \subseteq B$. Hence, $k \in B$ also. Furthermore, L^B is idempotent and so $k \neq i$. Thus, $L_{i,k} = L^B_{i,k} = j$ because L^B is involutory. The lemma follows. □

Combining Lemma 6.4.2, Lemma 6.4.3, and Lemma 6.4.4, we obtain the following corollary.

Corollary 6.4.5. *Let v be a positive integer and let T and T' be subsets of $\mathbb{N} \setminus \{0, 1, 2\}$ such that T' contains only odd integers. If there exists a PBD(v, T) with at least two blocks, then there exists an anti-atomic Latin square of order v. If there exists a PBD(v, T') with at least two blocks, then there exists an anti-perfect 1-factorisation of K_{v+1}.*

A result of Colbourn, Haddad, and Linek [29] implies the existence of a PBD(v, T) with at least two blocks for some $T \subseteq \mathbb{N} \setminus \{0, 1, 2\}$ that contains only odd integers whenever $v \geqslant 7$ is an odd integer. Combining this with Corollary 6.4.5 proves Theorem 6.0.5.

Let v be an odd integer. As mentioned in §2.3.3, Dukes and Ling [46] have constructed a $1720^{>}$-cycle free 1-factorisation $\mathcal{F}_v$ of K_{v+1}. This 1-factorisation comes from the PBD construction, in the sense that $\mathcal{F}_v = \mathscr{G}(L)$ for some Latin square L of order v that is obtained from a PBD$(v, \{3, 5\})$. Lemma 6.4.3 tells us that $\mathcal{F}_v$ is anti-perfect as long as $v \geqslant 7$.

We next prove Theorem 6.0.7.

Proof of Theorem 6.0.7. A result of Hartman and Heinrich [57] implies the existence of a PBD(v, T) with at least two blocks for some $T \subseteq \mathbb{N} \setminus \{0, 1, 2\}$ whenever $v = 7$ or $v \geqslant 9$ is an integer. Thus, Corollary 6.4.5 implies that there exists an anti-atomic Latin square of order v whenever $v \notin \{1, 2, 3, 4, 5, 6, 8\}$ is a positive integer.

Let v be a positive integer, let G be a group of order v, and let L be the Latin square corresponding to the operation table of G. By [31, Theorem 4.2.2], every conjugate of L is isotopic to L. Thus, Lemma 2.3.7 implies that L is anti-atomic if and only if it does not contain a row cycle of length v. Let g and h be distinct elements of G. Every cycle in the row permutation $\tau_{g,h}$ of L has length equal to the order of gh^{-1} in G. Thus, the existence of a non-cyclic group of order v implies the existence of an anti-atomic Latin square of order v. Thus, an anti-atomic Latin square of order v exist when $v \in \{4, 6, 8\}$. It is easy to verify that every Latin square of order $v \in \{2, 3, 5\}$ contains a row cycle of length v, thus is not anti-atomic. □

The PBD construction was used in [17, 45, 46] to build $x^{>}$-cycle free 1-factorisations of complete bipartite graphs. Lemma 6.4.2 and Lemma 6.4.3 together imply that the Latin squares corresponding to these 1-factorisations are anti-atomic (except for some trivial exceptions). We also record that the operation table of any Steiner quasigroup (see, e.g., [20]) is an anti-atomic Latin square. This gives us a construction of anti-atomic Latin squares of all integer orders $v > 3$ such that $v \equiv 1 \bmod 6$ or $v \equiv 3 \bmod 6$.

Let n be a positive integer. By combining Theorem 6.0.7 and [97, Theorem 5], it follows that an anti-atomic Latin square of order n exists if and only an anti-perfect 1-factorisation of $K_{n,n}$ exists. Of course, if L is an anti-atomic Latin square of order n, then $\mathscr{F}(L)$ is an anti-perfect 1-factorisation of $K_{n,n}$. However, the converse is not true in general. For example, let $\mathcal{L}$ be the quadratic Latin square $\mathcal{L}[2, 6]$ of order 11. Then $\mathscr{F}(\mathcal{L})$ is anti-perfect, but the $(2, 1, 3)$-conjugate of $\mathcal{L}$ is row-Hamiltonian.

The remainder of this section is devoted to proving Theorem 6.0.8. The first step in this direction is to find for which prime powers q there exists an idempotent, involutory quadratic Latin squares of order q that does not contain a row cycle of length q. Every quadratic Latin square is idempotent. The following lemma [63] shows one circumstance where we know that a quadratic Latin square is involutory.

Lemma 6.4.6. *Suppose that $q \equiv 3 \bmod 4$ and let $a \in \mathcal{N}_q \setminus \{-1\}$. The Latin square $\mathcal{L}[a, a^{-1}]$ of order q is involutory.*

Let $\mathcal{L} = \mathcal{L}[a, b]$ be a quadratic Latin square of order q. If $a \in \mathcal{R}_q$, then the row-inverse of $\mathcal{L}$ is $\mathcal{L}[a^{-1}, b^{-1}]$ and if $a \in \mathcal{N}_q$, then the row-inverse of $\mathcal{L}$ is $\mathcal{L}[b^{-1}, a^{-1}]$ [120]. Using this result, it is easy to verify that the only involutory quadratic Latin square of order q that is not covered by Lemma 6.4.6 is the square $\mathcal{L}[-1, -1]$. In particular, if $q \equiv 1 \bmod 4$, then the square $\mathcal{L}[-1, -1]$ of order q is the only involutory quadratic Latin square of order q. Since $\mathcal{L}[-1, -1]$ is isotopic to $(\mathbb{F}_q, +)$, it has a row cycle of length q if and only if q is prime.

The following is a consequence of Corollary 6.0.2.

Lemma 6.4.7. *Suppose that $q \equiv 3 \bmod 4$ and let $a \in \mathcal{N}_q$. The Latin square $\mathcal{L}[a, a^{-1}]$ of order q contains an intercalate if and only if $\{2(1-a), 2(a^2+1)\} \subseteq \mathcal{N}_q$.*

Proof. Corollary 6.0.2 implies that $\mathcal{L}[a, a^{-1}]$ contains an intercalate if and only if

$$(2 - a - a^{-1})(a + a^{-1})(a - 1) \in \mathcal{R}_q \text{ and } \left\{2(a + a^{-1} - 2)(a - 1), 2a(a + a^{-1})\right\} \subseteq \mathcal{N}_q. \quad (6.26)$$

The condition (6.26) is equivalent to the condition

$$\left\{2(a + a^{-1} - 2)(a - 1), 2a(a + a^{-1})\right\} \subseteq \mathcal{N}_q \quad (6.27)$$

because $(2(a+a^{-1}-2)(a-1))(2a(a+a^{-1})) = -4a(2-a-a^{-1})(a+a^{-1})(a-1)$. The condition (6.27) is equivalent to $\{2(1-a), 2(a^2+1)\} \subseteq \mathcal{N}_q$ because $a + a^{-1} - 2 = a^{-1}(a-1)^2$. □

Suppose that $q \equiv 3 \bmod 4$. Dinitz and Dukes [34] studied 1-factorisations of K_{q+1} of the form $\mathscr{G}(\mathcal{L}[a, a^{-1}])$ with $a \in \mathcal{N}_q \setminus \{-1\}$. Among other things, they characterised when such 1-factorisations contain a cycle of length 4. Their Theorem 3.2 is equivalent to our Lemma 6.4.7. Vázquez-Ávila [113] also studied 1-factorisations of the form $\mathscr{G}(\mathcal{L}[a, a^{-1}])$ and showed, among other things, that if $q \equiv 11 \bmod 24$, then there is a 1-factorisation $\mathcal{F}$ of this form such that if g and h are distinct 1-factors in $\mathcal{F}$, then $K_{q+1}[g \cup h]$ contains exactly one cycle of length 4.

Suppose that $q \equiv 3 \bmod 4$ and let $\mathcal{L}$ be an idempotent, involutory quadratic Latin square of order q that contains an intercalate. Lemma 6.1.1 implies that every row permutation of $\mathcal{L}$ contains a transposition, thus $\mathcal{L}$ does not contain a row cycle of length q. We can use Lemma 6.4.7 in conjunction with a standard application of Theorem 6.2.6 and Theorem 6.2.7 to show that there exists an idempotent, involutory quadratic Latin square of order q that contains an intercalate if $q \geqslant 83$. Supplementing this result with a computer search allows us to prove the following.

Lemma 6.4.8. *Suppose that $3 < q \equiv 3 \bmod 4$. There exists an idempotent, involutory quadratic Latin square of order q that contains no row cycle of length q.*

The next step in proving Theorem 6.0.8 is to determine for which prime powers q there exists an anti-atomic quadratic Latin square of order q.

Lemma 6.4.9. *Suppose that $q \notin \{3, 5\}$. There exists an anti-atomic quadratic Latin square of order q.*

Proof. First suppose that $q \equiv 3 \bmod 4$. Our first claim is that there exists a quadratic Latin square of order q that contains an intercalate. If $3 < q < 83$, then a computer search can be used to verify the claim and if $q \geqslant 83$, then the claim follows from the discussion before Lemma 6.4.8. Let $\mathcal{L}$ be a quadratic Latin square of order q that contains an intercalate. Lemma 6.1.1 implies that every row permutation of $\mathcal{L}$ contains a transposition. Since the property of containing an intercalate is a species invariant, it follows that if $\mathcal{L}'$ is a conjugate of $\mathcal{L}$, then $\mathcal{L}'$ also contains an intercalate. Using Lemma 6.1.1 again, we see that that every row permutation of $\mathcal{L}'$ contains a transposition. Thus, $\mathcal{L}$ is anti-atomic.

Now suppose that $q \equiv 1 \bmod 4$. If $q \in \{13, 17, 37, 41\}$, then we can use a computer to verify that an anti-atomic quadratic Latin square of order q exists. So we may assume that $q \notin \{5, 13, 17, 37, 41\}$. We can use Theorem 6.2.6 and Theorem 6.2.7 in the usual way to prove that there exists a valid pair $(a, -a) \in \mathbb{F}_q^2$. Let $\mathcal{L} = \mathcal{L}[a, -a]$ for some valid pair $(a, -a) \in \mathbb{F}_q^2$.

A result of Wanless [120] allows us to deduce the conjugates of a quadratic Latin square. This result implies that every conjugate of $\mathcal{L}$ is of the form $\mathcal{L}[a', b']$ where $b' \in \{-a', 2-a', a'/(2a'-1)\}$. Thus, Lemma 6.1.1 and Lemma 6.2.11 together imply that every row permutation of any conjugate of $\mathcal{L}$ contains a transposition. Therefore, $\mathcal{L}$ is anti-atomic. □

Lemma 6.4.8 proves the second claim of Theorem 6.0.8 in the case where $n \equiv 3 \bmod 4$ is a prime power and Lemma 6.4.9 proves the first claim of Theorem 6.0.8 in the case where n is a prime power. To completely resolve Theorem 6.0.8, we first need to prove some simple results concerning the direct product.

Lemma 6.4.10. *Let L and M be Latin squares. Let the set of lengths of row cycles of L and M be X_1 and X_2, respectively. The set of lengths of row cycles of $L \times M$ is*

$$X_1 \cup X_2 \cup \{\operatorname{lcm}(x_1, x_2) : x_1 \in X_1, x_2 \in X_2\}.$$

Proof. Let symbol set of L and M be S_1 and S_2, respectively, so that the symbol set of $L \times M$ is $S_1 \times S_2$. For distinct i and j in S_1, denote the row permutation of L mapping row i to row j by $u_{i,j}$. Similarly, for distinct k and ℓ in S_2, denote the row permutation of M mapping row k to row ℓ by $v_{k,\ell}$. For convenience, we will define $u_{i,i} = \mathrm{Id}_{S_1}$ and $v_{k,k} = \mathrm{Id}_{S_2}$ for any $i \in S_1$ and $k \in S_2$. Let $\{(i,k),(j,\ell)\} \subseteq S_1 \times S_2$ with $(i,k) \neq (j,\ell)$ and consider the row permutation $\tau_{(i,k),(j,\ell)}$ of $L \times M$. We will show that $\tau_{(i,k),(j,\ell)} = u_{i,j} \times v_{k,\ell}$. Let $x \in S_1 \times S_2$. Then $x = (L \times M)_{(i,k),(g,h)}$ for some $(g,h) \in S_1 \times S_2$. So,

$$\begin{aligned}
\tau_{(i,k),(j,\ell)}(x) &= \tau_{(i,k),(j,\ell)}((L \times M)_{(i,k),(g,h)}) \\
&= (L \times M)_{(j,\ell),(g,h)} \\
&= (L_{j,g}, M_{\ell,h}) \\
&= (u_{i,j}(L_{i,g}), v_{k,\ell}(M_{k,h})) \\
&= u_{i,j} \times v_{k,\ell}(L_{i,g}, M_{k,h}) \\
&= u_{i,j} \times v_{k,\ell}(x).
\end{aligned}$$

Hence, $\tau_{(i,k),(j,\ell)} = u_{i,j} \times v_{k,\ell}$, as claimed. Therefore, the length of the cycle in $\tau_{(i,k),(j,\ell)}$ containing $(y,w) \in S_1 \times S_2$ is the lowest common multiple of the length of the cycle of $u_{i,j}$ containing y and the length of the cycle of $v_{k,\ell}$ containing w. The lemma should now be clear. □

Corollary 6.4.11. *Let L and M be Latin squares such that L or M is anti-atomic. Then $L \times M$ is anti-atomic.*

Proof. Let the order of L and M be n_1 and n_2, respectively. Lemma 6.4.10 implies that if L does not contain a row cycle of length n_1 or M does not contain a row cycle of length n_2, then $L \times M$ does not contain a row cycle of length $n_1 n_2$. It is a simple task to verify that the Ψ-conjugate of $L \times M$ is equal to the direct product of the Ψ-conjugate of L and the Ψ-conjugate of M for any 1-line permutation Ψ of $\{1,2,3\}$. The result follows. □

Lemma 6.4.12. *Let L and M be idempotent, involutory Latin squares. Then $L \times M$ is also idempotent and involutory.*

Proof. Let symbol set of L and M be S_1 and S_2, respectively. Let $(x,y) \in S_1 \times S_2$. Since L and M are idempotent, it follows that $(L \times M)_{(x,y),(x,y)} = (L_{x,x}, M_{y,y}) = (x,y)$. Hence, $L \times M$ is

idempotent. Let $\{(u,v),(s,t)\} \subseteq S_1 \times S_2$ be such that $(L \times M)_{(u,v),(x,y)} = (s,t)$. Then $L_{u,x} = s$ and so $L_{u,s} = x$ because L is involutory. Similarly, $M_{v,t} = y$. Thus, $(L \times M)_{(u,v),(s,t)} = (x,y)$ and so $L \times M$ is involutory. □

We are now ready to prove Theorem 6.0.8.

Proof of Theorem 6.0.8. Let the prime power factorisation of n be $q_1 q_2 \dots q_k$. Since $n \notin \{1,3,5,15\}$, there is some $i \in [k]$ such that $q_i \notin \{3,5\}$. Lemma 6.4.9 says that there exists an anti-atomic quadratic Latin square of order q_i. It is easy to verify that there is a quadratic Latin square of every prime power order. Thus, the existence of an anti-atomic Latin square of order n that is the direct product of quadratic Latin squares follows from Corollary 6.4.11.

We now prove the second claim of the theorem. Assume that n contains a prime power divisor $m \neq 3$ where m is not prime or $m \equiv 3 \bmod 4$. Without loss of generality, $m = q_1$. For each $i \in \{2,3,\dots,k\}$, the Latin square $\mathcal{L}[-1,-1]$ of order q_i is idempotent and involutory. If $m \equiv 3 \bmod 4$, then Lemma 6.4.8 implies the existence of an idempotent, involutory quadratic Latin square of order m that does not contain a row cycle of length m. If m is not prime, then the square $\mathcal{L}[-1,-1]$ of order m is idempotent and involutory and does not contain a row cycle of length m. Combining these facts with Lemma 6.4.10, Lemma 6.4.12, and Lemma 2.3.17 proves the claim. □

6.5 Isotopisms of quadratic quasigroups

In this section, we prove Theorem 6.0.11 and Theorem 6.0.12. This material in this section is more naturally discussed using the language of quasigroups rather than Latin squares. We will also use the term 'parastrophe' rather than 'conjugate' (see Definition 2.1.5) to avoid confusion with the algebraic term conjugate.

We now outline the structure of this section. For a quasigroup Q and $i \in \{1,2,3\}$, denote by $\mathrm{Atp}_i(Q)$ the projection of $\mathrm{Atp}(Q)$ onto the i-th coordinate. Let $\mathcal{Q} = \mathcal{Q}_{a,b}$ be a quadratic quasigroup with $a \neq b$ and let $i \in \{1,2,3\}$. In §6.5.1, we prove that any autotopism of $\mathcal{Q}$ whose components all lie in $\mathrm{AGL}_d(p)$ is an automorphism of $\mathcal{Q}$. In §6.5.2, we prove that $\mathrm{Atp}_i(\mathcal{Q}) \subseteq \mathrm{AGL}_d(p)$ if $\mathrm{Atp}_i(\mathcal{Q})$ is not 2-transitive and in §6.5.3, we prove that $\mathrm{Atp}_i(\mathcal{Q}) \subseteq \mathrm{AGL}_d(p)$ if $\mathrm{Atp}_i(\mathcal{Q})$ is 2-transitive. In §6.5.4, we finish the proof of Theorem 6.0.12 and we prove Theorem 6.0.11.

6.5.1 Autotopisms with components in $\mathrm{AGL}_d(p)$

Some of the arguments that we will use in §6.5.1, §6.5.2, and §6.5.3 to help prove Theorem 6.0.12 do not work for 'small' values of q. Since Theorem 6.0.12 is easy to verify using a computer if $q \leqslant 23$, we will assume, for §6.5.1, §6.5.2, and §6.5.3, that $q > 23$. For these subsections, we will also fix the following definitions and notation. Let $(a,b) \in \mathbb{F}_q^2$ be valid with $a \neq b$, let $\mathcal{Q} = \mathcal{Q}_{a,b}$, let $\mathcal{L} = \mathcal{L}[a,b]$, and let $\varphi = \varphi[a,b]$. Also let $*$ denote the binary operation $*_{a,b}$ defined in §2.4.

The goal of this subsection is to prove Lemma 6.5.1 below, which states that any autotopism of $\mathcal{Q}$ whose components are all elements of $\mathrm{AGL}_d(p)$ is an automorphism of $\mathcal{Q}$. Lemma 6.5.1 is a key ingredient in the proof of Theorem 6.0.12.

Lemma 6.5.1. *Let $(\alpha,\beta,\gamma) \in \mathrm{Atp}(\mathcal{Q})$ and suppose that $\{\alpha,\beta,\gamma\} \subseteq \mathrm{AGL}_d(p)$. Then $\alpha = \beta = \gamma$.*

Proof. Since $\gamma(x * y) = \alpha(x) * \beta(y)$, it follows that

$$\gamma(x + \varphi(y - x)) = \alpha(x) + \varphi(\beta(y) - \alpha(x)). \tag{6.28}$$

By applying the automorphism $\kappa_{-\alpha(0)}$ of $\mathcal{Q}$ to (α, β, γ), we may assume that α fixes 0. Thus, $\gamma \circ \varphi = \varphi \circ \beta$ by (6.28). Since $\{\beta, \gamma\} \subseteq \mathrm{AGL}_d(p)$, there exist $\{g, h\} \subseteq \mathrm{GL}_d(p)$ and $\{u, v\} \subseteq \mathbb{F}_q$ such that $\gamma = \kappa_u \circ g$ and $\beta = \kappa_v \circ h$. Our first goal is to show that $u = v = 0$.

Since $\gamma \circ \varphi = \varphi \circ \beta$, for all $x \in \mathbb{F}_q$ we have $g(\varphi(x)) + u = \varphi(h(x) + v)$ and so $g(x) = \varphi(h(\varphi^{-1}(x)) + v) - u$. Setting $x = 0$ shows that $u = \varphi(v)$. Suppose that $\{x, y\} \subseteq \mathbb{F}_q$ is such that $\chi(x) = \chi(y) = \chi(x + y) = \chi(a)$. Then the value of $g(x + y)$ is

$$\begin{cases} ah(a^{-1}x) + ah(a^{-1}y) + av - \varphi(v) & \text{if } \chi(h(a^{-1}x) + h(a^{-1}y) + v) = 1, \\ bh(a^{-1}x) + bh(a^{-1}y) + bv - \varphi(v) & \chi(h(a^{-1}x) + h(a^{-1}y) + v) \neq 1, \end{cases}$$

and the value of $g(x) + g(y)$ is

$$\begin{cases} ah(a^{-1}x) + ah(a^{-1}y) + 2av - 2\varphi(v) & \text{if } \chi(h(a^{-1}x) + v) = 1 = \chi(h(a^{-1}y) + v), \\ ah(a^{-1}x) + bh(a^{-1}y) + v(a + b) - 2\varphi(v) & \text{if } \chi(h(a^{-1}x) + v) = 1 \neq \chi(h(a^{-1}y) + v), \\ bh(a^{-1}x) + ah(a^{-1}y) + v(a + b) - 2\varphi(v) & \text{if } \chi(h(a^{-1}x) + v) \neq 1 = \chi(h(a^{-1}y) + v), \\ bh(a^{-1}x) + bh(a^{-1}y) + 2bv - 2\varphi(v) & \text{if } 1 \notin \{\chi(h(a^{-1}x) + v), \chi(h(a^{-1}y) + v)\}. \end{cases}$$

Since $g(x + y) = g(x) + g(y)$, we have eight possible cases to consider.

Case 1: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) = 1$, $\chi(h(a^{-1}x) + v) = 1$, and $\chi(h(a^{-1}y) + v) = 1$. Then $av = \varphi(v)$, which implies that $v \in \mathcal{R}_q \cup \{0\}$.

Case 2: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) = 1$, $\chi(h(a^{-1}x) + v) = 1$, and $\chi(h(a^{-1}y) + v) \neq 1$. Then $y = ah^{-1}((bv - \varphi(v))(a - b)^{-1})$.

Case 3: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) = 1$, $\chi(h(a^{-1}x) + v) \neq 1$, and $\chi(h(a^{-1}y) + v) = 1$. Then $x = ah^{-1}((bv - \varphi(v))(a - b)^{-1})$.

Case 4: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) = 1$, $\chi(h(a^{-1}x) + v) \neq 1$, and $\chi(h(a^{-1}y) + v) \neq 1$. Then $y = ah^{-1}(((b - a)h(a^{-1}x) + v(2b - a) - \varphi(v))(a - b)^{-1})$.

Case 5: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) \neq 1$, $\chi(h(a^{-1}x) + v) = 1$, and $\chi(h(a^{-1}y) + v) = 1$. Then $y = ah^{-1}(((a - b)h(a^{-1}x) + v(2a - b) - \varphi(v))(b - a)^{-1})$.

Case 6: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) \neq 1$, $\chi(h(a^{-1}x) + v) = 1$, and $\chi(h(a^{-1}y) + v) \neq 1$. Then $x = ah^{-1}((av - \varphi(v))(b - a)^{-1})$.

Case 7: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) \neq 1$, $\chi(h(a^{-1}x) + v) \neq 1$, and $\chi(h(a^{-1}y) + v) = 1$. Then $y = ah^{-1}((av - \varphi(v))(b - a)^{-1})$.

Case 8: $\chi(h(a^{-1}x) + h(a^{-1}y) + v) \neq 1$, $\chi(h(a^{-1}x) + v) \neq 1$, and $\chi(h(a^{-1}y) + v) \neq 1$. Then $bv = \varphi(v)$, which implies that $v \in \mathcal{N}_q \cup \{0\}$.

Let X denote the set of all elements $x \in \mathbb{F}_q \setminus \{ah^{-1}((bv - \varphi(v))(a - b)^{-1}), ah^{-1}((av - \varphi(v))(b - a)^{-1})\}$ such that $\chi(x) = \chi(a)$. For $x \in X$, let $Y(x)$ denote the set of $y \in \mathbb{F}_q$ such that

$\chi(y) = \chi(x+y) = \chi(a)$ and

$$y \notin \{ah^{-1}((bv-\varphi(v))(a-b)^{-1}), ah^{-1}(((b-a)h(a^{-1}x)+v(2b-a)-\varphi(v))(a-b)^{-1}),\\ ah^{-1}(((a-b)h(a^{-1}x)+v(2a-b)-\varphi(v))(b-a)^{-1}), ah^{-1}((av-\varphi(v))(b-a)^{-1})\}.$$

Suppose, for a contradiction, that $v \neq 0$. First, consider when $v \in \mathcal{R}_q$. By construction, if $x \in X$ and $y \in Y(x)$, then Case 1 must hold. In particular, $\chi(h(a^{-1}x)+h(a^{-1}y)+v) = 1 = \chi(h(a^{-1}x)+v) = \chi(h(a^{-1}y)+v)$. We can use Theorem 6.2.6 and Theorem 6.2.7 in the usual way to show that $Y(x) \neq \varnothing$ for all $x \in X$. This conclusion relies on the fact that $q > 23$. It follows that $\chi(h(a^{-1}x)+v) = 1$ for every $x \in X$.

Define X' to be the set of elements $x \in \mathbb{F}_q \setminus \{bh^{-1}((bv-\varphi(v))(a-b)^{-1}), bh^{-1}((av-\varphi(v))(b-a)^{-1})\}$ such that $\chi(x) = -\chi(a)$. By repeating the above arguments, we can show that $\chi(h(b^{-1}x)+v) = 1$ for every $x \in X'$. Note that if $x \in X$ and $x' \in X'$, then $a^{-1}x \neq b^{-1}x'$, since $\chi(a^{-1}x) = 1$ and $\chi(b^{-1}x') = -1$. Hence, there are at least $2((q-1)/2-2) = q-5$ elements in $\mathbb{F}_q$ such that $\chi(h(x)+v) = 1$. However, the map $\kappa_v \circ h$ is a permutation of $\mathbb{F}_q$, so there are exactly $(q-1)/2$ elements $x \in \mathbb{F}_q$ such that $\chi(h(x)+v) = 1$. This is a contradiction, since $q-5 > (q-1)/2$ because $q > 23$. Analogous arguments can be used to reach a similar contradiction in the case where $v \in \mathcal{N}_q$. Therefore, $v = 0$ and so $u = \varphi(v) = 0$ also.

We may now assume that $\{\alpha, \beta, \gamma\} \subseteq \mathrm{GL}_d(p)$. We will show that $\alpha = \beta$. The lemma will then follow from [121, Lemma 5]. Let $z \in \mathbb{F}_q$. By (6.28), for any $\{x, y\} \subseteq \mathbb{F}_q$,

$$\begin{aligned}\gamma(x+\varphi(y-x))+\gamma(z) &= \gamma(x+z+\varphi(y+z-(x+z)))\\ &= \alpha(x+z)+\varphi(\beta(y+z)-\alpha(x+z))\\ &= \alpha(x)+\alpha(z)+\varphi(\beta(y)+\beta(z)-\alpha(x)-\alpha(z)).\end{aligned} \tag{6.29}$$

Let $k \in \mathbb{F}_q$ be such that $\chi(k) = \chi(\beta(z)-\alpha(z)+k) = 1$. Since $q > 23$, such a $k \in \mathbb{F}_q$ can be shown to exist using Theorem 6.2.6 and Theorem 6.2.7 in the usual way. Let $\{x, y\} \subseteq \mathbb{F}_q$ be such that $\beta(y)-\alpha(x) = k$. From (6.29),

$$\begin{aligned}\gamma(x+\varphi(y-x))+\gamma(z) &= \alpha(x)+\alpha(z)+a(\beta(y)+\beta(z)-\alpha(x)-\alpha(z))\\ &= \alpha(x)+\varphi(\beta(y)-\alpha(x))+\alpha(z)+a(\beta(z)-\alpha(z))\\ &= \gamma(x+\varphi(y-x))+\alpha(z)(1-a)+a\beta(z).\end{aligned}$$

Hence, $\gamma(z) = \alpha(z)(1-a)+a\beta(z)$. Now let $\{x, y\} \subseteq \mathbb{F}_q$ be such that $\chi(\beta(y)-\alpha(x)) = \chi(\beta(y)-\alpha(x)+\beta(z)-\alpha(z)) = -1$. Using the same argument as above, we deduce that $\gamma(z) = \alpha(z)(1-b)+b\beta(z)$. Therefore, $(b-a)(\alpha(z)-\beta(z)) = 0$ and so $\alpha(z) = \beta(z)$, since $a \neq b$. Since z was arbitrary, it follows that $\alpha = \beta$ and so we are done. □

6.5.2 Not 2-transitive autotopism projections

The goal of this subsection is to prove the following lemma.

Lemma 6.5.2. *Let $i \in \{1,2,3\}$. If $\mathrm{Atp}_i(\Omega)$ is not 2-transitive, then $\mathrm{Atp}_i(\Omega) \leqslant \mathrm{AGL}_d(p)$.*

We will need the following simple result.

Lemma 6.5.3. *Let $i \in \{1,2,3\}$ and suppose that there exists some $\delta \in \mathrm{Atp}_i(\Omega)$ such that $\delta(0) = 0$ and $\delta(1) \in \mathcal{N}_q$. Then $\mathrm{Atp}_i(\Omega)$ is 2-transitive.*

Proof. Let $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$. We will show that there is some $\eta \in \mathrm{Atp}_i(\mathcal{Q})$ such that $\eta(0) = x$ and $\eta(1) = y$. This will prove the lemma. If $\chi(y - x) = 1$, then set $\eta = \kappa_x \circ \lambda_{y-x}$. If $\chi(y - x) = -1$, then set $\eta = \kappa_x \circ \lambda_{(y-x)\delta(1)^{-1}} \circ \delta$. □

We are now ready to prove Lemma 6.5.2.

Proof of Lemma 6.5.2. Suppose that $\mathrm{Atp}_i(\mathcal{Q})$ is not 2-transitive. Let $\alpha_1 \in \mathrm{Atp}_i(\mathcal{Q})$ and define $\alpha = \lambda_{((\kappa_{-\alpha_1(0)} \circ \alpha_1)(1))^{-1}} \circ \kappa_{-\alpha_1(0)} \circ \alpha_1$. Note that $\kappa_{-\alpha_1(0)} \circ \alpha_1(1) \in \mathcal{R}_q$ by Lemma 6.5.3 and so $\alpha \in \mathrm{Atp}_i(\mathcal{Q})$. Also note that $\alpha(0) = 0$ and $\alpha(1) = 1$. Suppose that there is some $\{u, v\} \subseteq \mathbb{F}_q$ such that $\chi(v - u) \neq \chi(\alpha(v) - \alpha(u))$. First, assume that $v - u \in \mathcal{R}_q$ and $\alpha(v) - \alpha(u) \in \mathcal{N}_q$. Let $c \in \mathcal{N}_q$ and let $\alpha_2 = \lambda_{c(\alpha(v)-\alpha(u))^{-1}} \circ \kappa_{-\alpha(u)} \circ \alpha \circ \kappa_u \circ \lambda_{v-u} \in \mathrm{Atp}_i(\mathcal{Q})$. Then $\alpha_2(0) = 0$ and $\alpha_2(1) = c$, which contradicts Lemma 6.5.3. Now suppose that $v - u \in \mathcal{N}_q$ and $\alpha(v) - \alpha(u) \in \mathcal{R}_q$. Then $\alpha^{-1}(\alpha(v)) - \alpha^{-1}(\alpha(u)) \in \mathcal{N}_q$. We can thus run the above argument with α^{-1} in place of α to reach a contradiction. Hence, $\chi(v - u) = \chi(\alpha(v) - \alpha(u))$ for every $\{u, v\} \subseteq \mathbb{F}_q$. We can now apply a theorem of Carlitz [25] to conclude that $\alpha \in \mathrm{Aut}(\mathbb{F}_q)$. Thus, $\alpha_1 \in \mathrm{AGL}_d(p)$. Since $\alpha_1 \in \mathrm{Atp}_i(\mathcal{Q})$ was arbitrary, $\mathrm{Atp}_i(\mathcal{Q}) \leqslant \mathrm{AGL}_d(p)$. □

6.5.3 2-transitive autotopism projections

The goal of this subsection is to prove the following lemma.

Lemma 6.5.4. *Let $i \in \{1, 2, 3\}$. If $\mathrm{Atp}_i(\mathcal{Q})$ is 2-transitive, then $\mathrm{Atp}_i(\mathcal{Q}) \leqslant \mathrm{AGL}_d(p)$.*

The group $\mathcal{T}_q$ is an elementary abelian regular subgroup of each $\mathrm{Atp}_i(\mathcal{Q})$. This allows us to make use of Theorem 6.5.5 below, which is a special case of [81, Theorem 1.1]. Let v be a prime power and let u be a positive integer. For the remainder of this section, we will consider any subgroup of $\mathrm{AGL}_u(v)$ to be acting naturally on $\mathbb{F}_{v^u}$ and we will consider any subgroup of $\mathrm{P\Gamma L}_u(v)$ to be acting naturally on the points of the projective space $\mathbf{P}^{u-1}(v)$.

Theorem 6.5.5. *Let X be a set of cardinality $n > 23$ and let $G \leqslant \mathrm{Sym}(X)$ be 2-transitive with an elementary abelian regular subgroup. Then up to permutation isomorphism, one of the following is true:*

(i) $G \leqslant \mathrm{AGL}_u(v)$ *where v is a prime and u is a positive integer such that $n = v^u$.*

(ii) $G \in \{\mathrm{Sym}(X), \mathrm{Alt}(X)\}$.

(iii) $\mathrm{PGL}_u(v) \leqslant G \leqslant \mathrm{P\Gamma L}_u(v)$ *for some prime power v and positive integer u such that $n = (v^u - 1)/(v - 1)$ is prime.*

Let $i \in \{1, 2, 3\}$. If $\mathrm{Atp}_i(\mathcal{Q})$ is 2-transitive, then it satisfies one of (i), (ii), or (iii) in Theorem 6.5.5. We first rule out the possibility that $\mathrm{Atp}_i(\mathcal{Q})$ satisfies Theorem 6.5.5(ii).

Lemma 6.5.6. *Let $n \geqslant 7$ be a positive integer, let Q be a quasigroup of order n, and let $i \in \{1, 2, 3\}$. Then $\mathrm{Atp}_i(Q) \notin \{\mathrm{Sym}(Q), \mathrm{Alt}(Q)\}$.*

Proof. By [18, Theorem 3.1],

$$|\mathrm{Atp}(Q)| \leqslant n^2 \prod_{i=1}^{\lfloor \log_2 n \rfloor} (n - 2^{i-1}). \tag{6.30}$$

It is easy to see that $n!/2$ is strictly larger than the right hand side of (6.30) since $n \geqslant 7$. The result then follows, since $|\mathrm{Atp}_i(Q)| \leqslant |\mathrm{Atp}(Q)|$. □

Let $i \in \{1,2,3\}$. Our next task is to rule out the possibility that $\mathrm{Atp}_i(\mathcal{Q})$ satisfies Theorem 6.5.5(*iii*). Suppose that $\mathrm{Atp}_i(\mathcal{Q})$ does satisfy Theorem 6.5.5(*iii*). So q is prime, there is some prime power v and some positive integer u such that $(v^u-1)/(v-1) = q$, and up to permutation isomorphism, $\mathrm{PGL}_u(v) \leqslant \mathrm{Atp}_i(\mathcal{Q}) \leqslant \mathrm{P\Gamma L}_u(v)$. To reach a contradiction, we consider two cases, depending on whether or not $v = 2$. We first deal with the case where $v \neq 2$. To do this, we prove that there must be an element in $\mathrm{P\Gamma L}_u(v)$ of order $(q-1)/2 = (v^u - v)/(2(v-1))$. We then show that this is impossible. Note that $\mathrm{P\Gamma L}_u(2)$ does contain an element of order $2^{u-1}-1$ and so this method cannot be extended to include the case where $v = 2$.

Lemma 6.5.7. *For each $i \in \{1,2,3\}$, there is an element in $\mathrm{Atp}_i(\mathcal{Q})$ of order $(q-1)/2$.*

Proof. Let $i \in \{1,2,3\}$ and let v be a primitive element of $\mathbb{F}_q^*$. The map $\lambda_{v^2} \in \mathrm{Atp}_i(\mathcal{Q})$ has order $(q-1)/2$. □

Suppose that $v \neq 2$ is a prime power and u is a positive integer such that $(v^u-1)/(v-1) = q$ is prime. Our next task is to rule out the existence of an element of $\mathrm{P\Gamma L}_u(v)$ with order $(v^u-v)/(2(v-1))$. To do this, we will use the following lemma regarding the order of elements in $\mathrm{GL}_u(v)$ (see, e.g., [28]).

Lemma 6.5.8. *Let v be a prime power and let u be a positive integer. Let $A \in \mathrm{GL}_u(v)$ and let $h \in \mathbb{F}_v[x]$ be the minimal polynomial of A with distinct irreducible factors $h_1, h_2, \ldots, h_k$. For $i \in [k]$, let e_i be the degree of h_i and let m_i be the multiplicity of h_i in h. Let $m = \max\{m_i : i \in [k]\}$ and let $n = \lceil \log_r m \rceil$ where r is the characteristic of $\mathbb{F}_v$. Then the order of A divides $\mathrm{lcm}(v^{e_1}-1, v^{e_2}-1, \ldots, v^{e_k}-1)r^n$.*

Lemma 6.5.9. *Suppose that q is prime and that there is a prime power $v \neq 2$ and a positive integer u such that $q = (v^u-1)/(v-1) > 23$. There is no element in $\mathrm{P\Gamma L}_u(v)$ of order $(q-1)/2$.*

Proof. If $(u,v) \in \{(2,4),(2,8),(2,16),(3,3)\}$, then $q \leqslant 23$, which is false. We can use a computer to verify that $\mathrm{P\Gamma L}_3(8)$ has no element of order 36. Therefore, we may assume that $(u,v) \notin \{(2,4),(2,8),(2,16),(3,3),(3,8)\}$. From [41, Lemma 3.1], we know that u is prime and if $v = 4$, then $u = 2$.

Let r be the characteristic of $\mathbb{F}_v$ and let $s = \log_r v$. The proof of this lemma has three parts. First, we prove that there is no element in $\mathrm{GL}_u(v)$ of order $(q-1)/(2x)$ for any divisor x of s. Then, we prove that there is no element in $\mathrm{\Gamma L}_u(v)$ of order $(q-1)/2$. Finally, we prove that there is no element in $\mathrm{P\Gamma L}_u(v)$ with order $(q-1)/2$.

Let x be a divisor of s and suppose, for a contradiction, that A is an element of $\mathrm{GL}_u(v)$ of order $(q-1)/(2x)$. First, suppose that $u = 2$. Then $(q-1)/(2x) = v/(2x)$ and so $v = 2^s$. It is well known that every element of $\mathrm{GL}_2(2^s)$ must have order dividing $2(2^s-1)$ or $2^{2s}-1$. The only way that $v/(2x) = 2^{s-1}/x$ divides $2(2^s-1)$ or $2^{2s}-1$ is if $2^{s-1}/x$ divides 2. Therefore, $2^{s-1} \leqslant 2x \leqslant 2s$, which implies that $s \leqslant 4$. But this implies that $(u,v) \in \{(2,4),(2,8),(2,16)\}$, which is a contradiction.

Now suppose that $u \geqslant 3$ is odd. Let $e_1, e_2, \ldots, e_k$, $m_1, m_2, \ldots, m_k$, m, and n be the parameters from Lemma 6.5.8 relating to the order of A so that $(q-1)/(2x)$ divides $\mathrm{lcm}(v^{e_1} -$

$1, v^{e_2}-1, \ldots, v^{e_k}-1)r^n$ and $m_1e_1 + m_2e_2 + \ldots + m_ke_k \leqslant u$. Without loss of generality, $1 \leqslant e_1 \leqslant e_2 \leqslant \ldots \leqslant e_k \leqslant u$.

Write $2x = r^w x'$ for some integer $w \geqslant 0$ and some integer x' coprime to r. We now prove some restrictions on the values that w can take. If $w \geqslant s$, then $v \leqslant r^w \leqslant 2x \leqslant 2\log_r v$. The only way that $v \leqslant 2\log_r v$ is possible is if $v = 4$. But as noted above, if $v = 4$, then $u = 2$. Thus, $w < s$. Now suppose that $w = s - 1$. First consider when $r \geqslant 3$, so that $2|x'$. Then $r^w = 2x/x' \leqslant s/(x'/2) = (w+1)/(x'/2)$, which implies that $w = 0$ and $x' = 2$. Now consider when $r = 2$. If $x' \neq 1$, then $x' \geqslant 3$, since x' is coprime to r. Thus, $2^w = 2x/x' \leqslant 2s/3 = 2(w+1)/3$, which is a contradiction. Thus, $x' = 1$. Now suppose that $w = s - 2$, $r = 2$, and $u = 3$ and suppose that $x' \neq 1$. Then $2^w = 2x/x' \leqslant 2s/3 = 2(w+2)/3$, which implies that $w \leqslant 1$. Since x' is coprime to r, it follows that $w \neq 0$, thus $w = 1$. Hence, $(u, v) = (3, 8)$, which is a contradiction. To summarise, we have proved the following restrictions on w.

Fact 1: $w < s$.

Fact 2: If $w = s - 1$ and $r \geqslant 3$, then $x' = 2$,

Fact 3: If $w = s - 1$ and $r = 2$, then $x' = 1$.

Fact 4: If $w = s - 2$, $r = 2$, and $u = 3$, then $x' = 1$.

Since $r^{s-w}(v^{u-1}-1)/(x'(v-1)) = (q-1)/(2x)$ divides $\operatorname{lcm}(v^{e_1}-1, v^{e_2}-1, \ldots, v^{e_k}-1)r^n$ and $x'(v-1)$ is coprime to v, it follows that r^{s-w} divides r^n. Thus,

$$s - w \leqslant n = \lceil \log_r m \rceil < \log_r m + 1$$

and so $m > r^{s-w-1}$. Fact 1 implies that r^{s-w-1} is an integer and so $m \geqslant 1 + r^{s-w-1}$. Hence,

$$\sum_{i=1}^{k} e_i \leqslant u - \sum_{i=1}^{k}(m_i - 1)e_i \leqslant u - e_1 r^{s-w-1}, \tag{6.31}$$

where the second inequality in (6.31) is obtained by setting $m_1 = m \geqslant r^{s-w-1} + 1$ and $m_i = 1$ for all $i \in \{2, 3, \ldots, k\}$. By Lemma 6.5.8, there exist pairwise coprime integers $\ell_1, \ell_2, \ldots, \ell_k$ such that $\ell_i | v^{e_i} - 1$ for all $i \in [k]$ and $(v^{u-1}-1)/(x'(v-1)) = \ell_1\ell_2\cdots\ell_k$. Since $v - 1 | v^{e_i} - 1$ for all $i \in [k]$, it follows that there are integers $y_1, y_2, \ldots, y_k$ such that $y_1y_2\cdots y_k | v - 1$ and $\ell_i | y_i(v^{e_i}-1)/(v-1)$ for all $i \in [k]$. Therefore,

$$\frac{v^{u-1}-1}{x'(v-1)} = \prod_{i=1}^{k} \ell_i \left| \prod_{i=1}^{k} y_i \frac{v^{e_i}-1}{v-1} \right| (v-1)^{1-k} \prod_{i=1}^{k} (v^{e_i}-1). \tag{6.32}$$

Also, from (6.31),

$$\prod_{i=1}^{k}(v^{e_i}-1) \leqslant \left(\prod_{i=1}^{k} v^{e_i}\right) - 1 = v^{e_1+e_2+\ldots e_k} - 1 \leqslant v^{u-e_1r^{s-w-1}} - 1. \tag{6.33}$$

Furthermore, the first inequality in (6.33) is strict if $k \geqslant 2$.

We first deal with the case where $k \geqslant 2$. Suppose that $e_1 + e_2 + \ldots + e_k \leqslant u - 2$. Then the

combination of (6.32) and (6.33) yields,

$$v^{u-1} - 1 < x'(v-1)^{2-k}(v^{u-2}-1) \leqslant x'(v^{u-2}-1).$$

This implies that $v^{u-2}(v-x') < 1-x'$ and in particular $v < x' \leqslant 2x \leqslant 2\log_r v$, which is impossible. Thus, we may assume that $e_1 + e_2 + \ldots + e_k \geqslant u-1$. By (6.31), we know that $e_1+e_2+\ldots+e_k = u-1$ and $e_1 = 1 = r^{s-w-1}$. So $s = w+1$. Fact 2 and Fact 3 together imply that $x' \in \{1,2\}$. The combination of (6.32) and (6.33) tells us that $v^{u-1}-1 < x'(v-1)^{2-k}(v^{u-1}-1)$. Thus, $(v-1)^{k-2} < x'$ and so $k = 2 = x'$. Since $e_1 = 1$, it follows that $e_2 = u-2$ and (6.32) implies that $(v^{u-1}-1)|2(v-1)(v^{u-2}-1)$. If $v^{u-1}-1 < 2(v-1)(v^{u-2}-1)$, then $v^{u-1}-1 \leqslant (v-1)(v^{u-2}-1)$, which is false. So $v^{u-1}-1 = 2(v-1)(v^{u-2}-1)$. Thus, $v^{u-2}(2-v) = 3-2v$, which implies that $3-2v \geqslant 2-v$. However, this forces $v \leqslant 1$, a contradiction.

We now deal with the case where $k = 1$. Since $(v^{u-1}-1)/(x'(v-1))$ divides $v^{e_1}-1$ and $v^{u-1}-1$, it must also divide $\gcd(v^{e_1}-1, v^{u-1}-1) = v^{\gcd(u-1,e_1)}-1$. If $e_1 = u-1$, then (6.31) says that $u-1 \leqslant u-(u-1)r^{s-w-1}$, forcing $u \leqslant 2$, which is false. So $e_1 \neq u-1$ and thus $\gcd(u-1, e_1) \leqslant (u-1)/2$. Then (6.32) says that $v^{u-1}-1 \leqslant x'(v-1)(v^{(u-1)/2}-1) \leqslant x'(v^{(u+1)/2}-1)$, which implies that

$$v^{(u+1)/2}(v^{(u-3)/2} - x') \leqslant 1 - x'. \tag{6.34}$$

If $x' = 1$, then (6.34) implies that $v^{(u-3)/2} \leqslant 1$, so $u = 3$. If $x' > 1$, then (6.34) implies that $v^{(u-3)/2} < x' \leqslant 2\log_r v$, which also implies that $u = 3$. Thus, we may assume that $u = 3$. Since $e_1 \neq u-1$, it follows that $e_1 = 1$. So (6.31) implies that $r^{s-w-1} \leqslant 2$.

First consider when $r \geqslant 3$. Since $r^{s-w-1} \leqslant 2$, Fact 1 and Fact 2 together imply that $x' = 2$. So (6.32) implies that $(v+1)/2 = (v^{u-1}-1)/(2(v-1))$ divides $v-1$. Since $(v+1)/2 > (v-1)/2$, it follows that $(v+1)/2 = v-1$. Hence, $v = 3$ and so $(u,v) = (3,3)$, a contradiction.

Now suppose that $r = 2$. Since $2^{s-w-1} \leqslant 2$, Fact 1, Fact 3, and Fact 4 together imply that $x' = 1$. Hence, (6.32) implies that $v+1 = (v^{u-1}-1)/(v-1)$ divides $v-1$, which is impossible. This completes the proof of the fact that no element in $\mathrm{GL}_u(v)$ has order $(q-1)/(2x)$.

We now prove that there is no element in $\Gamma\mathrm{L}_u(v)$ of order $(q-1)/2$. Recall that $\Gamma\mathrm{L}_u(v)$ is the semidirect product $\mathrm{GL}_u(v) \rtimes \mathrm{Aut}(\mathbb{F}_v)$ where an element $\theta \in \mathrm{Aut}(\mathbb{F}_v)$ acts entry-wise on an element $A \in \mathrm{GL}_u(v)$. Suppose, for a contradiction, that there is some element $A\theta \in \Gamma\mathrm{L}_u(v)$ of order $(q-1)/2$. Let x be the order of $\theta \in \mathrm{Aut}(\mathbb{F}_v)$ and note that $x|s$. Then $(A\theta)^x = B$ for some $B \in \mathrm{GL}_u(v)$. Therefore, we can write $(q-1)/2 = yx$ where y divides the order of B. Let b denote the order of B so that $b = yb'$ for some positive integer b'. Then $B^{b'} \in \mathrm{GL}_u(v)$ has order $y = (q-1)/(2x)$, which is a contradiction.

We now prove that there is no element in $\mathrm{P\Gamma L}_u(v)$ of order $(q-1)/2$. Let I denote the $u \times u$ identity matrix in $\mathrm{GL}_u(v)$. Let $Z = \{kI : k \in \mathbb{F}_v\}$ be the centre of $\mathrm{GL}_u(v)$. Recall that $\mathrm{P\Gamma L}_u(v)$ is the quotient group $\Gamma\mathrm{L}_u(v)/Z$. For an element $A\theta \in \Gamma\mathrm{L}_u(v)$, we will denote by $\overline{A\theta}$ the image of $A\theta$ under the projection map from $\Gamma\mathrm{L}_u(v)$ to $\mathrm{P\Gamma L}_u(v)$. Suppose, for a contradiction, that there is some element $\overline{A\theta} \in \mathrm{P\Gamma L}_u(v)$ of order $(q-1)/2$. Then there is some $k \in \mathbb{F}_v$ such that $(A\theta)^{(q-1)/2} = kI$. Let the order of k in $\mathbb{F}_v$ be y. Then the order of $(A\theta)^y$ in $\Gamma\mathrm{L}_u(v)$ is $(q-1)/2$, which is a contradiction. □

Let $i \in \{1,2,3\}$ and suppose that $\mathrm{Atp}_i(\Omega)$ satisfies Theorem 6.5.5(*iii*). So, up to permutation isomorphism, $\mathrm{PGL}_u(v) \leqslant \mathrm{Atp}_i(\Omega) \leqslant \mathrm{P\Gamma L}_u(v)$ for some prime power v and positive integer

u such that $q = (v^u - 1)/(v - 1)$ and q is prime. Lemma 6.5.7 and Lemma 6.5.9 together imply that $v = 2$. To reach a contradiction, we first prove that $\mathrm{Atp}_i(\mathfrak{Q})$ must contain an element that is the product of $(q+1)/4$ disjoint transpositions. We then use some results from §6.2 about the structure of quadratic Latin squares to prove that this is impossible. Note that $2^u - 1 \equiv 3 \bmod 4$ for any positive integer $u \geqslant 2$.

Lemma 6.5.10. *Suppose that q is prime and that there is an integer $u \geqslant 2$ such that $q = 2^u - 1$. Let $G \leqslant \mathrm{Sym}(\mathbb{F}_q)$ be permutation isomorphic to $\mathrm{PGL}_u(2)$. There is some $g \in G$ that is the product of $(q+1)/4$ disjoint transpositions.*

Proof. Identify the action of $\mathrm{PGL}_u(2)$ on the points of $\mathbf{P}^{u-1}(2)$ with $\mathrm{GL}_u(2)$ acting naturally on the set of non-zero elements of $\mathbb{F}_2^u$. Let $A \in \mathrm{GL}_u(2)$ be defined by

$$A_{i,j} = \begin{cases} 1 & \text{if } i = j \text{ or both } i = u \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Let $x = (x_1, x_2, \ldots, x_u)$ be a non-zero element of $\mathbb{F}_2^u$. If $x_1 = 0$, then $Ax = x$ and there are $2^{u-1} - 1$ possibilities for x. If $x_1 = 1$, then $A^2x = x \neq Ax$ and there are $2^{u-1} = (q+1)/2$ possibilities for x. The lemma follows. □

Lemma 6.5.11. *Suppose that $q \equiv 3 \bmod 4$ and q is prime. For each $i \in \{1, 2, 3\}$, there is no permutation in $\mathrm{Atp}_i(\mathfrak{Q})$ that is the product of $(q+1)/4$ disjoint transpositions.*

Proof. By taking parastrophes, it suffices to prove that $\mathrm{Atp}_1(\mathfrak{Q})$ has no element that is the product of $(q+1)/4$ disjoint transpositions. Suppose, for a contradiction, that $\alpha \in \mathrm{Atp}_1(\mathfrak{Q})$ is the product of $(q+1)/4$ disjoint transpositions. Then α has $(q-1)/2$ fixed points. Let $\beta \in \mathrm{Atp}_2(\mathfrak{Q})$ and $\gamma \in \mathrm{Atp}_3(\mathfrak{Q})$ be such that $(\alpha, \beta, \gamma) \in \mathrm{Atp}(\mathfrak{Q})$. Using [92, Lemma 8], we deduce that the order of β is 2 and the order of γ is 2. Since q is odd, it follows that β and γ must have fixed points. Then [88, Theorem 1] implies that β and γ have exactly $(q-1)/2$ fixed points.

Let R, C, and S be the set of elements of $\mathbb{F}_q$ fixed by α, β, and γ, respectively. Also let R', C', and S' be the complements of R, C, and S in $\mathbb{F}_q$, respectively. Note that if $x \in R$ and $y \in C$, then $x * y \in S$. Fix $x' \in R'$. We claim that there is a unique $y' \in C'$ such that $x' * y' \in S'$. For any $y \in C$, it is true that $x' * y \in S'$, since all symbols $x * y$ with $x \in R$ lie in S. There are $(q+1)/2$ symbols in S' and there are $(q-1)/2$ elements $y \in C$ such that $x' * y \in S'$. Hence, there is a unique $y' \in C'$ such that $x' * y' \in S'$, as claimed. Let $y' \in C'$ be such that $\{x' * y', x' * \beta(y')\} \subseteq S$. Note that there are at least $(q-3)/2$ choices for y'. Since $(\alpha, \beta, \gamma) \in \mathrm{Atp}(\mathfrak{Q})$ and $\{x' * y', x' * \beta(y')\} \subseteq S$, it follows that $x' * y' = \alpha(x') * \beta(y')$ and $x' * \beta(y') = \alpha(x') * \beta^2(y') = \alpha(x') * y'$. Equivalently, the row permutation $r_{x',\alpha(x')}$ of $\mathcal{L}$ contains the transposition $(x' * y', x' * \beta(y'))$. Since there are at least $(q-3)/2$ choices for y', it follows that $r_{x',\alpha(x')}$ contains at least $(q-3)/4$ transpositions. Recall that $b \notin \{-a, 2-a, a/(2a-1)\}$ since $q \equiv 3 \bmod 4$. Thus, Lemma 6.2.12 combined with Lemma 6.1.1 implies that $r_{x,\alpha(x)}$ contains at most two transpositions, which is a contradiction, since $q > 23$. □

By combining Theorem 6.5.5, Lemma 6.5.6, Lemma 6.5.7, Lemma 6.5.9, Lemma 6.5.10, and Lemma 6.5.11, we obtain the following result.

Corollary 6.5.12. *Let $i \in \{1,2,3\}$. If $\mathrm{Atp}_i(\mathcal{Q})$ is 2-transitive, then up to permutation isomorphism, $\mathrm{Atp}_i(\mathcal{Q}) \leqslant \mathrm{AGL}_d(p)$.*

We are now ready to prove Lemma 6.5.4. Let G and H be groups with $H \leqslant G \leqslant \mathrm{Sym}(\mathbb{F}_q)$ and let $g \in G$. We denote by H^g the subgroup $\{g^{-1} \circ h \circ g : h \in H\} \leqslant G$.

Proof of Lemma 6.5.4. Suppose that $\mathrm{Atp}_i(\mathcal{Q})$ is 2-transitive. From Corollary 6.5.12, there is some $G \leqslant \mathrm{AGL}_d(p)$ and some $\delta \in \mathrm{Sym}(\mathbb{F}_q)$ such that $\mathrm{Atp}_i(\mathcal{Q}) = G^\delta$. Let $\mathcal{T} = \mathcal{T}_q$. Since $\mathcal{T} \leqslant \mathrm{Atp}_i(\mathcal{Q})$, it follows that $\mathcal{T}^{\delta^{-1}} \leqslant G$. There is some $u \in \mathbb{F}_q^*$ such that $\kappa_u \in \mathcal{T} \cap \mathcal{T}^{\delta^{-1}} \leqslant G$ (see, e.g., [24, Lemma 4]). Since $\kappa_u \in \mathcal{T}^{\delta^{-1}}$, it follows that $\delta^{-1} \circ \kappa_u \circ \delta = \kappa_v$ for some $v \in \mathbb{F}_q^*$. Since $\mathcal{T}$ is normal in $\mathrm{AGL}_d(p)$, it follows that $\mathcal{T} \cap G$ is normal in G. Hence, $(\mathcal{T} \cap G)^\delta$ is normal in $\mathrm{Atp}_i(\mathcal{Q})$. Note that $\kappa_v \in (\mathcal{T} \cap G)^\delta$, since $\kappa_u \in \mathcal{T} \cap G$. Since $(\mathcal{T} \cap G)^\delta$ is normal in $\mathrm{Atp}_i(\mathcal{Q})$ and $\{\lambda_c : c \in \mathcal{R}_q\} \leqslant \mathrm{Atp}_i(\mathcal{Q})$, it follows that $\kappa_{cv} = \lambda_c \circ \kappa_v \circ \lambda_{c^{-1}} \in (\mathcal{T} \cap G)^\delta$ for all $c \in \mathcal{R}_q$. Therefore, $|\mathcal{T} \cap (\mathcal{T} \cap G)^\delta| \geqslant (q+1)/2 > |\mathcal{T}|/2$, hence $\mathcal{T} = (\mathcal{T} \cap G)^\delta$ and so $\mathcal{T}^\delta = \mathcal{T}$. Therefore, δ is in the normaliser of $\mathcal{T}$ in $\mathrm{Sym}(\mathbb{F}_q)$, which is $\mathrm{AGL}_d(p)$. Thus, $\mathrm{Atp}_i(\mathcal{Q}) = G^\delta \leqslant \mathrm{AGL}_d(p)$. □

6.5.4 Proof of Theorem 6.0.12 and Theorem 6.0.11

In this subsection, we prove our main results regarding isotopisms of quadratic quasigroups.

Proof of Theorem 6.0.12. As mentioned at the beginning of §6.5.1, the theorem is easy to verify using a computer if $q < 23$. If $a \neq b$ and $q \geqslant 23$, then the result follows by combining Lemma 6.5.1, Lemma 6.5.2, and Lemma 6.5.4. It remains to prove the theorem in the case where $a = b$.

The autotopism group of an abelian group $(G, +)$ is isomorphic to the semidirect product $G^2 \rtimes \mathrm{Aut}(G)$ with multiplication defined by $((g_1, g_2), \theta) \cdot ((h_1, h_2), \phi) = ((\phi^{-1}(g_1) + h_1, \phi^{-1}(g_2) + h_2), \theta \circ \phi)$. Furthermore, every autotopism of G is of the form (α, β, γ) where $\alpha(x) = \theta(x + u)$, $\beta(x) = \theta(x + v)$, and $\gamma(x) = \theta(x + u + v)$ for some $\{u, v\} \subseteq G$ and $\theta \in \mathrm{Aut}(G)$ [16]. The result now follows, since $(\lambda_{1-a}, \lambda_a, \mathrm{Id})$ is an isotopism from $\mathcal{Q}_{a,a}$ to $(\mathbb{F}_q, +)$ and the automorphism group of $(\mathbb{F}_q, +)$ is $\mathrm{GL}_d(p)$. □

Proof of Theorem 6.0.11. Let $\mathcal{Q} = \mathcal{Q}_{a,b}$ and $\mathcal{Q}' = \mathcal{Q}_{a',b'}$ be quadratic quasigroups of order q. First, suppose that $a = b$. It is known [43] that $\mathcal{Q}$ is isotopic to the group $(\mathbb{F}_q, +)$ and if $a' \neq b'$, then $\mathcal{Q}'$ is not isotopic to any group. Therefore, $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic if and only if $a' = b'$.

Now assume that $a \neq b$ and $a' \neq b'$. By Theorem 6.0.9, if $\{a, b\} = \{\theta(a'), \theta(b')\}$ for some $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, then $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic. Now assume that $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic and let (α, β, γ) be an isotopism from $\mathcal{Q}$ to $\mathcal{Q}'$. Then $(\alpha^{-1} \circ \theta \circ \alpha, \beta^{-1} \circ \theta \circ \beta, \gamma^{-1} \circ \theta \circ \gamma) \in \mathrm{Atp}(\mathcal{Q})$ for any $\theta \in \mathrm{Aut}(\mathcal{Q}')$. Theorem 6.0.12 implies that $\alpha^{-1} \circ \theta \circ \alpha = \beta^{-1} \circ \theta \circ \beta$ and so $\alpha \circ \beta^{-1}$ centralises θ. Since $\theta \in \mathrm{Aut}(\mathcal{Q}')$ was arbitrary, $\alpha \circ \beta^{-1}$ centralises $\mathrm{Aut}(\mathcal{Q}')$. In particular, $\alpha \circ \beta^{-1}$ centralises $\mathcal{T}_q$ and so must be an element of $\mathcal{T}_q$. But $\alpha \circ \beta^{-1}$ also centralises the permutation λ_c where c is some fixed element of $\mathcal{R}_q \setminus \{1\}$. The only element of $\mathcal{T}_q$ that can centralise this permutation is Id. Therefore, $\alpha = \beta$. Similar arguments show that $\beta = \gamma$ also. Hence, $\mathcal{Q}$ and $\mathcal{Q}'$ are isomorphic and the theorem follows from Theorem 6.0.9. □

Chapter 7

Future work

In this chapter, we discuss a number of fascinating open problems regarding Latin subrectangles. Of course, there are plenteous problems regarding subrectangles that have not been touched in this thesis. For examples, see the papers [15, 18, 19, 35, 59, 62, 68, 69] or the survey [32, Chapter 4]. In this chapter, we will focus on open problems that are directly related to work done in this thesis.

Throughout this chapter, let n be a positive integer. Let k and m be positive integer functions of n with $k \leqslant n$ and $m \leqslant \min\{k, n/2\}$. Unless otherwise stated, all asymptotics in this chapter are as $n \to \infty$. In Chapter 3, we proved that $\mathbb{E}_m(k,n) = O(n^{-2})$ whenever $m \geqslant 4$. Although this is enough to resolve Conjecture 2.2.8(i), we expect that $\mathbb{E}_m(k,n)$ tends to 0 much quicker than n^{-2} does. From [112], we know that the number of Latin squares of order m is

$$\exp\left(-2m^2 + m^2 \log m + O\left(m \log^2 m\right)\right).$$

Also note that $\binom{k}{m} = \exp(m \log k - m \log m + O(m))$ and $\binom{n}{m} = \exp(m \log n - m \log m + O(m))$. Thus, if Conjecture 2.2.9 is true and $m = o(n)$, then

$$\begin{aligned}
\mathbb{E}_m(k,n) &= \binom{k}{m}\binom{n}{m}^2 \exp\left(-2m^2 + m^2 \log m + O\left(m \log^2 m\right)\right)\left(\frac{1+o(1)}{n}\right)^{m^2} \\
&= \exp\Big(m \log k + 2m \log n - 3m \log m + O(m) - 2m^2 + m^2 \log m + O\left(m \log^2 m\right) \\
&\quad + m^2 \log(1+o(1)) - m^2 \log n\Big) \\
&= \left(\frac{m}{n}\right)^{m^2} \exp\left(m \log k + 2m \log n - \Omega\left(m^2\right)\right),
\end{aligned}$$

which goes to 0 quicker than n^{-2} does if $m \geqslant 4$. Thus, a direction for future research is to give better asymptotics for $\mathbb{E}_m(k,n)$ when $m \geqslant 4$.

Conjecture 2.2.8(ii) and Conjecture 2.2.4(ii) both remain unresolved. Hence, the resolution of these conjectures is an obvious direction for future research. Another interesting direction is to prove the following weak version of Conjecture 2.2.4(ii): There is a constant $c > 0$ such that $\mathbb{E}_3(n,n) \geqslant c - o(1)$. Theorem 3.0.4 implies that $\mathbb{E}_3(n,n) \leqslant 2/3 + o(1)$. Thus, if we could prove that $\mathbb{E}_3(n,n) \geqslant c - o(1)$ for some constant $c > 0$, then it would follow that $\mathbb{E}_3(n,n)$ is asymptotically bounded between positive constants. This is not true if we replace 3 by any

other meaningful integer m, since $\mathbb{E}_2(n,n)$ is unbounded and $\mathbb{E}_m(n,n) = o(1)$ if $m \geqslant 4$.

Most of the open problems that we have discussed so far are implied by Conjecture 2.2.9. Thus, attempting to resolve Conjecture 2.2.9 is a very worthwhile endeavour. Due to the dependence of ϵ on δ in Conjecture 2.2.9 being unclear, the conjecture is not useful for predicting the occurrence of substructures in $k \times n$ Latin rectangles that have $\Theta(n)$ entries in a row, column, or with a particular symbol. Indeed, Conjecture 2.2.9 is false if we drop the condition that P is ϵ-dense [39]. It would be valuable to formulate a conjecture that predicts the probability of a random $k \times n$ Latin rectangle containing any ϵ-dense $k \times n$ partial Latin rectangle where $\epsilon > 0$ is an absolute constant. In particular, motivated by subsquares in random Latin rectangles, it would be of interest to formulate such a conjecture with $\epsilon = 1/2$.

In Chapter 4, we resolved Conjecture 2.2.13 by constructing N_∞ Latin squares of orders of the form $2^a 3^b$ where $a \geqslant 1$ and $b \geqslant 0$ are integers. Our construction used corrupting pairs of orders 8 and 9. It seems likely that our method could be generalised to construct N_∞ squares of other orders. There are no corrupting pairs of order less than 7, but they probably exist for all orders 7 and above [117]. If we have a corrupting pair (A, B) of order $\zeta \geqslant 8$ that satisfies Properties 1–7 from §4.2, then the same arguments as used in Chapter 4 can be used to prove that an N_∞ Latin square of order $\zeta\mu$ exists whenever there is an N_∞ Latin square M of order μ and integer $s \in [\mu - 1]$ such that (M, s) satisfies Conditions (i)–(iii) in §4.2. The condition that $\mu \geqslant 8$ is needed for some of our arguments to be directly applied, but we do not believe that there is an intrinsic obstacle to building N_∞ Latin squares using the construction from Chapter 4 with a corrupting pair of order 7.

Another direction for future research is to provide asymptotic estimates for the number of N_∞ Latin squares, along the lines of the asymptotic estimates for the number of N_2 Latin squares given by Theorem 2.2.12. In Chapter 3, we resolved Conjecture 2.2.4(i), proving that with probability $1 - o(1)$, a random Latin square of order n has no proper subsquare of order 4 or more. Conjecture 2.2.4(ii) suggests that the proportion of Latin squares of order n that contain a subsquare of order 3 is asymptotically at most 1/18. Thus, we propose the following new conjecture.

Conjecture 7.0.1. *Let $\mathcal{N}_\infty(n)$ and $\mathcal{N}_2(n)$ denote the number of N_∞ and N_2 Latin squares of order n, respectively. Then*

$$\frac{\mathcal{N}_\infty(n)}{\mathcal{N}_2(n)} = \Omega(1).$$

In Chapter 5, we enumerated the perfect 1-factorisations of $K_{11,11}$ and the row-Hamiltonian Latin squares of order 11. The complete enumeration of the perfect 1-factorisations of $K_{13,13}$ or the row-Hamiltonian Latin squares of order 13 seems, at the moment, to be an unrealistic goal. A more realistic, and still very worthwhile, goal would be to enumerate the atomic Latin squares of order 13.

In Chapter 6, we investigated many problems regarding subrectangles of quadratic Latin squares. The most tantalising open problem in this area is the following: When is a quadratic Latin square row-Hamiltonian? We know [5] that there are infinitely many row-Hamiltonian quadratic Latin squares. However, we also know, from Theorem 6.0.4, that for each odd prime p, there are only finitely many integers d for which there might exist a row-Hamiltonian quadratic

Latin square of order p^d. Let p be an odd prime. It would be a worthwhile goal to find sufficient conditions for a quadratic Latin square of order p^d to be row-Hamiltonian for 'small' values of d. This may allow progress to be made on Conjecture 2.3.21. If we restrict our attention to involutory quadratic Latin squares, then progress could be made on Conjecture 2.3.12.

Allsop and Wanless [5] conjectured, and gave some numerical evidence to suggest, that there are $\Theta(p)$ row-Hamiltonian quadratic Latin squares of prime order p as $p \to \infty$. If this conjecture is true, then Theorem 2.3.5 and Theorem 6.0.11 would together imply that the number of isomorphism classes of perfect 1-factorisations of $K_{p,p}$ with p prime goes to ∞ as $p \to \infty$. Allsop and Wanless [5] also gave numerical evidence to suggest that the number of involutory, row-Hamiltonian quadratic Latin squares of prime order $p \equiv 3 \bmod 4$ goes to ∞ as $p \to \infty$. If this is true, then Theorem 2.3.5 and Theorem 6.0.11 would together imply that the number of isomorphism classes of perfect 1-factorisations of K_{p+1} tends to ∞ as $p \to \infty$, which would partially resolve a conjecture of Rosa [104].

Let p be prime, let d be a positive integer, and let $q = p^d$. Given Lemma 6.1.1, it would be worthwhile to investigate whether quadratic Latin squares can be used to improve Theorem 2.3.27 or even help resolve Conjecture 2.3.26. Theorem 6.0.4 tells us that a quadratic Latin square $\mathcal{L}[a, b]$ of order q could only be useful for this purpose if d is 'small' or $\{a, b\} \subseteq \mathbb{F}_p \cap \mathcal{N}_q$. Unfortunately, computational evidence seems to suggest that Latin squares $\mathcal{L}[a, b]$ of order q with $\{a, b\} \subseteq \mathbb{F}_p \cap \mathcal{N}_q$ contain some long row cycles.

Recall the definition of a cyclotomic orthomorphism from §2.4. Also recall that a quadratic quasigroup is a quasigroup that is generated by a cyclotomic orthomorphism of index 2. If φ is a cyclotomic orthomorphism of index u and φ is not cyclotomic of any index $u' < u$, then φ has *least index* u. The quadratic quasigroups of the form $\mathcal{Q}_{a,a}$ are the quasigroups generated by a cyclotomic orthomorphism of index 1. Theorem 6.0.12 implies the following statement.

$$\begin{aligned}&\text{If } \mathcal{Q} \text{ is a quasigroup generated by a cyclotomic orthomorphism}\\&\text{of least index 2, then every autotopism of } \mathcal{Q} \text{ is an automorphism.}\end{aligned} \tag{7.1}$$

Theorem 6.0.11 implies the following statement.

$$\begin{aligned}&\text{If } \mathcal{Q} \text{ and } \mathcal{Q}' \text{ are isotopic quasigroups generated by cyclotomic}\\&\text{orthomorphisms of least index 2, then } \mathcal{Q} \text{ and } \mathcal{Q}' \text{ are isomorphic.}\end{aligned} \tag{7.2}$$

It would be interesting to determine for which integers u (7.1) is true if we replace 2 by u and for which integers u (7.2) is true if we replace 2 by u. Neither (7.1) nor (7.2) are true if we replace 2 by 1. Let $\mathcal{Q}$ and $\mathcal{Q}'$ be quasigroups of order q that are generated by cyclotomic orthomorphisms of least index 1. Theorem 6.0.10 and Theorem 6.0.12 together imply that there are autotopisms of $\mathcal{Q}$ that are not automorphisms of $\mathcal{Q}$. Theorem 6.0.9 and Theorem 6.0.11 together imply that $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic, but may not be isomorphic.

Identify $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 - x - 1)$. Let $\mathcal{Q}$ be the quasigroup generated by the cyclotomic orthomorphism $\varphi_x[-1, x + 1, -x + 1, x - 1]$ and let $\mathcal{Q}'$ be the quasigroup generated by the cyclotomic orthomorphism $\varphi_x[x, x + 1, -x - 1, -x + 1]$. Then $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic, but not isomorphic. Identify $\mathbb{F}_{25} = \mathbb{F}_5[x]/(x^2 - x + 2)$, let $\mathcal{Q}$ be the quasigroup generated by $\varphi_x[2, -1, -x-2, x-1, 2x-2, 2x-2]$, and let $\mathcal{Q}'$ be the quasigroup generated by $\varphi_x[2, -2, 2x, 1-x, x, 2 - 2x]$. Then $\mathcal{Q}$ and $\mathcal{Q}'$ are isotopic, but not isomorphic. Therefore, (7.2) is false if we replace 2 by 4 or 6. For $u \in \{3, 5\}$, there are no two quasigroups $\mathcal{Q}$ and $\mathcal{Q}'$ of order less than

50 that are generated by cyclotomic orthomorphisms of least index u and that are isotopic but not isomorphic. For $u \in \{3, 4, 5\}$, there is no quasigroup of order less than 50 generated by a cyclotomic orthomorphism of least index u that has an autotopism that is not an automorphism. The only quasigroup of order less than 50 generated by a cyclotomic orthomorphism of least index 6 that has an autotopism that is not an automorphism is the quasigroup $\mathcal{Q}$ of order 7 generated by $\varphi_3[3, 3, 6, 3, 2, 4]$. Explicitly, $\mathrm{Aut}(\mathcal{Q}) \cong \mathbb{Z}_7$ and $\mathrm{Atp}(\mathcal{Q}) \cong \mathrm{PGL}_3(2)$. However, we note that a cyclotomic orthomorphism of index $q-1$ over $\mathbb{F}_q$ is, in some sense, a degenerate cyclotomic orthomorphism, since every orthomorphism of $\mathbb{F}_q$ that fixes 0 is cyclotomic of index $q-1$.

The only known quasigroups that violate (7.2) when 2 is replaced by some other index are not of prime order. Thus, it would be interesting to determine for which integers u (7.2) is true when replacing 2 by u if we impose that the orders of $\mathcal{Q}$ and $\mathcal{Q}'$ are prime. It would also be interesting to determine for which integers u (7.1) is true when replacing 2 by u if we impose that the order of $\mathcal{Q}$ is prime.

Glossary of notation

This glossary contains a list of mathematical symbols that are used in this thesis, along with a brief definition of each symbol and the page number that it was defined on. The criteria for a symbol to be included in this glossary is:

- The symbol is non-standard,
- The symbol is used for a singular purpose throughout this thesis, and
- The symbol is used in places other than the immediate vicinity of its definition.

Symbol	pp.	Meaning
$[m]$	4	$\{1, 2, \ldots, m\}$
$M[I, J]$	5	The submatrix of M induced by the rows in I and the columns in J
$\mathrm{Sym}(X)$	5	The group of permutations of the set X
Id_X / Id	5	The identity permutation of the set X
$\mathrm{Aut}(L)$ / $\mathrm{Aut}(Q)$	6	The automorphism group of the Latin square L/quasigroup Q
$\mathrm{Atp}(L)$ / $\mathrm{Atp}(Q)$	6	The autotopism group of the Latin square L/quasigroup Q
$\mathrm{Apar}(L)$ / $\mathrm{Apar}(Q)$	6	The autoparatopism group of the Latin square L/quasigroup Q
$f = O(g)$	7	There exists a positive constant C such that $\lvert f(n)\rvert \leqslant C\lvert g(n)\rvert$ for all sufficiently large integers n
$f = \Omega(g)$	7	There exists a positive constant K such that $\lvert f(n)\rvert \geqslant K\lvert g(n)\rvert$ for all sufficiently large integers n
$f = \Theta(g)$	7	$f = O(g)$ and $f = \Omega(g)$
$f = o(g)$	7	$f(n)/g(n) \to 0$ as $n \to \infty$
$\Pr(X)$	7	The probability of event X occurring in the discrete uniform distribution
$\mathbb{E}_m(k, n)$	7	The expected number of subsquares of order m in a uniformly random $k \times n$ Latin rectangle
$L \supseteq P$	7	The Latin rectangle L contains each entry of the partial Latin rectangle P
N_2	10	Describes a Latin square devoid of intercalates
N_∞	10	Describes a Latin square devoid of proper subsquares
$\mathrm{Aut}(\mathcal{F})$	11	The automorphism group of the 1-factorisation $\mathcal{F}$
$[f_1, f_2, ..., f_a]$	12	An ordered 1-factorisation with 1-factors $f_1, f_2, \ldots, f_a$

$\mathcal{F}\langle\theta,\psi\rangle$	12	The ordered 1-factorisation obtained from $\mathcal{F}$ by applying ψ to its 1-factors and θ to the vertices of the underlying graph
$\mathrm{OAut}(\mathcal{F})$	12	The group of ordered automorphisms of the ordered 1-factorisation $\mathcal{F}$
$\mathscr{F}(L)$	13	The ordered 1-factorisation of $K_{n,n}$ obtained from the Latin square L
$\mathscr{L}(\mathcal{F})$	13	The Latin square obtained from the ordered 1-factorisation $\mathcal{F}$ of $K_{n,n}$
$\Gamma[M]$	14	The subgraph of Γ with vertex set $V(\Gamma)$ and edge set M
GK_{p+1}	15	The perfect 1-factorisation of K_{p+1} due to Kotzig
GA_{2p}	15	The perfect 1-factorisation of K_{2p} due to Kotzig and Anderson
GB_{p+1}	15	The perfect 1-factorisation of K_{p+1} due to Bryant, Maenhaut, and Wanless
$\mathcal{K}(\mathcal{F},v)$	16	The ordered 1-factorisation of $K_{n,n}$ obtained from the rooted 1-factorisation $(\mathcal{F},v)$ of K_{n+1}
$\mathscr{L}(\mathcal{F},v)$	18	$\mathscr{L}(\mathcal{K}(\mathcal{F},v))$
$\mathscr{G}(L)$	18	The ordered 1-factorisation of K_{n+1} obtained from the Latin square L
$\nu(L)$	23	The number of conjugates of L that are row-Hamiltonian
$\mathcal{R}_q$	25	The quadratic residues in $\mathbb{F}_q^*$
$\mathcal{N}_q$	25	The quadratic non-residues in $\mathbb{F}_q^*$
$\varphi_\iota[a_0,a_1,\ldots,a_{u-1}]$	25	A cyclotomic map of index u
$\varphi[a,b]$	25	A quadratic map
$\mathcal{L}[a,b]$	26	The quadratic Latin square generated by the quadratic orthomorphism $\varphi[a,b]$
$\mathcal{Q}_{a,b}$	26	The quadratic quasigroup generated by the quadratic orthomorphism $\varphi[a,b]$
$*_{a,b}$	26	The binary operation that defines the quadratic quasigroup $\mathcal{Q}_{a,b}$
$\rho(i,j,c)$	29	The row cycle of a Latin rectangle that hits rows i and j and column c
$\sigma(i,j,r)$	30	The column cycle or incomplete column cycle of a Latin rectangle that hits columns i and j and row r
$\tau_{i,j}$	30	The row permutation of a Latin rectangle mapping row i to row j
$\xi_{i,j}$	30	The partial permutation mapping column i of a Latin rectangle to column j
T_i	31	The first i cells of the submatrix of a Latin rectangle induced by the rows and columns in $[m]$ in the natural ordering
t_i	31	The cell in $T_i \setminus T_{i-1}$
Δ_i	31	The set of Latin rectangles for which every cell in T_i contains a symbol in $[m]$

$\Upsilon(T)$	33	The set of partial Latin rectangles whose non-empty cells are T and every non-empty cell contains a symbol in $[m]$
$\Upsilon^*(T)$	33	$\cup_{T' \subseteq T} \Upsilon(T')$
$\sigma \hookrightarrow L_{i,j}$	45	The Latin square obtained from L by replacing the entry $(i, j, L_{i,j})$ with (i, j, σ)
$\prec_1$	46	The order on $[n] \times [m]$ defined by $(a, b) \prec (c, d)$ if $a < c$ or both $a = c$ and $b < d$
$L \times M$	46	The direct product of the Latin squares L and M
$\mathscr{J}_i$	46	$\{(i, \ell) : \ell \in [m]\}$
$\mathscr{K}_i$	46	$\{(\ell, i) : \ell \in [n]\}$
Φ_1	46	The projection of $[n] \times [m]$ onto the first coordinate
Φ_2	47	The projection of $[n] \times [m]$ onto the second coordinate
$(A, B) *_s M$	47	The corrupted product of (A, B) and M of shift s
$\mathbb{T}_M$	48	The principal M-block of a corrupted product $(A, B) *_s M$, which is a subsquare
$\eta(i, j, x)$	50	A collection of entries of a Latin square that can be 'switched' on to produce a new Latin square
A^8 / B^8	54	Latin squares of order 8 that together form a corrupting pair which we use to build N_∞ squares
A^9 / B^9	54	Latin squares of order 9 that together form a corrupting pair which we use to build N_∞ squares
$\mathscr{d}_1/\mathscr{d}_2/\mathscr{d}_3$	55	$A_{1,1}/A_{1,2}/A_{1,3}$ where $A \in \{A^8, A^9\}$
$\mathcal{X}$	55	The set of pairs (M, s) satisfying Conditions (i)–(iii) in §4.2
$N(\mathcal{X})$	56	The set of integers μ for which there is a member (M, s) of $\mathcal{X}$ where M is of order μ
$\mathbb{Q}$	59	The Latin square obtained from a corrupted product $(A, B) *_s M$ by switching on a row cycle of length 3 where $A = A^\zeta$ and $B = B^\zeta$ for some $\zeta \in \{8, 9\}$ and $(M, s) \in \mathcal{X}$
$\mathbb{Q}_1$	59	$\mathbb{Q}$ relabelled using $\prec_1$
$\mathbb{Q}'\langle\epsilon, \delta\rangle/\mathbb{Q}'$	59	$(\mathbb{Q}_{\epsilon,\delta} + (1, 0)) \hookrightarrow \mathbb{Q}_{\epsilon,\delta}$
$\mathcal{P} \Vert f$	69	The ordered partial 1-factorisation obtained from $\mathcal{P}$ by appending f
$\mathcal{P}^i$	69	The ordered partial 1-factorisation consisting of the first i 1-factors in $\mathcal{P}$
$\mathscr{L}^*(\mathcal{F}, v)$	77	An alternative Latin square obtained from the rooted 1-factorisation $(\mathcal{F}, v)$ of K_{n+1}
$\mathrm{Alt}(X)$	82	The group of even permutations of a set X
κ_c	82	The map $x \mapsto x + c$
λ_c	82	The map $x \mapsto cx$
$\mathcal{T}_q$	82	$\{\kappa_c : c \in \mathbb{F}_q\}$
χ	83	The extended quadratic character on $\mathbb{F}_q$
$\omega[a, b]$	84	The row permutation $\tau_{0,1}$ of the quadratic Latin square $\mathcal{L}[a, b]$

Λ	84	The set of row permutations $\tau_{0,1}$ of quadratic Latin squares
ω_0	84	The cycle of ω containing 0
ω_a	84	The cycle of $\omega = \omega[a,b]$ containing a
z^i	85	The sequence obtained from z by a cyclic rotation of i positions
e^+	85	Measures the number of 1's in an even indexed position in a $(-1,1)$-sequence
o^+	85	Measures the number of 1's in an odd indexed position in a $(-1,1)$-sequence
e^-	85	Measures the number of (-1)'s in an even indexed position in a $(-1,1)$-sequence
o^-	85	Measures the number of (-1)'s in an odd indexed position in a $(-1,1)$-sequence
u^+	85	$o^+ - e^+$
u^-	85	$o^- - e^-$
o^+	85	$o^+ - e^-$
o^-	85	$o^- - e^+$
$X_{c,\omega}$	89	The set of sequences $z \in \{-1,1\}^{2c}$ that are not even periodic such that (z,ω) is of Type One
$\sim$	89	The relation on $\{-1,1\}^{2c}$ defined by $z \sim z'$ if $z' = z^{2i}$ for some $i \in \{0,1,\ldots,c-1\}$
Λ_m	89	The permutations $\omega[a,b] \in \Lambda$ such that ab^{-1} is not a k-th root of unity for any $k \in [m]$
$X_{c,1}$	90	The set $X_{c,\omega}$ for a permutation $\omega = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{R}_q$
$X_{c,2}$	90	The set $X_{c,\omega}$ for a permutation $\omega = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{N}_q$
$F_{i,z}$	90	A polynomial that can be used to determine whether a permutation $\omega = \omega[a,b]$ with $a \in \mathcal{R}_q$ satisfies a sequence $z \in X_{c,\omega}/\sim$
$G_{i,z}$	90	A polynomial that can be used to determine whether a permutation $\omega = \omega[a,b]$ with $a \in \mathcal{N}_q$ satisfies a sequence $z \in X_{c,\omega}/\sim$
$Y_{c,\omega}$	91	The set of sequences $z \in \{-1,1\}^{2c}$ such that (z,ω) is of Type Two
$Y_{c,1}$	91	The set $Y_{c,\omega}$ for a permutation $\omega = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{R}_q$
$Y_{c,2}$	91	The set $Y_{c,\omega}$ for a permutation $\omega = \omega[a,b] \in \Lambda_c$ with $a \in \mathcal{N}_q$
$s(\omega,z)$	91	The number of $j \in \mathbb{F}_q$ such that ω satisfies z with j
g_z	92	A polynomial such that if some $\omega = \omega[a,b]$ with $a \in \mathcal{R}_q$ satisfies z and (z,ω) is of Type Two, then (a,b) is a root of g_z
h_z	92	A polynomial such that if some $\omega = \omega[a,b]$ with $a \in \mathcal{N}_q$ satisfies z and (z,ω) is of Type Two, then (a,b) is a root of h_z
Λ^*	93	The permutations $\omega[a,b] \in \Lambda$ with $a \neq b$
$\mathrm{Atp}_i(Q)$	108	The projection of $\mathrm{Atp}(Q)$ onto the i-th coordinate

Bibliography

[1] P. Adams, D. Bryant, and M. Buchanan, *Completing partial Latin squares with two filled rows and two filled columns*, Electron. J. Combin., 15 (2008). R56, 26pp.

[2] J. Allsop, *Cycles of quadratic Latin squares and antiperfect 1-factorisations*, J. Combin. Des., 31 (2023), pp. 447–475.

[3] ——, *Isotopisms of quadratic quasigroups*, arXiv:2506.02446, (2025).

[4] J. Allsop and I. M. Wanless, *Latin squares without proper subsquares*, arXiv:2310.01923, (2023).

[5] ——, *Row-Hamiltonian Latin squares and Falconer varieties*, Proc. Lond. Math. Soc. (3), 128 (2024). Paper No. e12575, 28pp.

[6] ——, *Perfect 1-factorisations of* $K_{11,11}$, arXiv:2506.02455, (2025).

[7] ——, *Subsquares in Random Latin Rectangles*, Combinatorica, 45 (2025). Paper No. 29, 18pp.

[8] L. D. Andersen and E. Mendelsohn, *A direct construction for Latin squares without proper subsquares*, in Algebraic and geometric combinatorics, vol. 65 of North-Holland Math. Stud., North-Holland, Amsterdam, 1982, pp. 27–53.

[9] B. A. Anderson, *Finite topologies and Hamiltonian paths*, J. Combinatorial Theory Ser. B, 14 (1973), pp. 87–93.

[10] ——, *A perfectly arranged Room square*, in Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1973), vol. VIII of Congress. Numer., Utilitas Math., Winnipeg, MB, 1973, pp. 141–150.

[11] ——, *A class of starter induced* 1*-factorizations*, in Graphs and combinatorics (Proc. Capital Conf., George Washington Univ., Washington, D.C., 1973), vol. Vol. 406 of Lecture Notes in Math., Springer, Berlin-New York, 1974, pp. 180–185.

[12] ——, *Some perfect* 1*-factorizations*, in Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing (Louisiana State Univ., Baton Rouge, La., 1976), vol. No. XVII of Congress. Numer., Utilitas Math., Winnipeg, MB, 1976, pp. 79–91.

[13] ——, *Symmetry groups of some perfect* 1*-factorizations of complete graphs*, Discrete Math., 18 (1977), pp. 227–234.

[14] B. A. Anderson and D. Morse, *Some observations on starters*, in Proceedings of the Fifth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1974), vol. No. X of Congress. Numer., Utilitas Math., Winnipeg, MB, 1974, pp. 229–235.

[15] N. Astromujoff and M. Matamala, *A quantitative approach to perfect one-factorizations of complete bipartite graphs*, Electron. J. Combin., 22 (2015). P1.72, 10pp.

[16] V. D. Belousov, *Elements of quasigroup theory: a special course*, Kishinev State University Printing House, Kishinev, (1981).

[17] N. M. A. Benson and P. J. Dukes, *Pairwise balanced designs covered by bounded flats*, Ann. Comb., 20 (2016), pp. 419–431.

[18] J. Browning, D. S. Stones, and I. M. Wanless, *Bounds on the number of autotopisms and subsquares of a Latin square*, Combinatorica, 33 (2013), pp. 11–22.

[19] J. M. Browning, P. J. Cameron, and I. M. Wanless, *Bounds on the number of small Latin subsquares*, J. Combin. Theory Ser. A, 124 (2014), pp. 41–56.

[20] R. H. Bruck, *A survey of binary systems*, Reihe: Gruppentheorie, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1958. Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.), Heft 20.

[21] D. Bryant, B. M. Maenhaut, and I. M. Wanless, *A family of perfect factorisations of complete bipartite graphs*, J. Combin. Theory Ser. A, 98 (2002), pp. 328–342.

[22] ——, *New families of atomic Latin squares and perfect 1-factorisations*, J. Combin. Theory Ser. A, 113 (2006), pp. 608–624.

[23] P. J. Cameron, *Minimal edge-colourings of complete graphs*, J. London Math. Soc. (2), 11 (1975), pp. 337–346.

[24] A. Caranti, F. Dalla Volta, and M. Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen, 69 (2006), pp. 297–308.

[25] L. Carlitz, *A theorem on permutations in a finite field*, Proc. Amer. Math. Soc., 11 (1960), pp. 456–459.

[26] N. J. Cavenagh and R. M. Falcón, *Latin bitrades derived from quasigroup autoparatopisms*, J. Algebraic Combin., 62 (2025). Paper No. 30, 20pp.

[27] N. J. Cavenagh, C. Greenhill, and I. M. Wanless, *The cycle structure of two rows in a random Latin square*, Random Structures Algorithms, 33 (2008), pp. 286–309.

[28] F. Celler and C. R. Leedham-Green, *Calculating the order of an invertible matrix*, in Groups and computation, II (New Brunswick, NJ, 1995), vol. 28 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 1997, pp. 55–60.

[29] C. Colbourn, L. Haddad, and V. Linek, *Equitable embeddings of Steiner triple systems*, J. Combin. Theory Ser. A, 73 (1996), pp. 229–247.

[30] C. J. Colbourn and J. H. Dinitz, eds., *Handbook of combinatorial designs*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, second ed., 2007.

[31] J. Dénes and A. D. Keedwell, *Latin squares and their applications*, Academic Press, New York-London, 1974.

[32] ——, *Latin squares*, vol. 46 of Annals of Discrete Mathematics, North-Holland Publishing Co., Amsterdam, 1991.

[33] L. E. Dickson and F. H. Safford, *Solution to problem 8 (group theory)*, Amer. Math. Monthly, 13 (1906), pp. 150–151.

[34] J. H. Dinitz and P. Dukes, *On the structure of uniform one-factorizations from starters in finite fields*, Finite Fields Appl., 12 (2006), pp. 283–300.

[35] J. H. Dinitz, P. Dukes, and D. R. Stinson, *Sequentially perfect and uniform one-factorizations of the complete graph*, Electron. J. Combin., 12 (2005). R1, 12pp.

[36] J. H. Dinitz and D. K. Garnick, *There are* 23 *nonisomorphic perfect one-factorizations of* K_{14}, J. Combin. Des., 4 (1996), pp. 1–4.

[37] 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.

[38] J. H. Dinitz and D. R. Stinson, *Some new perfect one-factorizations from starters in finite fields*, J. Graph Theory, 13 (1989), pp. 405–415.

[39] A. Divoux, T. Kelly, C. Kennedy, and J. Sidhu, *Subsquares in random latin squares and rectangles*, arXiv:2311.04152, (2023).

[40] J. D. Dixon and B. Mortimer, *Permutation groups*, vol. 163 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[41] J. D. Dixon and A. E. Zalesskii, *Finite primitive linear groups of prime degree*, J. London Math. Soc. (2), 57 (1998), pp. 126–134.

[42] A. Drápal and I. M. Wanless, *Maximally nonassociative quasigroups via quadratic orthomorphisms*, Algebr. Comb., 4 (2021), pp. 501–515.

[43] ——, *Isomorphisms of quadratic quasigroups*, Proc. Edinb. Math. Soc. (2), 66 (2023), pp. 1085–1109.

[44] ——, *On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups*, J. Aust. Math. Soc., 115 (2023), pp. 311–336.

[45] P. Dukes and A. C. H. Ling, *Edge-colourings of* $K_{n,n}$ *with no long two-coloured cycles*, Combinatorica, 28 (2008), pp. 373–378.

[46] ——, *Linear spaces with small generated subspaces*, J. Combin. Theory Ser. A, 116 (2009), pp. 485–493.

[47] 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.

[48] A. B. Evans, *Orthomorphism graphs of groups*, vol. 1535 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1992.

[49] ——, *Orthogonal Latin squares based on groups*, vol. 57 of Developments in Mathematics, Springer, Cham Switzerland, 2018.

[50] V. Fack and B. D. McKay, *A generalized switching method for combinatorial estimation*, Australas. J. Combin., 39 (2007), pp. 141–154.

[51] E. N. Gelling and R. E. Odeh, *On* 1*-factorizations of the complete graph and the relationship to round robin schedules*, in Proceedings of the Third Manitoba Conference on Numerical Mathematics (Winnipeg, Man., 1973), vol. IX of Congress. Numer., Utilitas Math., Winnipeg, MB, 1974, pp. 213–221.

[52] P. B. Gibbons and E. Mendelsohn, *The existence of a subsquare free Latin square of side* 12, SIAM J. Algebraic Discrete Methods, 8 (1987), pp. 93–99.

[53] M. J. Gill, A. Mammoliti, and I. M. Wanless, *Canonical labeling of Latin squares in average-case polynomial time*, Random Structures Algorithms, 66 (2025). Paper No. e70015, 23pp.

[54] M. J. Gill and I. M. Wanless, *Perfect 1-factorisations of* K_{16}, Bull. Aust. Math. Soc., 101 (2020), pp. 177–185.

[55] C. D. Godsil and B. D. McKay, *Asymptotic enumeration of Latin rectangles*, J. Combin. Theory Ser. B, 48 (1990), pp. 19–44.

[56] R. Häggkvist, *Problems*, in Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, vol. 18 of Colloq. Math. Soc. János Bolyai, North-Holland, Amsterdam-New York, 1978, pp. 1203–1204.

[57] A. Hartman and K. Heinrich, *Pairwise balanced designs with holes*, in Graphs, matrices, and designs, vol. 139 of Lecture Notes in Pure and Appl. Math., Dekker, New York, 1993, pp. 171–204.

[58] M. Hasheminezhad and B. D. McKay, *Combinatorial estimates by the switching method*, in Combinatorics and graphs, vol. 531 of Contemp. Math., Amer. Math. Soc., Providence, RI, 2010, pp. 209–221.

[59] K. Heinrich, *Latin squares composed of four disjoint subsquares*, in Combinatorial mathematics, V (Proc. Fifth Austral. Conf., Roy. Melbourne Inst. Tech., Melbourne, 1976), vol. Vol. 622 of Lecture Notes in Math., Springer, Berlin-New York, 1977, pp. 118–127.

[60] ——, *Latin squares with no proper subsquares*, J. Combin. Theory Ser. A, 29 (1980), pp. 346–353.

[61] K. Heinrich and W. D. Wallis, *The maximum number of intercalates in a Latin square*, in Combinatorial mathematics, VIII (Geelong, 1980), vol. 884 of Lecture Notes in Math., Springer, Berlin, 1981, pp. 221–233.

[62] F. Hiner and R. Killgrove, *Subsquare complete latin square*, Notices Amer. Math. Soc., 17 (1970), pp. 758–758.

[63] J. D. Horton, *Room designs and one-factorizations*, Aequationes Math., 22 (1981), pp. 56–63.

[64] S. Huczynska, *Powerline communication and the 36 officers problem*, Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci., 364 (2006), pp. 3199–3214.

[65] A. Hulpke, P. Kaski, and P. R. J. Östergård, *The number of Latin squares of order 11*, Math. Comp., 80 (2011), pp. 1197–1219.

[66] E. C. Ihrig, E. S. Seah, and D. R. Stinson, *A perfect one-factorization of* K_{50}, in Proceedings of the first Carbondale combinatorics conference (Carbondale, Ill., 1986), vol. 1, 1987, pp. 217–219.

[67] P. Kaski and P. R. J. Östergård, *There are* $1,132,835,421,602,062,347$ *nonisomorphic one-factorizations of* K_{14}, J. Combin. Des., 17 (2009), pp. 147–159.

[68] T. Kemp, *Latin squares with five disjoint subsquares*, J. Combin. Des., 33 (2025), pp. 39–57.

[69] R. B. Killgrove and E. Milne, *Subsquare complete Latin squares of order* 12, in Proceedings of the Fifth Southeastern Conference on Combinatorics, Graph Theory and Computing (Florida Atlantic Univ., Boca Raton, Fla., 1974), vol. No. X of Congress. Numer., Utilitas Math., Winnipeg, MB, 1974, pp. 535–547.

[70] M. Kobayashi, H. Awoki, Y. Nakazaki, and G. Nakamura, *A perfect one-factorization of* K_{36}, Graphs Combin., 5 (1989), pp. 243–244.

[71] M. Kobayashi and Kiyasu-Zen'iti, *Perfect one-factorizations of* K_{1332} *and* K_{6860}, J. Combin. Theory Ser. A, 51 (1989), pp. 314–315.

[72] 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.

[73] A. Kotzig, *Hamilton graphs and Hamilton circuits*, in Theory of Graphs and its Applications (Proc. Sympos. Smolenice, 1963), Publ. House Czechoslovak Acad. Sci., Prague, 1964, pp. 63–82.

[74] A. Kotzig, C. C. Lindner, and A. Rosa, *Latin squares with no subsquares of order two and disjoint Steiner triple systems*, Utilitas Math., 7 (1975), pp. 287–294.

[75] A. Kotzig and J. Turgeon, *On certain constructions for Latin squares with no Latin subsquares of order two*, Discrete Math., 16 (1976), pp. 263–270.

[76] M. Kwan, A. Sah, and M. Sawhney, *Large deviations in random Latin squares*, Bull. Lond. Math. Soc., 54 (2022), pp. 1420–1438.

[77] M. Kwan, A. Sah, M. Sawhney, and M. Simkin, *Substructures in Latin squares*, Israel J. Math., 256 (2023), pp. 363–416.

[78] M. Kwan and B. Sudakov, *Intercalates and discrepancy in random Latin squares*, Random Structures Algorithms, 52 (2018), pp. 181–196.

[79] P. J. Laufer, *On strongly Hamiltonian complete bipartite graphs*, Ars Combin., 9 (1980), pp. 43–46.

[80] C. F. Laywine and G. L. Mullen, *Discrete mathematics using Latin squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[81] C. H. Li, *The finite primitive permutation groups containing an abelian regular subgroup*, Proc. London Math. Soc. (3), 87 (2003), pp. 725–747.

[82] R. Lidl and H. Niederreiter, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, second edition ed., 1997.

[83] C. C. Lindner and C. A. Rodger, *Design theory*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, second ed., 2009.

[84] P. Lisoněk, *Maximal nonassociativity via fields*, Des. Codes Cryptogr., 88 (2020), pp. 2521–2530.

[85] B. Maenhaut, I. M. Wanless, and B. S. Webb, *Subsquare-free Latin squares of odd order*, European J. Combin., 28 (2007), pp. 322–336.

[86] B. M. Maenhaut and I. M. Wanless, *Atomic Latin squares of order eleven*, J. Combin. Des., 12 (2004), pp. 12–34.

[87] B. D. McKay, *Combinatorial data. latin cubes and hypercubes.* https://users.cecs.anu.edu.au/~bdm/data/latincubes.html.

[88] B. D. McKay, A. Meynert, and W. Myrvold, *Small Latin squares, quasigroups, and loops*, J. Combin. Des., 15 (2007), pp. 98–119.

[89] B. D. McKay and A. Piperno, *Practical graph isomorphism, II*, J. Symbolic Comput., 60 (2014), pp. 94–112.

[90] B. D. McKay and I. M. Wanless, *Most Latin squares have many subsquares*, J. Combin. Theory Ser. A, 86 (1999), pp. 322–347.

[91] ——, *A census of small Latin hypercubes*, SIAM J. Discrete Math., 22 (2008), pp. 719–736.

[92] B. D. McKay, I. M. Wanless, and X. Zhang, *The order of automorphisms of quasigroups*, J. Combin. Des., 23 (2015), pp. 275–288.

[93] M. McLeish, *On the existence of Latin squares with no subsquares of order two*, Utilitas Math., 8 (1975), pp. 41–53.

[94] M. Meszka, *k-cycle free one-factorizations of complete graphs*, Electron. J. Combin., 16 (2009). R3, 14pp.

[95] ——, *There are 3155 nonisomorphic perfect one-factorizations of K_{16}*, J. Combin. Des., 28 (2020), pp. 85–94.

[96] J. Ninčák, *A note concerning the colourings of bipartite graphs*, in Proc. of 6th Conference of EF TU, Math. Section, Košice, 1992, pp. 65–69.

[97] J. Ninčák and P. J. Owens, *On a problem of R. Häggkvist concerning edge-colouring of bipartite graphs*, Combinatorica, 24 (2004), pp. 325–329.

[98] H. W. Norton, *The 7 x 7 squares*, Ann. Eugenics, 9 (1939), pp. 269–307.

[99] P. J. Owens and D. A. Preece, *Some new non-cyclic Latin squares that have cyclic and Youden properties*, Ars Combin., 44 (1996), pp. 137–148.

[100] ——, *Some new non-cyclic Latin squares that have cyclic and Youden properties*, Ars Combin., 44 (1996), pp. 137–148.

[101] A. P. Petrenyuk and A. Y. Petrenyuk, *Intersection of perfect* 1*-factorizations of complete graphs*, Cybernetics, 16 (1980), pp. 6–9.

[102] D. A. Pike, *A perfect one-factorisation of K_{56}*, J. Combin. Des., 27 (2019), pp. 386–390.

[103] D. A. Preece, *Classifying Youden rectangles*, J. Roy. Statist. Soc. Ser. B, 28 (1966), pp. 118–130.

[104] A. Rosa, *Perfect 1-factorizations*, Math. Slovaca, 69 (2019), pp. 479–496.

[105] A. Sade, *Enumération des Carrés Latins. Application au 7^e Ordre. Conjecture pour les Ordres Supérieurs*, privately published, 1948.

[106] P. N. Saxena, *A simplified method of enumerating Latin squares by MacMahon's differential operators. II. The 7×7 Latin squares*, J. Indian Soc. Agric. Statist., 3 (1951), pp. 24–79.

[107] E. Schönhardt, *über lateinische Quadrate und Unionen*, J. Reine Angew. Math., 163 (1930), pp. 183–230.

[108] E. S. Seah, *Perfect one-factorizations of the complete graph—a survey*, Bull. Inst. Combin. Appl., 1 (1991), pp. 59–70.

[109] E. S. Seah and D. R. Stinson, *A perfect one-factorization for K_{36}*, Discrete Math., 70 (1988), pp. 199–202.

[110] ——, *A perfect one-factorization for K_{40}*, Congr. Numer., 68 (1989), pp. 211–213.

[111] G. Tarry, *Le problème des 36 officiers*, Ass Franç Paris, 29 (1900), pp. 170–203.

[112] J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge University Press, Cambridge, second ed., 2001.

[113] A. Vázquez-Ávila, *On* $(1, C_4)$ *one-factorization and two orthogonal* $(2, C_4)$ *one-factorizations of complete graphs*, Graphs Combin., 38 (2022). Paper No. 18, 11pp.

[114] I. M. Wanless, *User homepage*. https://users.monash.edu.au/~iwanless/data/.

[115] ——, *Permanents, matchings and Latin rectangles*, PhD thesis, Australian National University, 1998.

[116] ——, *Perfect factorisations of bipartite graphs and Latin squares without proper subrectangles*, Electron. J. Combin., 6 (1999). R9, 16pp.

[117] ——, *Latin squares with one subsquare*, J. Combin. Des., 9 (2001), pp. 128–146.

[118] ——, *Cycle switches in Latin squares*, Graphs Combin., 20 (2004), pp. 545–570.

[119] ——, *Diagonally cyclic Latin squares*, European J. Combin., 25 (2004), pp. 393–413.

[120] ——, *Atomic Latin squares based on cyclotomic orthomorphisms*, Electron. J. Combin., 12 (2005). R22, 23pp.

[121] I. M. Wanless and E. C. Ihrig, *Symmetries that Latin squares inherit from 1-factorizations*, J. Combin. Des., 13 (2005), pp. 157–172.

[122] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A., 34 (1948), pp. 204–207.

[123] A. J. Wolfe, *A perfect one-factorization of* K_{52}, J. Combin. Des., 17 (2009), pp. 190–196.

[124] B. Zelinka, *On a problem of R. Häggkvist concerning edge-colourings of graphs*, Časopis Pěst. Mat., 103 (1978), pp. 289–290.