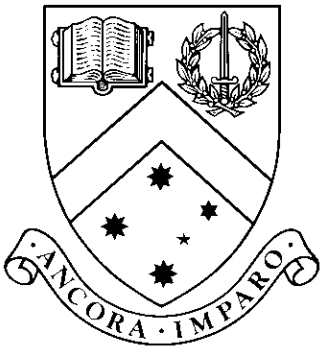
Autoparatopisms of Latin Squares

by

Mahamendige Jayama Lalani Mendis, BSc(Special), MSc. M.Phil



Thesis

Submitted by Mahamendige Jayama Lalani Mendis
for fulfilment of the Requirements for the Degree of
Doctor of Philosophy

Supervisor: Prof Ian M. Wanless
Associate Supervisor: Dr Daniel Horsley

School of Mathematical Sciences
Monash University

Autoparatopisms of Latin squares

Mahamendige Jayama Lalani Mendis, BSc(Special), M.Sc, M.Phil
[redacted]
Monash University, 2015

Supervisor: Prof. Ian M. Wanless
[redacted]
Associate Supervisor: Dr. Daniel Horsley
[redacted]

Abstract

In this thesis we study autoparatopisms and near-autoparatopisms of Latin squares. Also we find a family of Latin squares with an unique intercalate and no larger subsquares.

Paratopism is a well known action of the wreath product $\mathcal{S}_n \wr \mathcal{S}_3$ on Latin squares of order n. A paratopism that maps a Latin square to itself is an *autoparatopism* of that Latin square. Let $\mathrm{Par}(n)$ denote the set of paratopisms that are an autoparatopism of at least one Latin square of order n. We prove a number of general properties of autoparatopisms which between them are sufficient to determine $\mathrm{Par}(n)$ for $n \leqslant 17$.

Suppose that $n \equiv \pm 1 \mod 6$ and $n \geqslant 7$. We construct a Latin square L_n of order n with the following properties:

- L_n has no proper subsquares of order 3 or more.
- L_n has exactly one intercalate (subsquare of order 2).
- When the intercalate is replaced by the other possible subsquare on the same symbols, the resulting Latin square is in the same species as L_n.

Hence L_n generalises the square that Sade famously found to complete Norton's enumeration of Latin squares of order 7. In particular, L_n is what is known as a *self-switching* Latin square and possesses a *near-autoparatopism*.

Autoparatopisms of Latin Squares

Declaration

I declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at any university or other institute of tertiary education. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given.

Mahamendige Jayama Lalani Mendis
6 August 2015

Mahamendige Jayama Lalani Mendis
6 August 2015

Acknowledgement

Throughout the process of carrying out my thesis I was supported in numerous ways by my supervisor Prof Ian Wanless whose steady guidance, dedication and expert knowledge kept me confident on this thesis. He is thanked and reminded here with much gratitude. Again I am very grateful to my supervisor for giving every support including funds to enable me to participate at conferences which helped me to meet eminent experts in my field and to share knowledge on the subject among them. The knowledge I gained through conferences would help for my further career development. Also he is thanked for his extensive advice in editing my thesis. My associate supervisor Dr Daniel Horsley, Prof Graham Farr, Dr Kerri Morgan and all other research group colleagues are also thanked for their willingness to support me at any moment to achieve my target.

My parents, father late Mr Newton Mendis and Mrs Janet Mendis, whose dedication and attention paid on me, are close partners in my life towards not only this thesis but whatever success I've gained throughout my life. Taking this opportunity, they are fondly remembered.

My husband Mr Krishan De Silva, always behind me with all efforts in every possible way in encouraging me in this endeavour, is highly appreciated. Thanks to my husband as without his kindness and generous support this thesis would not have been completed to my best satisfaction.

My sister Sandya and brothers Piyal, Anil, Chandralal, Upul and sister in laws, brother in laws are remembered and thanked for their great support.

My friends Rosalind, Marie, Rema, Manjula, Jie, Marsha, Zohreh, Sangeeta, Sarada, Nevena are thanked for their involvement and well wishes which motivated and paved my path to accomplish this task.

Also I thank the administrative staff of the School of Mathematical Sciences for their excellent service.

Contents

1 Introduction **1**
- 1.1 Research contribution . . . 2
  - 1.1.1 Autoparatopisms . . . 2
  - 1.1.2 Near-autoparatopisms . . . 4

2 Literature Review **6**
- 2.1 Background . . . 6
- 2.2 Autotopisms of Latin squares . . . 8
  - 2.2.1 Block diagrams and contours . . . 11
- 2.3 Latin squares with a unique subsquare or no subsquares . . . 14
- 2.4 Cycle switches . . . 19
- 2.5 Near-autotopisms of Latin squares . . . 26

3 Autoparatopisms of Latin squares **29**
- 3.1 Introduction . . . 29
- 3.2 Some basic tools and terminology . . . 29
  - 3.2.1 Cycle structures . . . 29
  - 3.2.2 Cell orbits . . . 31
  - 3.2.3 Block diagrams and contours . . . 33
- 3.3 Basic conditions . . . 34
- 3.4 Automorphisms . . . 36
- 3.5 Autoparatopisms of the form $(\alpha, \beta, \gamma; (12))$ . . . 39
- 3.6 Autoparatopisms of the form $(\alpha, \beta, \gamma; (123))$ . . . 48
- 3.7 Wrapping up . . . 53

4 Near-Autoparatopisms **55**
- 4.1 Introduction . . . 55
- 4.2 Near-autoparatopisms . . . 56
- 4.3 The construction . . . 57
- 4.4 Small subsquares . . . 60
- 4.5 Non existence of large subsquares . . . 64

5 Conclusion **67**
- 5.1 Autoparatopisms . . . 67
- 5.2 Near-autoparatopisms . . . 67
- 5.3 Future research . . . 68

Bibliography **71**

Chapter 1

Introduction

A *quasigroup* is a non-empty set Q together with a binary operation $\circ$ such that for all $a, b \in Q$, there exist unique $x, y \in Q$ satisfying $a \circ x = b$ and $y \circ a = b$. A *Latin square* L of order n is an $n \times n$ array containing symbols from a set S of cardinality n, such that each symbol appears exactly once in each row and each column of L. Typically the rows and columns of L are indexed by elements of S. That way, L represents the (unbordered) Cayley table of a quasigroup on the set S, where the symbol $L(i, j)$ in the i^{th} row and j^{th} column of L records the product $i \circ j$. The set of n^2 ordered triples, $O(L) = \big\{(i, j, L(i, j)) : i, j \in S\big\}$ is called the *orthogonal array representation* of L. The elements of $O(L)$ will be called the *triples* or *entries* of L. The identity permutation is denoted by ε.

In the following definitions L will be the unbordered Cayley table of a quasigroup $(Q, \circ)$ of order n. Suppose $\theta = (\alpha, \beta, \gamma) \in \mathcal{S}_n^3$, where $\mathcal{S}_n$ is the symmetric group of degree n acting on Q. A new Latin square L^θ is obtained by permuting the rows, columns and symbols of L by α, β, and γ respectively. Specifically,

$$L^\theta(i, j) = L(i\alpha^{-1}, j\beta^{-1})\gamma. \tag{1.0.1}$$

Permutations act on the left. The map $\theta \in \mathcal{S}_n^3$ is known as an *isotopism* and L^θ is said to be *isotopic* to L. If $L^\theta = L$, then θ is called an *autotopism* of L. If $\theta = (\alpha, \alpha, \alpha)$ and $L^\theta = L$ then α is said to be an *automorphism* of L, since it is an automorphism of the underlying quasigroup $(Q, \circ)$.

Isotopism is a special case of *paratopism*, which is an action of the wreath product $\mathcal{P}_n = \mathcal{S}_n \wr \mathcal{S}_3$ on Latin squares of order n. Suppose $\theta = (\alpha, \beta, \gamma) \in \mathcal{S}_n^3$ and $\delta \in \mathcal{S}_3$. We use $(\alpha, \beta, \gamma; \delta)$ to denote the element $\sigma \in \mathcal{P}_n$ which acts on L by permuting the triples of L^θ by δ. The resulting triples determine a Latin square denoted by L^σ. For example, if (x, y, z) is a triple of L then L^σ contains a triple

$$\begin{cases} (y\beta, x\alpha, z\gamma), & \text{if } \delta = (12), \\ (z\gamma, x\alpha, y\beta), & \text{if } \delta = (123). \end{cases}$$

If $L^\sigma = L$, then σ is called an *autoparatopism* of L. Isotopism is the case of paratopism when $\delta = \varepsilon$. An orbit of Latin squares under paratopism is called a *species* (also known as a *main class*).

The groups of all automorphisms, autotopisms and autoparatopisms of L will be denoted by $\mathrm{Aut}(L)$, $\mathrm{Atp}(L)$ and $\mathrm{Par}(L)$ respectively. Let $\Delta(\theta)$, where $\theta \in \mathcal{S}_n^3$, be the number of Latin squares L of order n such that $\theta \in \mathrm{Atp}(L)$. Let $\mathrm{Atp}(n) = \{\theta \in \mathcal{S}_n^3 \ : \ \Delta(\theta) > 0\}$ and $\mathrm{Aut}(n) = \{\alpha \in \mathcal{S}_n : (\alpha, \alpha, \alpha) \in \mathrm{Atp}(n)\}$. Let $\Delta(\sigma)$, where $\sigma \in \mathcal{P}_n$, be the number of Latin squares L of order n such that $\sigma \in \mathrm{Par}(L)$. Let $\mathrm{Par}(n) = \{\sigma \in \mathcal{P}_n : \Delta(\sigma) > 0\}$.

If a submatrix M of L is also a Latin square then M is called a *subsquare* of L. If L is a Latin square of order n, and M is a subsquare of order m with $1 < m < n$, then we call M a *proper subsquare* of L. For every s, the number of subsquares of order s is invariant within a species. A subsquare of order 2 is an *intercalate*.

Suppose M is an intercalate of a Latin square L. Then M can be *turned* by swapping two symbols of M as follows.

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \qquad \leftrightarrow \qquad \begin{bmatrix} b & a \\ a & b \end{bmatrix}$$

Turning an intercalate is a special type of cycle switch in Latin squares [81] which are, in turn, a special type of Latin trade [13]. Also this is called an intercalate switching.

The *Hamming distance* between two Latin squares L and L' of the same order is defined by

$$\mathrm{dist}(L, L') = \big|\{d \in O(L) : d \notin O(L')\}\big|.$$

Hence $\mathrm{dist}(L, L^\sigma) = 0$ for $\sigma \in \mathcal{P}_n$ if and only if σ is an autoparatopism of L. The difference between two Latin squares gives rise to a Latin trade [13], which implies that $\mathrm{dist}(L, L^\sigma) \notin \{1, 2, 3, 5\}$, regardless of L and σ. This observation motivates the following definitions. An isotopism $\theta = (\alpha, \beta, \gamma) \in \mathcal{S}_n^3$ is said to be a *near-autotopism* of a Latin square L if $\mathrm{dist}(L, L^\theta) = 4$. If $\theta = (\alpha, \alpha, \alpha)$ is a near-autotopism of L, then α is called a *near-automorphism* of L. If $\sigma = (\alpha, \beta, \gamma; \delta) \in \mathcal{P}_n$, then σ is said to be a *near-autoparatopism* of L if $\mathrm{dist}(L, L^\sigma) = 4$. Any two Latin squares L, L' with $\mathrm{dist}(L, L') = 4$ differ only by turning an intercalate [15].

1.1 Research contribution

1.1.1 Autoparatopisms

Chapter 3 begins with some basic tools such as cycle structure, conjugacy, cell orbits, block diagrams and contours.

From Theorem 3.2.1, we are able to understand the connection between conjugacy and autoparatopism. If two paratopisms are conjugate and one is an autoparatopism of a Latin square then the other one is also an autoparatopism of another Latin square.

Theorem 3.2.2 gives the full picture regarding cycle structures of two paratopisms $\sigma_1 = (\alpha_1, \alpha_2, \alpha_3; \delta_1)$ and $\sigma_2 = (\beta_1, \beta_2, \beta_3; \delta_2)$ such that σ_1, σ_2 are conjugate in $\mathcal{P}_n$. For example, when $\delta_1 = \delta_2 = (12)$, σ_1 and σ_2 are conjugate if $\alpha_1\alpha_2$ and $\beta_1\beta_2$ have the same cycle structure and α_3 and β_3 have the same cycle structure. Also when $\delta_1 = \delta_2 = (123)$, σ_1 and σ_2 are conjugate when $\alpha_1\alpha_2\alpha_3$ and $\beta_1\beta_2\beta_3$ have the same cycle structure. Note that Stones, Vojtěchovský and Wanless [75] proved that whether $\theta = (\alpha, \beta, \gamma)$ is in $\mathrm{Atp}(n)$ depends only on the cycle structures of α, β and γ.

Sections 3.2.2 and 3.2.3 introduce cell orbits, block diagrams and contours which we use for construction of Latin squares L with $\sigma = (\alpha, \beta, \gamma; \delta) \in \mathrm{Par}(L)$ when $\delta = \varepsilon, (12), (123)$. The properties of block diagrams, cell orbits and contours are more complicated when $\delta = (12)$ and $\delta = (123)$. They have been investigated in Lemmas 3.2.3 and 3.2.4.

We study basic necessary conditions for $\mathrm{Par}(n)$ in Section 3.3. First we establish a most useful necessary condition known as the lcm condition. Stones, Vojtěchovský and Wanless [75] found this condition for autotopisms and we adapt it for autoparatopisms $\sigma = (\alpha, \beta, \gamma; \delta)$ when $\delta = (12)$ and (123). It is clear from Lemmas 3.3.1, 3.3.2 and 3.3.3 there are some differences and similarities in the lcm condition according to δ.

Then we give the definition for a strongly lcm closed set and use it in Theorems 3.3.4 and 3.3.6. How non autoparatopisms can be identified using these results is clear from the examples given after Theorem 3.3.4.

Corollary 3.3.5 proves the existence of a subsquare such that if $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$ then the submatrix M whose rows and columns belong to $\mathrm{Fix}(\beta)$ is a subsquare of L. Also Corollary 3.3.7 proves existence of a subsquare such that if $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(L)$ then the submatrix M whose rows and columns belong to $\mathrm{Fix}(\gamma)$ is a subsquare of L. Hence using subsquare properties we can conclude that $|\mathrm{Fix}(\beta)| \leqslant n/2$ if $\beta \neq \varepsilon$ when $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$ and $|\mathrm{Fix}(\gamma)| \leqslant n/2$ if $\gamma \neq \varepsilon$ when $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(L)$.

Theorem 3.3.11 was derived in terms of autoparatopisms since Bryant, Buchanan and Wanless [9] have established some results regarding Latin squares with cyclic automorphisms and additional conjugate symmetries.

Stones, Vojtěchovský and Wanless [75] determined several necessary conditions for an isotopism (α, β, γ) to be in $\mathrm{Atp}(n)$ and finally found $\mathrm{Atp}(n)$ for $n \leqslant 17$. In this process they investigated necessary and sufficient conditions for $(\alpha, \alpha, \alpha) \in \mathrm{Atp}(n)$ for general n when α has at most three cycles other than fixed points and when the non-fixed points of α are in cycles of the same length. Then we studied slightly further and found a sufficient condition for $(\alpha, \alpha, \alpha) \in \mathrm{Atp}(n)$ when α has four non-trivial cycles. Also we show that $\alpha = \alpha_1\alpha_1 \ldots \alpha_m \in \mathrm{Aut}(n)$ when the cycle structure of α is $d_1 d_2 \ldots d_p^a$ where $a = m - p + 1$.

In Section 3.5 and 3.6, we prove all relevant results to find $\mathrm{Par}(n)$ for $n \leqslant 17$ other than the basic necessary conditions which we already discussed above.

Autoparatopisms $\sigma = (\alpha, \beta, \gamma; (12))$

Since by Theorem 3.2.1, whether $\sigma = (\alpha, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ depends only on the cycle structure of $\alpha\beta$ and the cycle structure of γ, it is enough to study paratopisms of the form $(\varepsilon, \beta, \gamma; (12))$. Theorems 3.5.1, 3.5.3, 3.5.4, 3.5.5 and 3.5.6 prove some necessary conditions for the cycle structure of γ for $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ when the cycle structure of β is given. In these results we study the behaviour of γ when β has (i) a cycle of odd length d (ii) exactly r cycles of some length d (iii) precisely r cycles of some length d and r is odd, and further every cycle of β has length divisible by 2^u, where $n = 2^u v$, v is odd.

We find in Theorems 3.5.7, 3.5.8 all possible cycle structures of γ for $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ when β is ε and n^1. Also a sufficient condition for $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ has been proved in Corollary 3.5.9 using Theorem 3.5.8 and direct product when the cycle structure of β is d^r and the cycle structure of γ is $d_1^{ra_1} d_2^{ra_2} \cdots d_p^{ra_p}$.

We prove some necessary and sufficient condition for $\sigma = (\alpha, \alpha, \alpha; (12)) \in \mathrm{Par}(n)$ when the cycle structure of γ is $d^1 \cdot 1^f$, where $d > 1$. This result is used to prove Corollary 3.5.13.

In the study of paratopisms of the form $\sigma = (\varepsilon, \beta, \beta; (12))$, some necessary and sufficient conditions for σ to be an autoparatopism are established when the cycle structure of β is $d \cdot 1^f$, $d^2 \cdot 1^f$, where $d > 1$, $d_1 \cdot d_2 \cdot 1^f$, where $d_1 > d_2 > 1$ and $d_1 \cdot d_2^l$, where d_1 is even and d_1/d_2 is an odd integer.

Autoparatopisms $\sigma = (\alpha, \beta, \gamma; (123))$

Since already we have proved that $\sigma = (\alpha, \beta, \gamma; (123)) \in \mathrm{Par}(n)$ depends on the cycle structure of $\alpha\beta\gamma$ in Theorem 3.2.1 it suffices to study paratopisms of the form $(\varepsilon, \varepsilon, \gamma; (123))$ to find $\mathrm{Par}(n)$.

Theorem 3.6.1 proves conditions for non-existence of autoparatopisms $\sigma = (\varepsilon, \varepsilon, \gamma; (123))$ when γ has precisely r cycles of some length d.

Some necessary conditions for $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$ are determined in Theorem 3.6.2 when γ has cycle structure d^r. When the cycle structure of γ is 5^2, it is impossible to use Theorem 3.6.2 to show $\sigma \notin \mathrm{Par}(n)$. Hence we have a separate proof in Theorem 3.6.3 for this isolated case.

Theorem 3.6.4 investigates some necessary and sufficient conditions for a paratopism of the form $\sigma = (\alpha, \alpha, \alpha; (123))$ to be an autoparatopism when the cycle structure of α is $d^1 \cdot 1^f$. This result has some benefits since it paves the way to prove the essential Corollaries 3.6.5, 3.6.6, 3.6.7 for our requirement.

Using all of these results finally we found $\mathrm{Par}(n)$ for $n \leqslant 17$.

At the end of the Chapter 3 we see some contrasting properties regarding the behaviour of autoparatopisms $\sigma = (\alpha, \beta, \gamma; (12))$ when $\lambda = \varepsilon, (12), (123)$. McKay, Wanless and Zhang found for almost all $\alpha \in S_n$, there are no $\beta, \gamma \in \mathcal{S}_n$ such that $\theta = (\alpha, \beta, \gamma) \in \mathrm{Aut}(n)$. But this is not true for all other cases of autoparatopisms since we prove given any $\alpha \in \mathcal{S}_n$, there exist $\beta, \gamma \in \mathcal{S}_n$ such that $\sigma = (\alpha, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ and for all $\alpha, \beta \in S_n$ there exist $\gamma \in S_n$ such that $\sigma = (\alpha, \beta, \gamma; (123)) \in \mathrm{Par}(n)$.

1.1.2 Near-autoparatopisms

Cavenagh and Stones [15] introduced near-automorphisms and found many results regarding them. They observed Latin squares which admit near-automorphism and the existence of such Latin squares for $n \geqslant 5$ was proved. The problem to find Latin squares L that admit a near-automorphism α while both L and αL contain only a single intercalate was suggested by them in [15]. In Chapter 4, we take a similar approach for near-autoparatopism $\sigma = (\varepsilon, \beta, \gamma; (12))$ and establish an infinite family of Latin squares L_n with unique intercalate which admit near-autoparatopism σ. This is also a partial solution to Conjecture 4.1.2 from [79].

At the begining of Chapter 4 we discuss conjugacy of near-autoparatopisms. Here we prove if two paratopisms are conjugate and one is a near-autoparatopism of a Latin square then the other one is also a near-autoparatopism of another Latin square.

Theorem 4.2.2 explains how near-autoparatopism relates to autoparatopism. Theorem 4.2.3 proves the existence of a family of Latin squares which admit a near-autoparatopism.

In Section 4.3, we describe the construction of Latin squares L_n with one intercalate and no larger subsquares which admit a near-autoparatopism $\sigma = (\varepsilon, \beta^{(n-3)/2}, \beta^{(n-3)/2}(\star\diamond); (12))$, where $\beta = (01 \dots n-3)$ and the symbols $\star, \diamond$ are referred to as infinity symbols. This is the main focus of this chapter. These Latin squares consist of four main parts A, B, C, D according to the pattern of the symbols, where A, B, C, D are submatrices of L_n and D is the unique intercalate. There are some interesting results in this section to avoid plenty of cases in later results in this chapter. If there is a subsquare S in L_n other than D then S does not have consecutive symbols, infinity symbols, consecutive rows or consecutive columns and further S is not an intercalate consisting of one triple from each of the four regions.

In our process to prove non-existence of subsquares other than D first we show there are no larger subsquares of order $n \geqslant 5$. Then we prove non-existence of intercalates other than D and there are no subsquares of order 3 and 4 in L_n.

Chapter 2

Literature Review

2.1 Background

A *Latin rectangle* is defined as a matrix with order $m \times n, 1 \leqslant m \leqslant n$ with n symbols such that each symbol occurs exactly once in each row and at most once in each column. If R is a $2 \times n$ Latin subrectangle of some Latin square L, and R is minimal in that it contains no $2 \times n'$ Latin subrectangle for $n' \in [2, n-1]$, then R is said to be a *row cycle* of length n. *Column cycles* and *symbol cycles* are defined similarly. Collectively these three types of objects are commonly described as cycles.

Consider the following definitions regarding bitrades and trades in [13].

A *partial Latin square* P of order n is an $n \times n$ array, possibly with empty cells, such that each symbol from S occurs at most once in each row and at most once in each column. Hence any subset of $O(L)$ corresponds to a partial Latin square.

Definition: Suppose T, T' are partial Latin squares. A *Latin bitrade* (T, T') is a set of ordered triples from $R \times C \times S$ such that for each $(r_i, c_j, s_k) \in T$ (respectively, T'), there exists unique $i' \neq i$, $j' \neq j$ and $k' \neq k$ such that: $(r_{i'}, c_j, s_k) \in T'$ (respectively, T), $(r_i, c_{j'}, s_k) \in T'$, (respectively, T), and $(r_i, c_j, s_{k'}) \in T'$, (respectively, T).

If (T, T') is a Latin bitrade then T is called a *Latin trade* and T' its disjoint mate.

Another definition for Latin bitrade is as follows (see [13] for examples).

Definition: A *Latin trade* is any ordered pair of the form $(L \setminus L', L' \setminus L)$, where L and L' are distinct Latin squares of order n.

A *complete mapping* of a group, loop, or quasigroup $(G, \star)$ is a bijection $x \to \theta(x)$ of G upon G such that the mapping $x \to \eta(x)$ defined by $\eta(x) = x \star \theta(x)$ is again a bijection of G upon G.

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

The following theorem in [16] shows the connection between complete mappings and transversals in Latin squares.

Theorem 2.1.1. *If Q is a quasigroup which possesses a complete mapping, then its multiplication table is a Latin square with a transversal. Conversely, if L is a Latin square having a transversal, then any quasigroup which has L as its multiplication table has a complete mapping.*

Suppose $(Q, \cdot)$ is a given quasigroup of order n which possesses a complete mapping θ. Dénes and Keedwell [16] gave a construction for a quasigroup $(Q', \star)$ of order $n+1$ from $(Q, \cdot)$, where the set Q' is obtained from Q by the adjunction of one additional element, using a process called prolongation which was introduced by Belousov [3].

This is the explanation of the construction using prolongation. Let $Q = \{1, 2, \ldots, n\}$ and let L be the Latin square formed by the multiplication table of the quasigroup $(Q, \cdot)$. Then L possesses at least one transversal by Theorem 2.1.1 since $(Q, \cdot)$ has a complete mapping. Replace the elements in all the cells of this transversal by the additional element $n+1$ and then, without changing their order, adjoin the elements of the transversal to the resulting square as its $(n+1)$th row and $(n+1)$th column. To complete the enlarged square L', adjoin the element $n+1$ as the entry of the cell which lies at the intersection of the $(n+1)$th row and $(n+1)$th column. The square L' is then Latin (see Fig 2.1 for an example) and defines the multiplication table of a quasigroup $(Q', \star)$ of order one greater than that of $(Q, \cdot)$. In the example illustrated in Fig 2.1, $(Q, \cdot)$ is the cyclic group of order

$(\cdot)$	1	2	3
1	1	2	[3]
2	[2]	3	1
3	3	[1]	2

$(\star)$	1	2	3	4
1	1	2	4	3
2	4	3	1	2
3	3	4	2	1
4	2	1	3	4

Figure 2.1:

3 and its prolongation $(Q', \star)$ is a quasigroup of order 4.

If L has a second transversal, the process can be repeated; since then the cells of this second transversal of L together with the cell of the $(n+1)$th row and column of L', form a transversal of L'.

We can specify a prolongation by defining the product $x \star y$ of all the pairs of elements x, y of Q'. If $x \cdot \theta(x) = \eta(x)$ then:

$$x \star y = \begin{cases} x \cdot y, & \text{if } x, y \in Q, y \neq \theta(x), \\ n+1, & \text{if } x, y \in Q, y = \theta(x), \\ \eta(x), & \text{if } x \in Q, y = n+1, \\ \eta[\theta^{-1}(y)], & \text{if } y \in Q, x = n+1, \\ n+1, & \text{if } x = y = n+1. \end{cases}$$

In the example (Fig 2.1)

$$\begin{aligned} \theta(1) &= 3, & \eta(1) &= 3, \\ \theta(2) &= 1, & \eta(2) &= 2, \\ \theta(3) &= 2, & \eta(3) &= 1. \end{aligned}$$

Bruck is the first mathematician who studied the construction of prolongation. But he discussed only the case in which $(Q, \cdot)$ is an idempotent quasigroup. Later Dénes and Pasztor [18] and Osborn [64] defined the construction for arbitrary quasigroups.

2.2 Autotopisms of Latin squares

The origin of the study of Latin squares and quasigroups goes many years back. The first important result regarding our research problem begins in 1782 when Euler [24] showed that if $\alpha \in \mathcal{S}_n$ is a single cycle with length d then $\alpha \in \mathrm{Aut}(n)$ if and only if d is odd. Much later, Wanless [82] generalised this for automorphisms containing a single nontrivial cycle with fixed points, showing:

Theorem 2.2.1. *If $\alpha \in \mathcal{S}_n$ has the cycle structure $d \cdot 1^{n-d}$, where $d > 1$, then $\alpha \in \mathrm{Aut}(n)$ if and only if either $d = n$ is odd or $\lceil n/2 \rceil \leqslant d \leqslant n$.*

Bryant, Buchanan and Wanless [9] extended the results from [82] to include quasigroups with additional properties, such as semisymmetry or idempotency. They define an f-type quasigroup, of order n, to have an automorphism consisting of a single cycle of length m and $f = n - m$ fixed points.

Theorem 2.2.2. *For $n < 2f$, the only f-type quasigroups satisfy $n = f$ and the spectra for these quasigroups are as indicated in the Table 2.1.*

$f = n$	No specified conjugate Symmetry	commutative	Semi-symmetric	Totally Symmetric
Arbitrary	all	all	all	all
Idempotent	all except 2	all odd	0,1 mod 3 except 6	1, 3 mod 6
Unipotent	all	all even	1, 2 mod 3 except 7	2, 4 mod 6

Table 2.1:

The following theorem gives the spectrum for the case $n \geqslant 2f$.

Theorem 2.2.3. *There are no idempotent f-type quasigroups of order $n = 2f$. Otherwise, for $n \geqslant 2f$ there exists an f-type quasigroup of order n having the additional properties indicated if and only if n satisfies the condition given in the Tables 2.2 and 2.3.*

$f = 0$	No specified conjugate symmetry	Commutative	Semi-symmetric	Totally symmetric
Arbitrary	all odd	all odd	1,3 mod 6	1, 3 mod 6
Idempotent	all odd	all odd	1,3 mod 6 except 9	1, 3 mod 6 except 9
Unipotent	1	1	1	1

Table 2.2:

Let $\mathcal{I}_n = \mathcal{S}_n \times \mathcal{S}_n \times \mathcal{S}_n$. McKay, Meynert and Myrvold [55] derived an important necessary condition for $\theta \in \mathcal{I}_n$ to belong to $\mathrm{Atp}(n)$ in the course of enumerating quasigroups of orders $\leqslant 10$ up to isomorphism.

$f = 1$	No specified conjugate symmetry	Commutative	Semi-symmetric	Totally symmetric
Arbitrary	all	all	1,2,3,4,5 mod 6 except 10	3,9 mod 24 1,2 mod 3 except 10
Idempotent	all	all odd	1,3,4 mod 6 except 10	3,9 mod 24
Unipotent	all	all even	2,4 mod 6 except 10	2,4 mod 6 except 10

Table 2.3:

Theorem 2.2.4. *Let L be a Latin square of order n and let (α, β, γ) be a nontrivial autotopism of L. Then one of the following holds.*

(i) α, β and γ have the same cycle structure with at least 1 and at most $n/2$ fixed points,

(ii) one of α, β or γ has at least 1 fixed point and the other two permutations have the same cycle structure with no fixed points, or

(iii) α, β and γ have no fixed points.

Any nontrivial autotopism $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ of a Latin square must have at least two nontrivial components.

Recently, Hulpke, Kaski and Östergård [37] used the symmetries of Latin squares to count species of order 11. Falcón and Martín-Morales [27] gave the nonzero values of $\Delta(\theta)$ for all $\theta \in \mathrm{Atp}(n)$ with $n \leqslant 7$. Later, Falcón [26] determined $\mathrm{Atp}(n)$ for all $n \leqslant 11$, and he gave several results of general nature.

Now consider these notations. If $\lambda \in \mathcal{S}_3$, then $O(L)^\lambda$ is obtained from $O(L)$ by permuting the coordinates of all entries of $O(L)$ by λ. The Latin square L^λ induced by $O(L)^\lambda$ is called a *parastrophe* of L.

The group $\mathcal{S}_3$ also acts on $\mathcal{I}_n$ by permuting the coordinates of $\mathcal{I}_n$. For given $\theta \in \mathcal{I}_n$ and $\lambda \in \mathcal{S}_3$, the resulting isotopism is denoted by θ^λ.

Stones, Vojtěchovský and Wanless [75] proved the following result.

Lemma 2.2.5. *Let $\lambda \in \mathcal{S}_3$, let $\theta, \phi \in \mathcal{I}_n$, and let L be a Latin square of order n. Then*

(i) $\theta \in \mathrm{Atp}(L)$ if and only if $\phi^{-1}\theta\phi \in \mathrm{Atp}(L\phi)$,

(ii) $\theta \in \mathrm{Atp}(L)$ if and only if $\theta^\lambda \in \mathrm{Atp}(L^\lambda)$.

Proof. To prove (i), observe that $\phi^{-1}\theta\phi \in \mathrm{Atp}(L\phi)$ if and only if $L\phi\phi^{-1}\theta\phi = L\phi$ if and only if $L\theta\phi = L\phi$ if and only if $L^\theta = L$ if and only if $\theta \in \mathrm{Atp}(L)$.

(ii) is obvious. □

Since two permutations in $\mathcal{S}_n$ are conjugate if and only if they have the same cycle structure [12], it is clear from Lemma 2.2.5 that the value of $\Delta(\theta)$ depends only on the cycle

structure of θ. For example, if α, β and γ have the same cycle structures then $\Delta((\alpha, \beta, \gamma)) = \Delta((\alpha, \alpha, \alpha))$.

In 1968, Sade [71] studied autotopisms with a trivial component and found that $\theta = (\alpha, \beta, \varepsilon) \in \mathcal{S}_n^3$ is an autotopism if both α and β consist of n/d cycles of length d for some divisor d of n. This was rediscovered in [29, 52]. In 2012, Stones, Vojtěchovský and Wanless [75] proved easily this necessary condition is sufficient.

Lemma 2.2.5 implies that the following theorem [75] characterizes all nontrivial autotopisms with one trivial component.

Theorem 2.2.6. *Let $\theta = (\alpha, \beta, \varepsilon) \in \mathcal{I}_n$. Then $\theta \in \mathrm{Atp}(n)$ if and only if both α and β consist of n/d cycles of length d, for some divisor d of n.*

Proof. Suppose L is a Latin square with $\theta \in \mathrm{Atp}(L)$. Let $o_\alpha(i) = c$ and $o_\beta(j) = d$. Then $\theta^c(i, j, L(i, j)) = (i, j\beta^c, L(i, j))$ and $j\beta^c = j$. Hence $d \mid c$. A similar argument proves $d \mid c$. Hence $c = d$. Therefore both α and β have only d-cycles.

Conversely suppose that L is a Latin square with n symbols satisfying $L(i, j) = i + j \bmod n$. Let $\theta = (\alpha, \beta, \varepsilon)$ with $\alpha = (12 \dots n)^{n/d}, \beta = \alpha^{-1}$. Then $\theta \in \mathrm{Atp}(L)$ and α, β consist of n/d cycles of length d. □

Stones, Vojtěchovský and Wanless [75] proved the following two necessary conditions for $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ to be an autotopism, that is, $\theta \in \mathrm{Atp}(n)$.

Theorem 2.2.7. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be an autotopism of a Latin square L. If $o_\alpha(i) = a$ and $o_\beta(j) = b$, then $o_\gamma(L(i, j)) = c$, where $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c)$.*

Proof. Since $\alpha^{\mathrm{lcm}(a,b)}$ fixes i and $\beta^{\mathrm{lcm}(a,b)}$ fixes j the entry $(i, j, L(i, j))$ must be a fixed point of $\theta^{\mathrm{lcm}(a,b)}$. Hence c divides $\mathrm{lcm}(a, b)$, and $\mathrm{lcm}(a, b) = \mathrm{lcm}(a, b, c)$ follows. The result follows since $\theta^\lambda \in \mathrm{Atp}(L^\lambda)$ for all $\lambda \in \mathcal{S}_3$ by Lemma 2.2.5. □

A nonempty subset T of $\mathbb{N}$ is said to be *strongly lcm closed* if $\mathrm{lcm}(a, b) \in T$ if and only if $a \in T$ and $b \in T$ for every $a, b \in \mathbb{N}$. If T is a finite strongly lcm-closed set, then T is the set of divisors of $\max T$.

Now we describe how strongly lcm-closed sets can be used to identify subsquares within Latin squares that admit autotopisms. Let $L = L(i, j)$ be a Latin square of order n with $\theta = (\alpha, \beta, \gamma) \in \mathrm{Atp}(L)$. Suppose M is a subsquare of L formed by the rows whose indices belong to $R \subseteq [n]$ and columns whose indices belong to $C \subseteq [n]$. Let $S = \{k : (i, j, k) \in O(L), i \in R, j \in C\}$, so $|R| = |C| = |S|$. We will say M is closed under the action of θ if R, C, and S are closed under the action of α, β, and γ, respectively. If M is closed under the action of θ, then we can form the autotopism θ_M of M, by restricting the domains of α, β, and γ to R, C and S, respectively.

Given $(\alpha, \beta, \gamma) \in \mathcal{I}_n$ and a strongly lcm-closed set Λ, define

$$\begin{aligned} R_\Lambda &= \{i \in [n] : o_\alpha(i) = a \text{ and } a \in \Lambda\}, \\ C_\Lambda &= \{i \in [n] : o_\beta(i) = b \text{ and } b \in \Lambda\}, \\ S_\Lambda &= \{i \in [n] : o_\gamma(i) = c \text{ and } c \in \Lambda\}. \end{aligned}$$

For $X \subset [n]$ let $\overline{X} = [n] \setminus X$.

Theorem 2.2.8. *Suppose L is a Latin square of order n. Let $\theta = (\alpha, \beta, \gamma) \in \mathrm{Atp}(L)$ and let Λ be a strongly* lcm*-closed set. If at least two of R_Λ, C_Λ and S_Λ are nonempty, then $|R_\Lambda| = |C_\Lambda| = |S_\Lambda|$ and L contains a subsquare M on the rows R_Λ, columns C_Λ and symbols S_Λ. Moreover, M admits the autotopism θ_M.*

In addition, if $|R_\Lambda| = |C_\Lambda| = |S_\Lambda| = n/2$ then L has four subsquares, each with autotopisms induced by θ. The subsquares are on the rows, columns and symbols $(R_\Lambda, C_\Lambda, S_\Lambda)$, $(R_\Lambda, \overline{C}_\Lambda, \overline{S}_\Lambda)$, $(\overline{R}_\Lambda, C_\Lambda, \overline{S}_\Lambda)$,$(\overline{R}_\Lambda, \overline{C}_\Lambda, S_\Lambda)$.

Proof. Up to parastrophy, we may assume $|R_\Lambda| \geqslant |C_\Lambda| \geqslant |S_\Lambda|$. Let M be the (necessarily nonempty) submatrix induced by rows R_Λ and columns C_Λ.

Suppose (i, j, k) is an entry of M. Then $o_\alpha(i) = a$ for some $a \in \Lambda$ and $o_\beta(j) = b$ for some $b \in \Lambda$. Let $o_\gamma(k) = c$. Hence by Lemma 2.2.7, $\mathrm{lcm}(a, c) = \mathrm{lcm}(a, b)$. Then $\mathrm{lcm}(a, c) \in \Lambda$ and $c \in \Lambda$ since Λ is a strongly lcm-closed set. Therefore, the set of symbols in M is a subset of S_Λ. Hence we can conclude that $|S_\Lambda| \geqslant |R_\Lambda|$ and $|R_\Lambda| = |C_\Lambda| = |S_\Lambda|$. It follows that M is a subsquare of L.

Since R_Λ, C_Λ and S_Λ are closed under the action of α, β and γ respectively, θ_M is an autotopism of M.

The remainder of the Theorem follows since any Latin square containing a subsquare of exactly half its order is composed of four disjoint subsquares of that order. □

2.2.1 Block diagrams and contours

Block diagrams and contours are used to construct Latin squares with a prescribed autotopism. A block diagram of a Latin square L which admits an automorphism α is described as follows.

Let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the nontrivial cycles of $\alpha \in \mathcal{S}_n$ with lengths $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_m$ respectively. Suppose α_∞ is the set of all fixed points of α, and $d_\infty = |\alpha_\infty|$. Let $[m]^* = [m] \cup \{\infty\}$. The Latin square L is divided into blocks M_{ij} for $i, j \in [m]^*$ according to the cycle structure of α such that $i \in \alpha_i$ and $j \in \alpha_j$. If each symbol of α_k appears f_k times in M_{ij} block then this is written as $\alpha_k : f_k$ in that block.

In a block diagram the following two Latin square properties should be satisfied.

(i) $d_1 f_1(i, j) + d_2 f_2(i, j) + \cdots + d_m f_m(i, j) + d_\infty f_\infty(i, j) = d_i d_j$ in every block M_{ij}.

(ii) For any $i, k \in [m]^*$, $\sum_{j \in [m]^*} f_k(i, j) = d_i$ and for any $j, k \in [m]^*$, $\sum_{i \in [m]^*} f_k(i, j) = d_j$.

In addition to the above properties the block diagram of a Latin square L with $\alpha \in \mathrm{Aut}(L)$ satisfies other restrictions. For example, Theorem 2.2.7 restricts the values of i, j, k for which $f_k(i, j)$ can be positive.

Examples for block diagrams

The block diagram of any Latin Square L with $\alpha \in \mathrm{Aut}(L)$, where

(1) α has cycle structure $d_1 \cdot d_2 \cdot 1^{d_\infty}$ with $d_1 > d_2 > 1$ is

(2) α has cycle structure $d_1 \cdot d_2 \cdot d_3$ with $d_1 > d_2 > d_3$, $d_3 \nmid d_2$, $d_3 \mid d_1$, and $d_2 \mid d_1$ is

	α_1	α_2	α_∞
α_1	$\alpha_1 : d_1 - d_2 - d_\infty$ $\alpha_2 : d_1$ $\alpha_\infty : d_1$	$\alpha_1 : d_2$	$\alpha_1 : d_\infty$
α_2	$\alpha_1 : d_2$	$\alpha_2 : d_2 - d_\infty$ $\alpha_\infty : d_2$	$\alpha_2 : d_\infty$
α_∞	$\alpha_1 : d_\infty$	$\alpha_2 : d_\infty$	$\alpha_\infty : d_\infty$

.

	α_1	α_2	α_3
α_1	$\alpha_1 : d_1 - d_2 - d_3 + (2d_2d_3/d_1)$ $\alpha_2 : d_1 - d_3$ $\alpha_3 : d_1 - d_2$	$\alpha_1 : (d_1 - d_3)d_2/d_1$ $\alpha_3 : d_2$	$\alpha_1 : (d_1 - d_2)d_3/d_1$ $\alpha_2 : d_3$
α_2	$\alpha_1 : (d_1 - d_3)d_2/d_1$ $\alpha_3 : d_2$	$\alpha_2 : d_2$	$\alpha_1 : d_2d_3/d_1$
α_3	$\alpha_1 : (d_1 - d_2)d_3/d_1$ $\alpha_2 : d_3$	$\alpha_1 : d_2d_3/d_1$	$\alpha_3 : d_3$

.

If $\alpha \in \mathrm{Aut}(L)$, then L can be reconstructed from the knowledge of α and a contour of L. A contour only contains leading symbols such that each cell orbit contains precisely one leading symbol. The diagram determines a Latin square L with $\alpha \in \mathrm{Aut}(L)$.

Example : Consider $\alpha = (1234)(56)(7)$, and observe that $\alpha \in \mathrm{Aut}(7)$, since it is an automorphism of the Latin square

6	7	5	1	4	2	3
2	5	7	6	3	1	4
5	3	6	7	2	4	1
7	6	4	5	1	3	2
1	4	3	2	7	5	6
3	2	1	4	6	7	5
4	1	2	3	5	6	7

. (2.2.1)

The contour of α is of the following form.

·	·	·	1	·	·	·
·	·	7	·	·	1	·
5	·	·	·	·	·	1
·	·	·	5	1	·	·
1	·	·	·	·	5	·
·	·	1	·	·	7	5
·	1	·	·	5	·	7

.

Then Stones, Vojtěchovský and Wanless [75] proved a generalization of Theorem 2.2.1, when α consists of an arbitrary number of cycles of the same length.

Theorem 2.2.9. *Suppose that $\alpha \in \mathcal{S}_n$ has precisely m nontrivial cycles, each cycle having the same length d. If α has at least one fixed point, then $\alpha \in \mathrm{Aut}(n)$ if and only if $n \leqslant 2md$. If α has no fixed points, then $\alpha \in \mathrm{Aut}(n)$ if and only if d is odd or m is even.*

Kerby and Smith [46] independently obtained the case of the following corollary when θ is an automorphism. The special case when all cycles have length two can be found in the proof of Lemma 4 in [55].

Corollary 2.2.10. *Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. Suppose $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ is such that the length of each cycle in α, β and γ is divisible by 2^a. Then $\theta \notin \mathrm{Atp}(n)$.*

Proof. Suppose $\theta \in \mathrm{Atp}(L)$ for some Latin square L. Define the strongly lcm-closed set $\Lambda = \{s \in \mathbb{N} : 2^{a+1} \nmid s\}$. Theorem 2.2.8 implies that L contains a subsquare M that admits an autotopism θ_M whose components have cycle lengths that are divisible by 2^a but not by 2^{a+1}. Hence the order of θ_M is $2^a x$ for some odd $x \geqslant 1$.

Since $2^{a+1} \nmid n$, the order of M is $2^a b$ for some odd $b \geqslant 1$. Also, M admits the autotopism $(\theta_M)^x$. But the components of $(\theta_M)^x$ each consist of b disjoint 2^a-cycles, so Theorem 2.2.9 implies that $(\theta_M)^x \notin \mathrm{Atp}(2^a b)$, giving a contradiction. □

The following theorem from [75] proves necessary and sufficient conditions for membership in $\mathrm{Aut}(n)$ for those $\alpha \in \mathcal{S}_n$ that consist of precisely two nontrivial cycles.

Theorem 2.2.11. *Suppose $\alpha \in \mathcal{S}_n$ consists of a d_1-cycle, a d_2-cycle and d_∞ fixed points. If $d_1 = d_2$ then $\alpha \in \mathrm{Aut}(n)$ if and only if $0 \leqslant d_\infty \leqslant 2d_1$. If $d_1 > d_2$ then $\alpha \in \mathrm{Aut}(n)$ if and only if all the following conditions hold:*

(i) d_2 divides d_1,

(ii) $d_2 \geqslant d_\infty$,

(iii) if d_2 is even then $d_\infty > 0$.

This theorem from [75] characterizes automorphisms α of Latin squares with precisely three nontrivial cycles of length.

Theorem 2.2.12. *Suppose that $\alpha \in \mathcal{S}_n$ has precisely three nontrivial cycles of lengths $d_1 \geqslant d_2 \geqslant d_3$. Let d_∞ be the number of fixed points of α. Then $\alpha \in \mathrm{Atp}(n)$ if and only if one of the following cases holds:*

(i) $d_1 = d_2 = d_3$ and (a) $d_\infty \leqslant 3d_1$ and (b) if d_1 is even then $d_\infty \geqslant 1$,

(ii) $d_1 > d_2 = d_3$ and (a) $d_1 \geqslant 2d_2 + d_\infty$, (b) d_2 divides d_1, (c) $d_\infty \leqslant 2d_2$, and (d) if d_2 is even and d_1/d_2 is odd then $d_\infty > 0$,

(iii) $d_1 = d_2 > d_3$ and (a) d_3 divides d_1, (b) $d_\infty \leqslant d_3$, and (c) if d_3 is even then $d_\infty > 0$,

(iv) $d_1 > d_2 > d_3$ and (a) $d_1 = \mathrm{lcm}(d_2, d_3)$, (b) $d_3 \geqslant d_\infty$, and (c) if d_1 is even then $d_\infty > 0$,

(v) $d_1 > d_2 > d_3$ and (a) d_3 divides d_2 which divides d_1, (b) $d_3 \geqslant d_\infty$, and (c) if d_3 is even then $d_\infty > 0$.

Using all above results Stones, Vojtěchovský and Wanless [75] determined $\mathrm{Atp}(n)$ for $n \leqslant 17$ establishing a number of necessary conditions for (α, β, γ) to be in $\mathrm{Atp}(n)$. We observe that they found if $(\alpha, \alpha, \alpha) \in \mathrm{Atp}(n)$ for general n, provided that either α has at most three cycles other than fixed points or that the non-fixed points of α are in cycles of the same length. In Chapter 3, we take a similar approach for autoparatopisms and find $\mathrm{Par}(n)$ for $n \leqslant 17$.

Kerby and Smith [45, 46] considered isomorphisms from an algebraic point of view. Stones [73] used the divisors of $\Delta(\theta)$ for isomorphisms θ, to determine the parity of the number of quasigroups for small orders.

McKay et al. [55] explain how to use nauty to find $\mathrm{Atp}(L)$, $\mathrm{Aut}(L)$ and $\mathrm{Par}(L)$ for a general Latin square L. Kotlar [48] established a new algorithm to find the autotopism group of a Latin square, based on the cycle decomposition of its rows. Using this algorithm he derived upper bounds for the size of autotopism groups. He improved this algorithm in [49]. Consequently he obtained a bound for the size of the autotopism group and showed that the bound is tight for Cayley tables of cyclic groups. For other bounds on the order of autotopism groups see [7] and for bounds on the order of individual autotopisms, see [58]. Also Kotlar proved that the computation time for the autotopism group of Latin squares that have two rows or two columns that map from one to the other by a permutation which decomposes into a bounded number of disjoint cycles, is polynomial in n. The evidence from [14] suggests that almost all Latin squares have the required property.

2.3 Latin squares with a unique subsquare or no subsquares

If a submatrix M of L is also a Latin square then M is called a subsquare of L. If L is a Latin square of order n, and M is a subsquare of order m with $1 < m < n$, then we call M a proper subsquare and say that L properly contains M. Every Latin square of order n has n^2 subsquares of order 1 and one subsquare of order n.

The following theorem is classical. For a proof see [8].

Theorem 2.3.1. *Let L be the Cayley table of a finite group G. Suppose H is a subgroup of G and $x, y \in G$. Then L has a subsquare of order $|H|$ in the rows indexed by xH and columns indexed by Hy. Moreover, every subsquare of L can be produced in this way by an appropriate choice of x, y and H.*

A subsquare of order 2 is called an intercalate. A Latin square without intercalates is said to be N_2 and a Latin square without proper subsquares is said to be N_∞. By Lagrange's theorem and Theorem 2.3.1 the Cayley table of any group of odd order is N_2. The only groups with N_∞ Cayley tables are the cyclic groups of prime order.

A *Steiner triple system* consists of a set of n distinct elements arranged into subsets each containing exactly three distinct elements and with the property that, if a and b are any two distinct elements of the set, there is one and only one element c such that a, b, c are all different and form a triple of the system.

In the process of constructing Latin squares without certain subsquares, two main problems have been considered.

The first problem is the existence of N_2 Latin squares for all $n \neq 2, 4$. This was asked by Kotzig, Lindner and Rosa [50] since they required a Latin square of order $(v+1)/2$ with at least one column no cell of which was contained in a subsquare of order 2 to construct a set of $(v+1)/2$ pairwise disjoint Steiner triple systems of order $v \equiv 3$ *or* $7 \mod 12$ and $v > 7$. Apparently N_2 Latin squares have this property and they could be used to construct sets of disjoint such Steiner triple systems.

The second problem is regarding the existence of N_∞ Latin squares. This was raised by Hilton (see [17]).

Heinrich [35] exhibits a complete solution to the first problem and then describes constructions for N_∞ latin squares, giving partial solution to the second. In both problems she uses mainly a modified product construction.

McLeish [59] pointed out that if A and B are N_2 Latin squares then so too is their direct product. According to Denniston [19] this provides a straightforward recursive construction for N_2 latin squares of all orders n, $n \neq 2, 4$, once N_2 Latin squares of order $8, 16, 32, 2k+1, 2(2k+1)$, and $4(2k+1)$, where $k \geqslant 1$, have been constructed.

Kotzig, Lindner and Rosa [50] began by constructing N_2 Latin squares for all $n \neq 2^a$ and then McLeish [59] gave constructions based on direct and generalised direct product which included the cases $n = 2^a$ for $a \geqslant 6$ and $a \neq 7, 8$ or 13. Then she produced N_2 Latin square of orders 2^7 and 2^8 using prolongation and hence constructed an N_2 Latin square of order 2^{13} by direct product. We can see that every Latin square of order 2 and 4 has an order 2 subsquare and so only the cases $n = 8, 16,$ and 32 remained. Denniston [19] showed (by computer search) that there are exactly three species of N_2 Latin squares of order 8. However, the first N_2 Latin square of order 8 (as shown in Fig 2.2) was constructed by Regener (and appears in Kotzig and Turgeon [51]). In that same paper Kotzig and Turgeon gave a general construction for N_2 Latin squares of order n provided $n \not\equiv 0 \mod 3$ and $n \not\equiv 3 \mod 5$, by a prolongation involving the projection of three transversals from the Cayley table of the cyclic group of order $n-3$. This included the cases $n = 16$ and 32, and so the problem was solved.

1	2	3	4	5	6	7	8
2	3	1	5	6	7	8	4
3	1	4	6	7	8	2	5
4	6	8	2	1	3	5	7
5	8	2	7	3	4	6	1
6	5	7	1	8	2	4	3
7	4	5	8	2	1	3	6
8	7	6	3	4	5	1	2

Figure 2.2:

Then McLeish [60] gave a direct construction for N_2 Latin squares of all orders $n \geqslant 12$, $n \neq 14$, 20 or 30. The construction consists of a prolongation involving the projection of transversals from the Cayley table of the cyclic group of order $n - s$ for suitably chosen n and s.

McLeish [60] constructed a quasigroup $M_{n,s}$ on the set $[1,n]$ defining a binary operation $\otimes$ in four "regions" R_1, R_2, R_3, R_4 as follows.

R_1 : For $a \in [n-s+1, n]$ and $b \in [1, n-s]$ select $a \otimes b \in [1, n-s]$ satisfying $a \otimes b \equiv 2b + a - 2 - \frac{s-1}{2} \mod n-s$.

R_2 : For $a \in [1, n-s]$ and $b \in [n-s+1, n]$ select $a \otimes b \in [1, n-s]$ satisfying $a \otimes b \equiv 2a + 3b - 4 - 3\frac{s-1}{2} \mod n-s$.

R_3 : For $a, b \in [1, n-s]$ there are three cases

(i) if $a \equiv b + j \mod n-s$ for $j \in [0, \frac{s-1}{2}]$ then $a \otimes b = n - s + 2j + 1$,

(ii) if $a \equiv b + j \mod n-s$ for $j \in [-\frac{s-1}{2}, -1]$ then $a \otimes b = n - s - 2j$,

(iii) Otherwise $a \otimes b \equiv 3b - a - 1(\mod n-s)$ and $a \otimes b \in [1, n-s]$.

R_4 : For $a, b \in [n-s+1, n]$ select $a \otimes b \in [n-s+1, n]$ which satisfies $a \otimes b \equiv a + b - n - 3 \mod s$.

Wanless [80] pointed out errors published with regard to the construction of N_2 squares in [60]. Accordingly, he corrected Theorem 5.1 in [60] as follows.

Theorem 2.3.2. *Suppose $M_{n,s}$ is a quasigroup on the set $[1,n]$, where $[1,n] = \{1, 2 \ldots, n-1, n\}$. Then $M_{n,s}$ is N_2 if and only if*

(i) either (a) $n \equiv 0 \mod 4$, $n > 3s - 11$ and $2n > 5s - 5$ or (b) $n \equiv 2 \mod 4$ and $n > 4s - 6$,

(ii) $n - s$ is not divisible by 3 or 5,

(iii) $s \equiv 1 \mod 4$ and $s > 1$.

Wolfe et al. [88] showed that there exists an N_2 Latin square of order n with an orthogonal mate if and only if $n \notin \{2, 4, 6, 8\}$.

It is easily proved that every Latin square of order 4 or 6 has a proper subsquare, and that all three of the N_2 Latin squares of order 8 are N_∞ Latin squares.

The first general result on the existence of N_∞ Latin squares were obtained by Heinrich [34] who proved that there is an N_∞ Latin square of order $n = pq$, $n \neq 6$, where p and q are distinct primes.

In 1982, Andersen and Mendelsohn [2] proved there exists an N_∞ Latin square of order n when n is divisible by a prime $\geqslant 5$. Then Maenhaut, Wanless and Webb [54] determined if n is odd and divisible by 3 then there exists an N_∞ Latin square of order n. Combining these two results we can see that N_∞ Latin squares exist for all odd n.

An N_∞ Latin square of order 12 was found by Gibbons and Mendelsohn after a computer search using simulated annealing. The square is shown in Fig 2.3.

The existence of N_∞ Latin squares of large orders of the form $2^a 3^b$ for $a \geqslant 1$ and $b \geqslant 0$ remains open. However, examples for all orders up to 256 were constructed in [77].

The existence of an N_∞ Latin square was observed by Rosa if there exists a perfect 1-factorization of the complete graph of $2n$ vertices, K_{2n}. The order of the Latin square is $2n-1$. The N_∞ Latin square L is defined by $L(i,j) = k$ if $i \neq j$ and $\{i,j\} \in F_k$, and $L(i,i) = i$ for a given perfect 1-factorization of K_{2n}, with vertices $1, 2 \ldots, 2n$, consisting

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

Figure 2.3:

of the 1-factors $F_1, F_2, \ldots, F_{2n-1}$, where edge $\{i, 2n\}$ is in F_i. Observe that if A has a proper subsquare B containing no cell of the main diagonal of A, then any two elements in B can yield a cycle of length at most twice the order of B, contradicting the fact that they correspond to a hamilton cycle. Since A is symmetric, if B has an entry on the main diagonal, then B is symmetric about the main diagonal and has odd order. It is easy to see that any two elements yield a cycle of length at most one more than the order of B, again a contradiction.

Note that while perfect 1-factorizations yield N_∞ Latin squares the converse is not true. There are three infinite families of perfect 1-factorizations of complete graphs known [11, 76]. They exist for K_n whenever n is twice a prime or 1 more than a prime.

In 1989, Seah and Stinson [72] found a perfect one-factorization of K_{40}. After that K_{52} was the smallest complete graph for which a perfect one-factorization was unknown, until the determination of a perfect one-factorization of K_{52} by Wolfe [87] in 2009. The smallest unsolved order is now 54. The following list represents some orders $2n$ for which sporadic perfect one-factorization of K_{2n} are known [1], [85].

> 16, 28, 36, 40, 50, 52, 126, 170, 244, 344, 530, 730, 1332, 1370, 1850, 2198, 2810, 3126, 4490, 6860, 11450, 11882, 12168, 15626, 16808, 22202, 24390, 24650, 26570, 29792, 29930, 32042, 38810, 44522, 50654, 51530, 52442, 63002, 72362, 76730, 78126, 79508, 103824, 148878, 161052, 205380, 226982, 300764, 357912, 371294, 493040, 571788, 1030302, 1092728, 1225044, 1295030, 2048384, 2248092, 2476100, 2685620, 3307950, 3442952, 4330748, 4657464, 5735340, 6436344, 6967872, 7880600, 9393932, 11089568, 11697084, 13651920, 15813252, 18191448, 19902512, 22665188.

Above we have discussed building N_∞ Latin squares from perfect 1-factorizations of complete graphs. It is also possible to build them using perfect 1-factorizations of complete bipartite graphs. See [10, 78, 86] for more details.

Next consider the following standard result regarding intersection of subsquares before we describe the Latin squares with unique subsquares.

Theorem 2.3.3. *The intersection of two subsquares is itself a subsquare. In particular,*

if N is an N_∞ subsquare and it meets another subsquare M in two or more entries, then $N \subseteq M$.

Wanless [79] investigates the class $\mathcal{U}$ of Latin squares which contain exactly one proper subsquare. He uses the notation $\mathcal{U}_{n,m}$ for the subset of $\mathcal{U}$ consisting of order n Latin squares with an order m subsquare. His motivation in the paper [79] is as an approach to the long standing open problem of the construction of N_∞ squares. Observe that the subsquare of any member of $\mathcal{U}$ must itself be an N_∞ square.

In this process of studying Latin squares with a unique subsquare, Wanless [79] introduces a procedure known as skip-shift prolongations as a special case of the prolongations discussed in Section 2.1 to construct Latin squares. He starts by defining a few terms. A subset S of $[1, k]$ is said to be *regular* if it corresponds to a congruence class modulo m for some $m < k$ (called the modulus of S) which divides k. So, for example, $\{2, 5, 8, 11, 14\}$ is a regular subset of $[1, 15]$ but not of $[1, 16]$.

A *skip square* is a Latin square L of some order $n > 1$ which for all i and j satisfies $L[i, j] \equiv L[1, 1] + s_r(i - 1) + s_c(j - 1) \mod n$ where s_r, s_c are integers which are relatively prime to n. We call s_r the row skip and s_c the column skip of L. Any Latin rectangle consisting of consecutive rows of a skip square is a skip rectangle. A skip square of particular note is C_n, obtained from $C_n[1, 1] = 1$ with skips $s_r = s_c = 1$. This is the Cayley table of the cyclic group of order n. In fact it is not hard to see that all skip squares of order n are isotopic to C_n.

Then Wanless proves the following results in [79].

Lemma 2.3.4. *Suppose L is a skip square of order n and that R is a $2 \times r$ submatrix of L. If R is a row cycle then it consists of regular columns and symbols in L. Conjugate results also hold.*

Lemma 2.3.5. *Suppose L is a skip square of order n and that S is an $s \times s$ submatrix of L for $s > 1$. Then S is a subsquare if and only if it consists of regular rows and columns (each with modulus n/s). The symbols in a subsquare will also be regular.*

Lemma 2.3.6. *A skip square is N_∞ if and only if it is of prime order.*

Lemma 2.3.7. *Let M be a skip-shift prolongation with parameters n and $s \geqslant 3$. Then $M \in U$ if and only if*

(i) M is an N_2 square,

(ii) R_D is an N_∞ square,

(iii) $f \leqslant \min\{s, n - 2s\}$ for all $f < n - s$ which divide $n - s$.

In [51] Kotzig and Turgeon give a construction they call $\tau_g(T)$ extension. Note that this is an example of skip-shift prolongation with the parameter $s = 3$. Then Wanless [79] gives the proof for the following result.

Theorem 2.3.8. *Let $\mathcal{K}_n$ denote the set of N_2 squares of order n which are constructible by the method of $\tau_g(T)$ extensions. The Kotzig-Turgeon squares $\mathcal{K}_n \subseteq \mathcal{U}_{n,3}$ whenever $n = p + 3$ for a prime $p \geqslant 7$, and otherwise $\mathcal{K}_n$ and $\mathcal{U}$ are disjoint.*

Further details of skip-shift prolongation can be found in [79].

Also Wanless [79] proved the following two lemmas about the size of the unique subsquare.

Lemma 2.3.9. $\mathcal{U}_{n,m} = \emptyset$ *unless* $2m + 1 \leqslant n$.

Proof. Suppose L is a Latin square of order n. It is well known that a proper subsquare of L cannot be of order exceeding $n/2$. This bound can only be achieved if L is the union of 4 disjoint subsquares, in which case it is certainly not in $\mathcal{U}$. □

Lemma 2.3.10. *Let M be a N_∞ square on the symbol set $[1, m]$ where $m + 1$ is a prime > 3. Suppose that $M[i, j] \neq ((i-j) \mod m+1)$ for all i, j. Then there exists $N \in \mathcal{U}_{2m+1,m}$.*

In light of Lemma 2.3.9 the squares constructed in Lemma 2.3.10 have the largest possible subsquare. For example, by this Lemma there exists a Latin square $N \in \mathcal{U}_{21,10}$ since Heinrich [34] has found a suitable N_∞ Latin square of order 10.

The species which Norton missed has a single intercalate and no larger subsquares. The square given in [70] represents the unique species of minimal order in $\mathcal{U}$. Also in [19] there is a catalogue of order 8 squares with at most one intercalate, which clearly includes all candidates for $\mathcal{U}$. For $n = 8$ there are only three species of N_2 squares and all are N_∞ squares, so in particular $\mathcal{U}_{8,3} = \emptyset$. Of the 14 species of order 8 squares with precisely one intercalate, the first and sixth in Denniston's list contain a single order 3 subsquare each, and no other subsquares are present. Hence $\mathcal{U}_{8,2}$ consists of the other 12 species.

For $n = 9$, a table of the number of subsquares in N_2 squares of order 9 may be found in [78]. From there we know that $\mathcal{U}_{9,3}$ consists of 46 species. Also Theorem 2.3.8 shows that there are arbitrarily large n for which $\mathcal{U}_{n,3} \neq \emptyset$.

Considering all of these facts Wanless [79] conjectured that $\mathcal{U}_{n,2} \neq \emptyset$ for sufficiently large n. We give a partial proof of this conjecture in Chapter 4, showing that it is true for $n \equiv 1, 5 \mod 6$. Note that Latin squares that are N_2 or lie in $\mathcal{U}$ are extremely rare. McKay and Wanless [56] showed that asymptotically almost all Latin squares of order n have at least $n^{3/2-\varepsilon}$ intercalates and the probability of having 0 or 1 intercalates is less than exponentially small. See [6, 36] for work on the question of the maximum number of intercalates possible.

2.4 Cycle switches

Cycle switching is defined as follows. Switching any cycle of a Latin square L, we get a different Latin square L'. Let r and s be two rows involved in a row cycle of L and C be the set of columns involved in the cycle. Then L' is defined by

$$L'_{ij} = \begin{cases} L_{sj} & \text{if } i = r \text{ and } j \in C, \\ L_{rj} & \text{if } i = s \text{ and } j \in C, \\ L_{ij} & \text{otherwise.} \end{cases}$$

The similar definition for columns if c and d are relevant columns and R is the set of rows involved in the column cycle is

$$L'_{ij} = \begin{cases} L_{id} & \text{if } j = c \text{ and } i \in R, \\ L_{ic} & \text{if } j = d \text{ and } i \in R, \\ L_{ij} & \text{otherwise.} \end{cases}$$

Switching a symbol cycle on two symbols k_1 and k_2 is obtained by replacing every occurrence of k_1 in the cycle by k_2 and vice versa (see [82] for examples).

It is clear that cycle switches do not connect the whole space of Latin squares. For example an atomic Latin square (see [11, 53, 83] for definitions and properties) can never be converted to a non atomic Latin square by cycle switching. However Pittenger [69] introduced a set of simple moves (trades) that do connect all Latin squares of a given order. In design theory terms, Pittenger moves and cycle switches are based on trades. When two entries are swapped then it is easy to keep the Latin property by completing a cycle switch. The entries which end up being changed form a trade, as do the entries which replace them.

Cycle switching has an important role in producing new Latin squares from old. This practise has been done with various terminology by many mathematicians. Norton [62] dealt primarily with intercalates and referred to "intercalate reversals". Parker [68] "turned" intercalates in an order ten square without transversals to create a square with 5504 transversals and 12265168 orthogonal mates [53]. Elliot and Gibbons [22] used cycle switches, which they referred to as "rotations", in a simulated annealing approach to constructing N_∞ Latin squares. Jacobson and Matthews [38] call the operation a "cycle swap", whereas Pittenger [69] calls a symbol cycle switch a "name-change". It is obvious then, that cycle switching is useful when trying to enumerate Latin squares, or when trying to build, by local improvement, Latin squares with specific desirable properties.

The number of Latin squares increases very quickly with the order of the square, even when limited to special classes. Hence we should have an efficient method to store them in a catalogue. Cycle switching gives a way to accomplish this task. Accordingly we use a chain to store Latin squares. In a chain, only the first square is stored and for subsequent squares, instructions are stored as to how to make the square from its predecessor. In the best possible situation these instructions give only a single cycle switch. To designate a cycle switch requires significantly less space than it takes to store a new square. For example, a row cycle can be specified by identifying two rows and one column. Performing the cycle switch may also be quicker than loading a new square. But we face two new problems in this approach. The first is how to decide on an order for the catalogue which makes each square similar to its predecessor. The second problem is that on average half the catalogue must be processed in order to get to a random element. Many construction methods will automatically create squares in a suitable order for the first problem. The second problem can be eliminated by breaking the catalogue into a number of smaller chains. However it is possible to avoid both the problems by introducing a more general data structure such as a tree instead of the chain. We use a tree with the edges still corresponding to cycle switches. It should be easy to make a tree with small radius to store a large number of Latin squares.

Next we focus on a study of graphs which model how Latin squares are related by cycle

switches. Such graphs are known as switching graphs. Vertices of these switching graphs are sets of Latin squares and there exists an edge between two sets if a member of the first set can be turned into some member of the second set by a cycle switch. Since cycle switches can be combined to produce any isotopy, but in general cannot be used to take conjugates of a square, the most natural classes of squares to use as vertices are the isotopy classes, although it is also considered in [81] what happens when we use species as vertices.

Suppose M is an intercalate of a Latin square L. Then M can be *turned* by swapping two symbols of M as follows.

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \qquad \leftrightarrow \qquad \begin{bmatrix} b & a \\ a & b \end{bmatrix}$$

Turning an intercalate is a special type of cycle switch [81] which is, in turn, a special type of Latin trade [13]. Also this is called an intercalate switching.

Norton [62] is one of the first mathematicians who used cycle switching. He introduced the word "intercalates" for subsquares of order 2 and the phrase "generalized intercalate" for latin subrectangle. He switched his intercalates and generalized intercalates to change the structure of Latin square to enumerate the species of order seven. He found all of the Latin squares which could be generated by switching intercalates, one at a time, of any Latin square of order 7. The process could then be iterated from the new square. Eventually this process must stop creating new species, at which point we have what Norton called a domain of species. Norton defined as domain the set of a species obtained by cycle switching from a given species. He notes that cyclic group tables of prime order will be a domain on their own. We know that they are atomic. He knew only two N_2 Latin squares of order 7, which clearly must be domains on their own.

Then he computed manually an entire family of 144 species of Latin square containing intercalates. His effort came close to a complete catalogue together with the two N_2 species, given that it included 146 of the 147 species. A representative of the missing species was first pointed out by Sade [70]. The following is a semisymmetric representative of that missing species

$$\begin{array}{|ccccccc|} \hline 1 & 2 & 4 & 5 & 6 & 7 & 3 \\ 2 & 1 & 7 & 3 & 4 & 5 & 6 \\ 7 & 4 & 5 & 1 & 3 & 6 & 2 \\ 3 & 5 & 2 & 6 & 1 & 4 & 7 \\ 4 & 6 & 3 & 2 & 7 & 1 & 5 \\ 5 & 7 & 6 & 4 & 2 & 3 & 1 \\ 6 & 3 & 1 & 7 & 5 & 2 & 4 \\ \hline \end{array} \tag{2.4.1}$$

The Latin square has only a single intercalate and when that intercalate is turned the resulting Latin square is in the same species. Hence this Latin square is a *self-switching* square in the terminology of [62]. The name self-switching indicates that there are intercalates but when any of them is turned, the result is in the same species as the initial Latin square.

Norton's basic observations are useful in writing programs as well as providing a lot of data with which to check the results. He noted that switching Hamiltonian cycles never changes the isotopy class. He also argued that if a pair of rows, say, splits into just two cycles then we usually only need to try switching one of those cycles since switching the other will give an isotopic result.

Norton also pointed out the following description regarding 4-cycles in switching graphs. Let γ and γ' be two disjoint cycles in L_1 which can be switched. Suppose further, that switching γ produces a square L_2, switching γ' produces a square L_3 and switching γ and γ' produces a square L_4. Since γ and γ' are disjoint we must also get L_4 if we start with L_1 and switch γ' then γ. If L_1, L_2, L_3 and L_4 represent distinct vertices then the result will be a 4-cycle on those four vertices. The point is that disjoint cycles can be switched independently. The final result will not depend on the order in which switching took place, but the intermediate stages may.

If a permutation $\alpha \in \mathcal{S}_n$ can be written as a product of an even (odd) number of transpositions, then α is called an even (odd) permutation and the number, modulo 2, of factors in this product is defined to be the parity of the permutation.

Let r, c, s be any row, any column and any symbol respectively. Then the row permutation σ_r corresponding to row r, the column permutation σ_c corresponding to column c and the symbol permutation σ_s corresponding to symbol s are from $[n]$ to $[n]$ and defined by $\sigma_r(j) = L_{rj}$, $\sigma_c(i) = L_{ic}$ and $\sigma_s(i) = j$, where $L_{ij} = s$ respectively.

The row parity of a Latin square L is the sum, modulo 2, of the parities of the permutations corresponding to the rows of L. Similarly, the column parity of L is the sum, modulo 2, of the parities of the permutations corresponding to the columns of L and the symbol parity of L is the sum, modulo 2, of the parities of the permutations corresponding to the symbols of L. As parastrophy permutes rows, columns and symbols it naturally permutes the row, column and symbol parities as well. For example, the column parity of L is the row parity of the transpose of L.

The row and column parities have been studied in pursuit of what is known as the Alon-Tarsi conjecture. Suppose a Latin square L of order n belongs to the set A_n if L has an odd number of rows and columns that are odd permutations, otherwise it belongs to A_n^C. By the Alon-Tarsi conjecture, when n is even the number of Latin squares of A_n is not equal to the number of Latin squares of A_n^C. It is straightforward to verify that for odd orders these two numbers are equal. Fundamental to the Alon-Tarsi conjecture is the observation that row, column and symbol parities are isotopy invariants for squares of even order, but not for squares of odd order. More generally we have:

Proposition 2.4.1. *Switching a row cycle of length l reverses the column and symbol parities if and only if l is odd, but never changes the row parity. Switching a column cycle of length l leaves the column parity unchanged and reverses the row and symbol parities if and only if l is odd. Switching a symbol cycle of length l leaves the symbol parity unchanged and reverses the row and column parities if and only if l is odd.*

Proof. Suppose that R is a row cycle of length l between the rows r_1 and r_2. To switch R we multiply the row permutation corresponding to r_1 by some permutation σ and multiply the row permutation corresponding to r_2 by the inverse permutation σ^{-1}. Since σ and σ^{-1} have the same parity we either change the parity of both rows or leave them both the same. Either way, the row parity is unchanged. Each of the l columns and l symbols involved in R has its corresponding permutation multiplied by a single transposition when R is switched. Hence the column and symbol parties both change by l modulo 2. □

So far in this section we described the applications of switches related to Latin squares. Now we will explain more applications of switches described in [65].

In the study of discrete structures in combinatorics, there is an issue of whether two given structures are the same. Though the concept of isomorphism was introduced to handle this issue there is still much work to be done for the related problems of existence, enumeration and classification of combinatorial structures.

Östergård's motivation in [65] is to give a precise definition for a local transformation with variants for codes, designs, and related combinatorial structures. Using the definition of this transformation, termed switching, a variety of earlier methods and results for different structures can be unified.

In his survey paper [65], switching of various types of structures is considered, starting from error correcting codes and proceeding via constant weight codes, designs, equidistant codes and group divisible designs, (in particular, Latin squares) to covering codes.

Since the transformations switching and switches do not alter the basic parameters of a combinatorial structure, we can use them to obtain any structure with given parameters from any other structure, which is not useful in practice. So it is usual to consider some natural restricted class of transformation. In full generality the definition of switches allows an arbitrary transformation.

A binary *word* is a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, and a binary *code* is a nonempty set of (code) words $C \subseteq \mathbb{Z}_2^n$. The (Hamming) distance between two words, $\mathbf{x}$ and $\mathbf{y}$, is the number of coordinates in which they differ and is denoted by $d_H(\mathbf{x}, \mathbf{y})$. The minimum distance of the code C is

$$d(C) := \min\{d_H(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

A code $C \subseteq \mathbb{Z}_2^n$ with M codewords and minimum distance d is traditionally called an (n, M, d) *error-correcting code*. For a given n and d the largest possible value of M such that an (n, M, d) code exists is denoted by $A(n, d)$ and the corresponding codes are said to be optimal. To find $A(n, d)$ is one of major problems in coding theory. A code with odd minimum distance can be extended by adding a parity check bit to increase the minimum distance by 1, that is

$$A(n, 2d - 1) = A(n + 1, 2d).$$

Two codes are said to be equivalent if one can be coverted into the other by permuting the coordinates and or the values within each coordinates. The *automorphism group* of the code, $\mathrm{Aut}(C)$ is the set of all such permutations from a code C onto itself.

The concept of switching for error-correcting codes is introduced as follows.

Definition (1): A switch of a binary code is a transformation that concerns exactly one coordinate and keeps the studied parameter of the code unchanged.

For error-correcting codes, calculations of all possible switches of a given code has been described in [65].

A code is said to be a constant weight code if each codeword has the same weight, where the (Hamming) weight of a word is the number of non-zero coordinates. The notation $A(n, d, w)$ is used to represent the largest size of a code with length n, minimum distance d, and constant weight w.

Definition 1 decreases or increases the weight of a codeword by 1. In this case we have to alter at least two coordinates to use switching. More details can be found in [65].

Definition 2 : A switch of a constant weight code is a transformation that concerns exactly two coordinates and keeps the studied parameter of the code unchanged.

Next we discuss combinatorial designs. These are related to constant weight codes in several ways.

Suppose X is a finite set of v points and $\mathcal{B}$ is a multiset of k-subsets of X, known as blocks. If every t-subset of X occurs in exactly λ blocks, then a pair $(X, \mathcal{B})$ is said to be a $t-(v,k,\lambda)$ design. The order of the design is the number of points v. The number of blocks, b, as well as the number of blocks in which a point occurs, r, in a $t-(v,k,\lambda)$ design can be determined as

$$b = \lambda \binom{v}{t} \Big/ \binom{k}{t}, \qquad r = bk/v.$$

A design with $v = b$ is said to be symmetric.

Two designs are isomorphic if one of the designs can be mapped onto the other by a permutation of the points. All such mappings from a design $\mathfrak{D}$ on to itself form the automorphism group of the design, $\mathrm{Aut}(\mathfrak{D})$.

Designs $t-(v,k,1)$ with an optimal code of length v, constant weight k, and minimum distance $2(k-t+1)$ are known as Steiner systems. The smallest possible nontrivial parameters are $k = 3$, $t = 2$. Such Steiner triple systems exist exactly for $v \equiv 1, 3 \mod 6$.

The Pasch Configuration or quadrilateral is a collection of four triples isomorphic to $\{a,b,c\}, \{a,y,z\}, \{x,b,z\}, \{x,y,c\}$. The Pasch Configuration is the smallest trade that can occur in a Steiner triple system. If T_1 is the collection $\{a,b,c\}, \{a,y,z\}, \{x,b,z\}$ and $\{x,y,c\}$ then, it can be replaced by the collection T_2, $\{x,y,z\}, \{x,b,c\}, \{a,y,c\}$ and $\{a,b,z\}$. Crucially T_2 contains precisely the same pairs as T_1. This transformation is known as a Pasch switch and when applied to a Steiner triple system gives another, usually non-isomorphic, Steiner triple system.

The existence of a switching class of Steiner triple systems of order 15 that contains 79 isomorphism classes was found by Fisher [28]. But the total number of isomorphism classes of Steiner triple systems of order 15 is 80. Hence there is obviously one isomorphism class that is unaffected by Pasch switches. A Steiner triple system is anti-Pasch if it does not contain the Pasch Configuration. There is no anti-Pasch Steiner triple system of order 7 or 13. For every other $v \equiv 1, 3 \mod 6$, an anti-Pasch Steiner triple system of order v is known to exist [5, 31, 33].

Steiner triple systems with exactly one Pasch configuration before and after the switch is carried out have been studied in [30] and are termed twin systems. Twin systems reside in switching classes of size 1 or 2, depending on whether the two designs are isomorphic or not. The self-switching Latin squares that we study in Chapter 4 are analogous to twin systems.

We next describe operations on Steiner triple systems that are commonly called cycle switches. Suppose the switch is carried out with respect to two points s and t in a Steiner triple system $(X, \mathfrak{B})$ and let $\{s,t,u\} \in \mathfrak{B}$ be the unique block that contains the pair $\{s,t\}$. Let $X' = X \setminus \{s,t,u\}$. Suppose P and Q are the set of blocks in $\mathfrak{B} \setminus \big\{\{s,t,u\}\big\}$ that contain s and t, respectively. Both P and Q partition X' into pairs. These partitions correspond to perfect matchings in a graph with vertices X'. The union of two perfect matchings is a set of even length cycles. There is one cycle for each minimal switch. To switch we simply swap, for each edge in a cycle, whether the edge occurs in a triple with s or with t.

The (cycle) switching classes for Steiner triple systems of order at most 19 have been determined [32, 41]. There is exactly one switching class for each admissible set of parameters. Determination of the switching classes of the 11084874829 isomorphism classes of Steiner triple systems of order 19, classified in [43], required a major computational effort [41].

Next we will discuss equidistant codes. When switching is carried out in these codes, there are two different types of applications such as with and without restrictions to constant weight.

First we consider constant weight equidistant codes. Let $G = (V, E)$ be a graph with one vertex for each codeword with $m/2$ 1s in the particularized coordinates and edges between vertices whenever the distance within the particularized coordinates between the corresponding codewords differs from $m/2$. The graph G is complete when $4 \nmid m$. In this situation switching can produce an inequivalent code whenever $m \geqslant 4$. Note that this technique applies as such to unrestricted codes. Denniston [20] used $m = 4$ to apply switching to symmetric $2 - (25, 9, 3)$ designs. Also Jungnickel and Tonchev [39, 40] considered not only switching of symmetric designs but certain other closely related designs.

The next application is an example of equidistant unrestricted codes. A Hadamard matrix of order n is an $n \times n$ matrix H over $\{-1, 1\}$ such that $HH^T = nI$. If a Hadamard matrix of order n exists, then $n = 1$ or 2 or $n \equiv 0 \mod 4$.

Two Hadamard matrices are said to be equivalent if one can be obtained from the other by permuting rows, and changing the sign of some rows or permuting columns, and changing the sign of some columns.

A Hadamard matrix H forms an equidistant $(n, n, n/2)$ code over $\mathbb{Z}_2$ if the symbol -1 is replaced by the symbol 0 in H. Using this method Orrick [67] applied switching to Hadamard matrices with $m = 4$. Then switching is effective when there are four rows of the Hadamard matrix of the form

$$\left[\begin{array}{cccc|cccc|cccc|ccc} 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 & 1\dots & 1 \\ 1 & 1 & \dots & 1 & 1 & 1 & \dots & 1 & - & - & \dots & - & - & -\dots & - \\ 1 & 1 & \dots & 1 & - & - & \dots & - & 1 & 1 & \dots & 1 & - & -\dots & - \\ 1 & 1 & \dots & 1 & - & - & \dots & - & - & - & \dots & - & 1 & 1\dots & 1 \end{array}\right] \tag{2.4.2}$$

If a graph G is constructed with respect to (2.4.2) then there are four connected components in G and switching can be carried out in each component of G. A necessary condition to construct a Hadamard matrix containing four rows of the form (2.4.2) is 8 divides n. Also Orrick [67] found very effective transformation which does not have this switching framework when n is not divisible by 8.

The number of equivalence classes of Hadamard matrices is 1 for all admissible orders up to 12; there are $5, 3, 60$, 487, and 13710027 equivalence classes of Hadamard matrices of orders $16, 20, 24$, 28 and 32, respectively [47]. Orrick [67] showed that the number of switching classes of Hadamard matrices is 1 for order 16 and 9 for order 24; if transpose of matrices are also considered, then the number of equivalence classes of order 24 is reduced to 2. The transformation carried out in [67] for Hadamard matrices of order 20 and 28 gives 1 and 2 switching classes, respectively, for these parameters.

Perhaps most interestingly, Orrick used his switching to find 18292717 equivalence classes of Hadamard matrix of order 36. So even though complete enumeration is not

yet possible we do know that there are more equivalence classes of order 36 than there are of order 32. This is a notable achivement for switching since there is a dip from order 16 to order 20 and it was thought the same may happen from order 32 to 36.

Orrick determined it is possible to explain the method used by Denniston [20] for $2-(25,9,3)$ designs in the same framework and describes possible generalization in [67]. Also he has discussed the relationship between a doubling construction which produces Hadamard matrices of order $2n$ from matrices of order n and switching in [67].

In recent work Ó Catháin, and Wanless [63] have shown that any trade in a Hadamard matrix of order n must change at least n entries. The switching (2.4.2) is a non-trivial example for which this bound is tight.

Switching of D-optimal matrices, which are structures closely related to Hadamard matrices, has been studied in [66].

Next we describe group divisible designs. A (k,λ)-GDD of type $g_1^{a_1}g_2^{a_2}\dots g_p^{a_p}$ is a triple $(X,\mathfrak{g},\mathfrak{B})$, where X is a set of $\sum_{i=1}^{p} a_i g_i$ points, $\mathfrak{g}$ is a partition of X into a_i subsets of size g_i for $1 \leqslant i \leqslant p$ (called groups), and $\mathfrak{B}$ is a collection of k-subsets (blocks) of points, such that every 2-subset of points occurs in exactly λ blocks or one group, but not both. If $\lambda = 1$, we write k-GDD instead of $(k,1)$-GDD. Basic properties of group divisible designs can be found in [61].

Steiner triple systems and Latin squares are examples for 3-GDDs. A Steiner triple system of order v is a 3-GDD of type 1^v and a Latin square of order n is a 3-GDD of type n^3. Latin squares belong to a same species if their 3-GDDs are isomorphic.

As in the case of Steiner triple systems, the auxiliary graph obtained in determining possible switches for (3-GDDs related to) Latin squares consists of cycles only; depending on the origin of the group where the two particularized points reside, the terms row cycle, column cycle, and symbol cycle can be used.

As we discussed before some mathematicians have used switching to study Latin squares. Norton [62] and Parker [68] studied Latin squares of order 7 and 10 respectively using switching. Also Wanless investigated switching classes of Latin squares up to order 8. By [41], it is possible to find the number of cycle switching classes of the 19270853541 species of Latin squares of order 9 although nobody has yet done so.

In designs, transformations that are more general than switches, called trades, were briefly mentioned. Such general transformations have been considered also for Latin squares; these are then called Latin trades [4, 44, 84].

Clearly, switching can be considered for any k-GDDs. Switching results for the 3-GDDs of type $(2n-1)^1 1^{2n}$, which correspond to 1-factorizations of the complete graph K_{2n}, have recently been obtaining in [85]. Interestingly, there were no examples for small orders of switching classes of size 1 in cases when switchings were available. This contrast with the twin Steiner triple systems and self-switching Latin squares.

2.5 Near-autotopisms of Latin squares

As we mentioned in the previous section, Norton [62] gave an exhaustive account of the Latin squares of order 7 obtained using intercalate switches. However, Sade [70] later found

that a single species of Latin squares was missing from Norton's list. He gave the species representative of Latin square (2.4.1).

In this example, the Latin square L has a unique intercalate M, and turning M, we get a new Latin square L'. Observe that swapping 1 and 2 in L^T we have the same Latin square L'. Hence, L and L' are in the same species.

Cavenagh and Stones [15] determine a necessary and sufficient condition for α to be a near-automorphism when α has the cycle structure $(n-2)^1 2^1$, where $n \geqslant 0$ and $n \equiv 2 \mod 4$. Their main purpose in [15] is to prove the following theorem.

Theorem 2.5.1. *For all $n \geqslant 2$ except $n \in \{3, 4\}$ there exists a Latin square L of order n that contains an intercalate M, which when turned produces a Latin square L' isomorphic to L.*

The following Lemma [15] proves that whether or not α is a near-automorphism of some Latin square depends only on the cycle structure of α.

Lemma 2.5.2. *Let $\alpha \in \mathcal{S}_n$ be a near-automorphism of a Latin square L and let $\beta \in \mathcal{S}_n$. Then $\beta^{-1}\alpha\beta$ is a near-automorphism of $L\beta$.*

Proof. $\text{dist}(L\beta, L\beta(\beta^{-1}\alpha\beta)) = \text{dist}(L\beta, L\alpha\beta) = \text{dist}(L, L\alpha) = 4.$ □

Two permutations are conjugate if and only if they have the same cycle structure. Since α and $\beta^{-1}\alpha\beta$ are conjugate, Lemma 2.5 implies that if two permutations $\alpha, \gamma \in \mathcal{S}_n$ both have the same cycle structure, then α is a near-automorphism of some Latin square if and only if γ is a near-automorphism of some Latin square.

A natural permutation to consider as a candidate for being a near-automorphism is α with the cycle structure $(n-2)^1 2^1$. In [75] it was discovered that α of this form cannot be an automorphism of any Latin square except when $n \in [1, 2]$. But, as we will see, in some cases α can be a near-automorphism.

A *partial Latin square* of order n is an $n \times n$ array $P = (p_{ij})$ of $n+1$ symbols $Q \cup \{\cdot\}$, where $|Q| = n$, such that each symbol in Q occurs at most once in each row and at most once in each column. We say P_{ij} is *undefined* if $p_{ij} = \cdot$. We say that a Latin square $L = (l_{ij})$ is a completion of a partial Latin square $P = (P_{ij})$ if, for all $i, j \in [n]$, either $p_{ij} = l_{ij}$ or p_{ij} is undefined. If α is a permutation of Q such that $\alpha(p_{ij}) = p_{\alpha(i)\alpha(j)}$ for all $i, j \in [n]$ for which $p_{ij} \in Q$, then α is called an automorphism of P.

An orthomorphism of $\mathbb{Z}_n$ is a permutation $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ such that $i \to \sigma(i) - i$ is also a permutation. A partial orthomorphism is an injection $\sigma : S \to \mathbb{Z}_n$ for some $S \subset \mathbb{Z}_n$ such that $i \to \sigma(i) - i$ is also an injection. We say σ has deficit $d := n - |S|$. We use U to denote the range of σ and $V = \{\sigma(i) - i : i \in S\}$. Let $\bar{S} = \mathbb{Z}_n \setminus S$ and $\bar{U} = \mathbb{Z}_n \setminus U$ and $\bar{V} = \mathbb{Z}_n \setminus V$.

Links between partial orthomorphisms of $\mathbb{Z}_n$ and automorphisms of Latin squares are well known, and have been studied in [21, 74, 82]. Cavenagh and Stones [15] have studied the links between partial orthomorphisms of $\mathbb{Z}_n$ and near-automorphisms of Latin squares and proved the following result. Here they use the index set $Q = \{x, y\} \cup \mathbb{Z}_n$.

Theorem 2.5.3. *Suppose n is even and $n \geqslant 4$. There exists a Latin square of order $n+2$ that admits the near-automorphism $\alpha := (x\ y)(0, 1 \ldots n-1)$ if and only if there exists a partial orthomorphism $\sigma : S \to U$ of $\mathbb{Z}_n$ of deficit 2 that satisfies the following three conditions, where $\bar{S} = \{s_1, s_2\}$ and $\bar{U} = \{u_1, u_2\}$ and $\bar{V} = \{v_1, v_2\}$.*

(i) $s_1 \equiv s_2 \mod 2$,

(ii) $u_1 \equiv u_2 \mod 2$,

(iii) $v_1 \equiv v_2 \mod 2$.

Cavenagh and Stones [15] found necessary and sufficient conditions for there to exist some Latin square of order $n+2$ that admits a near-automorphism α with the cycle structure $n^1 2^1$. They use the convention that $\mathbb{Z}_0 = \emptyset$.

Theorem 2.5.4. *Suppose that α has the cycle structure $n^1 2^1$ where $n \geqslant 0$. Then α is a near-automorphism of some Latin square L of order $n+2$ if and only if $n \equiv 0 \mod 4$ and $n \neq 4$.*

Finally they proved [15] the following result.

Theorem 2.5.5. *Let L be a Latin square that admits the near-automorphism α. Let M be the submatrix formed by the rows and columns of L whose indices are fixed by α. Then M is a (possibly empty) subsquare of L. Moreover, L and αL agree in M.*

Chapter 3

Autoparatopisms of Latin squares

3.1 Introduction

Symmetry is one of the most important concepts in mathematics. In this chapter we investigate what symmetries a Latin square may have. See [75] for a survey of numerous earlier results on this topic, stretching all the way back to Euler's seminal work. In particular, we note that symmetry has played a critical role in enumerations such as [25, 37, 55].

The primary aim of this chapter is to better understand $\mathrm{Par}(n)$. We establish a number of necessary conditions for σ to be in $\mathrm{Par}(n)$. We find, by computation, that these necessary conditions are sufficient when $n \leqslant 17$. The analogous task for $\mathrm{Atp}(n)$ was carried out in [75].

3.2 Some basic tools and terminology

3.2.1 Cycle structures

Every $\alpha \in \mathcal{S}_n$ decomposes into a product of disjoint cycles, where we consider fixed points to be cycles of length 1. We say α has the *cycle structure* $c_1^{\lambda_1} \cdot c_2^{\lambda_2} \cdots c_m^{\lambda_m}$ if there are λ_i cycles of length c_i in the unique cycle decomposition of α and $c_1 > c_2 > \cdots > c_m \geqslant 1$. Hence $n = \sum c_i \lambda_i$. If $\lambda_i = 1$, we may write c_i instead of c_i^1 in the cycle structure. If i is a point moved by a particular cycle C then we say that i is in C and write $i \in C$. We use $o(C)$ to denote the length of a cycle C (in other words, the size of its orbit). We write $o_\alpha(i) = c$ to denote that i is in some cycle C of the permutation α for which $o(C) = c$.

A permutation in $\mathcal{S}_n$ is *canonical* if (i) it is written as a product of disjoint cycles, including 1-cycles corresponding to fixed points, (ii) the cycles are ordered according to their length, starting with the longest cycles, (iii) each c-cycle is of the form $(i, i+1, \ldots, i+c-1)$, with i being referred to as the leading symbol of the cycle, and (iv) if a cycle with leading symbol i is followed by a cycle with leading symbol j, then $i < j$. For each possible cycle structure there is precisely one canonical permutation with that cycle structure and there is a unique way to represent it as a product of disjoint cycles.

The task of understanding $\mathrm{Par}(n)$ is substantially simplified by the following two results.

Theorem 3.2.1. *Suppose σ_1 and σ_2 are conjugate in $\mathcal{P}_n$. If σ_1 is an autoparatopism of some Latin square then σ_2 is an autoparatopism of a (potentially) different Latin square.*

Proof. By assumption there exist $\tau \in \mathcal{P}_n$ such that $\sigma_2 = \tau^{-1}\sigma_1\tau$ and there is some Latin square L such that $\mathrm{dist}(L^{\sigma_1}, L) = 0$. Then,

$$\mathrm{dist}(L^{\tau\sigma_2}, L^\tau) = \mathrm{dist}(L^{\tau(\tau^{-1}\sigma_1\tau)}, L^\tau) = \mathrm{dist}(L^{\sigma_1\tau}, L^\tau) = \mathrm{dist}(L^{\sigma_1}, L) = 0.$$

Hence σ_2 is an autoparatopism of L^τ. □

In [75] the specialisation of Theorem 3.2.1 to autotopisms was used as the first step in studying which isotopisms are autotopisms of some Latin square. To assist a future similar classification of autoparatopisms and/or near-autoparatopisms we now have motivation to understand the conjugacy classes in $\mathcal{P}_n$. In the following, we will use $\nu_1 \sim \nu_2$ to denote that two permutations ν_1, ν_2 are conjugate in $\mathcal{S}_n$; in other words, ν_1 and ν_2 have the same cycle structure. Note also that in the next result we consider fixed points to be cycles (of length 1).

Theorem 3.2.2. *Suppose $\sigma_1 = (\alpha_1, \alpha_2, \alpha_3; \delta_1) \in \mathcal{P}_n$ and $\sigma_2 = (\beta_1, \beta_2, \beta_3; \delta_2) \in \mathcal{P}_n$. Then σ_1 is conjugate to σ_2 if and only if there is a length preserving bijection η from the cycles of δ_1 to the cycles of δ_2 with the following property: If η maps a cycle $(a_1 \cdots a_k)$ to $(b_1 \cdots b_k)$ then $\alpha_{a_1}\alpha_{a_2}\cdots\alpha_{a_k} \sim \beta_{b_1}\beta_{b_2}\cdots\beta_{b_k}$.*

Proof. First consider the case when $\sigma_2 = \tau^{-1}\sigma_1\tau$ for $\tau = (\gamma_1, \gamma_2, \gamma_3; \varepsilon) \in \mathcal{P}_n$. If $\delta_1 = \varepsilon$ then we are dealing with the familiar case of conjugacy of isotopisms (see, e.g. [75]) so $\alpha_i \sim \beta_i$ for $i = 1, 2, 3$. If $\delta_1 = (12)$ then

$$\sigma_2 = (\gamma_1^{-1}\alpha_1, \gamma_2^{-1}\alpha_2, \gamma_3^{-1}\alpha_3; (12))(\gamma_1, \gamma_2, \gamma_3; \varepsilon) = (\gamma_1^{-1}\alpha_1\gamma_2, \gamma_2^{-1}\alpha_2\gamma_1, \gamma_3^{-1}\alpha_3\gamma_3; (12)),$$

so $\beta_1\beta_2 = \gamma_1^{-1}\alpha_1\alpha_2\gamma_1 \sim \alpha_1\alpha_2$ and $\beta_3 = \gamma_3^{-1}\alpha_3\gamma_3 \sim \alpha_3$. The cases when $\delta_1 = (13)$ or (23) are similar. If $\delta_1 = (123)$ then

$$\sigma_2 = (\gamma_1^{-1}\alpha_1, \gamma_2^{-1}\alpha_2, \gamma_3^{-1}\alpha_3; (123))(\gamma_1, \gamma_2, \gamma_3; \varepsilon) = (\gamma_1^{-1}\alpha_1\gamma_2, \gamma_2^{-1}\alpha_2\gamma_3, \gamma_3^{-1}\alpha_3\gamma_1; (123)),$$

so $\beta_1\beta_2\beta_3 = \gamma_1^{-1}\alpha_1\alpha_2\alpha_3\gamma_1 \sim \alpha_1\alpha_2\alpha_3$. The case when $\delta_1 = (132)$ is similar. Thus in all cases consider so far, $\delta_1 = \delta_2$ and η can be taken to be the identity map.

Next consider the case when $\sigma_2 = \tau^{-1}\sigma_1\tau$ for $\tau = (\gamma_1, \gamma_2, \gamma_3; \delta_3) \in \mathcal{P}_n$ and $\delta_3 \neq \varepsilon$. Here we write $\tau = \tau_1\tau_2$ where $\tau_1 = (\gamma_1, \gamma_2, \gamma_3; \varepsilon)$ and $\tau_2 = (\varepsilon, \varepsilon, \varepsilon; \delta_3)$. Now $\sigma_2 = \tau_2^{-1}\tau_1^{-1}\sigma_1\tau_1\tau_2$ which is just $\tau_1^{-1}\sigma_1\tau_1$ conjugated by τ_2. Suppose $\tau_1^{-1}\sigma_1\tau_1 = (\nu_1, \nu_2, \nu_3; \delta_1)$, where the possible values of the ν_i are determined in the above discussion. Conjugating by τ_2 simply permutes the first 3 coordinates of the resulting σ_2, and conjugates its last coordinate by δ_3. Specifically, we have $\sigma_2 = (\nu_{1\delta_3^{-1}}, \nu_{2\delta_3^{-1}}, \nu_{3\delta_3^{-1}}; \delta_3^{-1}\delta_1\delta_3)$. Hence we can take η to map each cycle $(a_1a_2\cdots a_k)$ of δ_1 to $\big((a_1\delta_3)(a_2\delta_3)\cdots(a_k\delta_3)\big)$ and this must have the required properties.

It remains to show the "if" part of the theorem statement. Suppose that η exists. For brevity, we consider only the cases when $\delta_1 = (12)$ or (123) and η is the identity (all other cases can be handled as per the "only if" argument above).

First, suppose that $\delta_1 = (12)$, $\alpha_1\alpha_2 \sim \beta_1\beta_2$ and $\alpha_3 \sim \beta_3$. Then there exist $x, y \in \mathcal{S}_n$ such that $x^{-1}\alpha_1\alpha_2 x = \beta_1\beta_2$ and $y^{-1}\alpha_3 y = \beta_3$. Taking $\tau = (x, \alpha_1^{-1}x\beta_1, y; \varepsilon)$ we find that

$$\tau^{-1}\sigma_1\tau = (x^{-1}\alpha_1\alpha_1^{-1}x\beta_1, \beta_1^{-1}x^{-1}\alpha_1\alpha_2 x, y^{-1}\alpha_3 y; (12)) = (\beta_1, \beta_2, \beta_3; (12)) = \sigma_2$$

as required.

Second, suppose that $\delta_1 = (123)$ and $\alpha_1\alpha_2\alpha_3 \sim \beta_1\beta_2\beta_3$. Then there exist $x \in \mathcal{S}_n$ such that $x^{-1}\alpha_1\alpha_2\alpha_3 x = \beta_1\beta_2\beta_3$. Taking $\tau = (x, \alpha_1^{-1}x\beta_1, \alpha_3 x\beta_3^{-1}; \varepsilon)$ we find that

$$\tau^{-1}\sigma_1\tau = (x^{-1}\alpha_1\alpha_1^{-1}x\beta_1, \beta_1^{-1}x^{-1}\alpha_1\alpha_2\alpha_3 x\beta_3^{-1}, \beta_3 x^{-1}\alpha_3^{-1}\alpha_3 x; (123)) = (\beta_1, \beta_2, \beta_3; (123)) = \sigma_2$$

as required. □

It follows from the above two results that any autoparatopism $(\alpha, \beta, \gamma; \delta)$ is conjugate to an autoparatopism of the form $(\alpha, \beta, \gamma; \varepsilon)$, $(\varepsilon, \beta, \gamma; (12))$ or $(\varepsilon, \varepsilon, \gamma; (123))$. The first of these possibilities has been well studied in [75], so we will concentrate mostly on the second and third possibilities. Moreover, in these cases the only salient consideration is the cycle structures of β and γ. For this reason, we will often assume without loss of generality that these permutations are canonical.

3.2.2 Cell orbits

We now discuss a notion that proved useful for studying $\mathrm{Atp}(n)$ in [75]. In that work, the term *cell orbit* is used to describe the set of cells of a Latin square in an orbit induced by an autotopism. The concept is a useful one because the cell orbit is determined by the autotopism and is independent of the contents of the cells. The same property holds for autoparatopisms of the form $(\alpha, \beta, \gamma; (12))$, so we also discuss cell orbits in this case. Formally, suppose that $\sigma = (\alpha, \beta, \gamma; (12)) \in \mathrm{Par}(L)$ for some Latin square L. Then a cell orbit of σ on L is the projection onto the first two coordinates of an orbit under the action of σ on $O(L)$. In most cases, σ and L will be implied by context and we simply refer to "cell orbits".

Suppose L is a Latin square of order n. We start by considering the cell orbits of an autoparatopism $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$.

Lemma 3.2.3. *Suppose that $\beta = \beta_1\beta_2\cdots\beta_p$ is a canonical permutation with cycle structure $d_1 d_2 \cdots d_p$. Define M_{ij} to be the block of L consisting of rows with indices in β_i and columns with indices in β_j.*

(i) In each block M_{tt} where d_t is odd, there is one cell orbit with length d_t and there are $(d_t - 1)/2$ cell orbits with length $2d_t$.

(ii) In each block M_{tt} where d_t is even there are $d_t/2$ cell orbits with length $2d_t$.

(iii) If $s \neq t$ then there are $\gcd(d_s, d_t)$ cell orbits through $M_{st} \cup M_{ts}$, each with length $2\,\mathrm{lcm}(d_s, d_t)$. One half of each cell orbit lies in M_{st} and the other half lies in M_{ts}.

Proof. Suppose $1 \leqslant s, t \leqslant p$. The orbit of the cell (i, j) in the block M_{st} can be divided into two subsets A and B, where

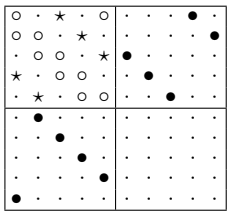
$$A = \{(i\beta^l, j\beta^l) : 1 \leqslant l \leqslant \mathrm{lcm}(d_s, d_t)\},$$
$$B = \{(j\beta^m, i\beta^{m-1}) : 1 \leqslant m \leqslant \mathrm{lcm}(d_s, d_t)\}.$$

Observe that $|A| = \operatorname{lcm}(d_s, d_t) = |B|$.

(i) Suppose $s = t$. Then A, B are subsets of the same block M_{tt}. Let $j = i\beta^q$ for some $q \in \{0, 1, \ldots, d_t - 1\}$. Then $j\beta^m = i$ when $m = d_t - q$. Then $i\beta^{m-1} = i\beta^{d_t-q-1} = j$ if $d_t - q - 1 = q$, that is, when $q = (d_t - 1)/2$. Note that such an integer q exists if and only if d_t is odd. Hence A and B coincide in the orbit of the cell $(i, i\beta^{(d_t-1)/2})$, so the length of that orbit is d_t. All cells in the set $\{(i, i\beta^{(d_t-1)/2}) : i \in \beta_t\}$ belong to the same cell orbit. The length of all other cell orbits is $2d_t$ when d_t is odd because A and B are disjoint. Similarly, when d_t is even all cell orbits of M_{tt} have length $2d_t$.

(ii) Now suppose $s \neq t$. Then $A \subseteq M_{st}$ and $B \subseteq M_{ts}$ and hence the length of each cell orbit is $2\operatorname{lcm}(d_s, d_t)$. □

Example: Let $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathcal{P}_n$ where β is the canonical permutation with cycle structure 5^2. Three different cell orbits of σ are represented by $\star$, $\circ$ and $\bullet$ in the following diagram.



Next we consider autoparatopisms of the form $(\varepsilon, \varepsilon, \gamma; (123))$. In this case the term "cell orbit" is no longer appropriate since all three coordinates in a triple affect its orbit. Hence we will simply refer to orbits.

Lemma 3.2.4. *Suppose that $\gamma = \gamma_1\gamma_2\cdots\gamma_p$ is a canonical permutation with cycle structure $d_1d_2\cdots d_p$. Define M_{ij} to be the block of L consisting of rows with indices in γ_i and columns with indices in γ_j.*

Suppose $i \in \gamma_a$, $j \in \gamma_b$, $k \in \gamma_c$ and let $\mathcal{O}$ be the orbit of the triple (i, j, k) under $\sigma = (\varepsilon, \varepsilon, \gamma; (123))$. If $|\{a, b, c\}| > 1$ then $\mathcal{O}$ has length $3\operatorname{lcm}(d_a, d_b, d_c)$, divided equally between three different blocks M_{ab}, M_{ca}, and M_{bc}. If $a = b = c$, then $\mathcal{O}$ lies entirely within M_{aa}. In this case, all orbits have length $3d_a$ except that there may be one orbit of length d_a when $d_a \not\equiv 0 \mod 3$.

Proof. Let (i, j, k) be a triple of L such that i, j, k are from cycles $\gamma_a, \gamma_b, \gamma_c$ respectively. The orbit of the triple (i, j, k) of L can be divided into 3 subsets A, B, C, where

$$A = \{(i\gamma^l, j\gamma^l, k\gamma^l) : 1 \leqslant l \leqslant \operatorname{lcm}(d_a, d_b)\}, \tag{3.2.1}$$

$$B = \{(k\gamma^m, i\gamma^{m-1}, j\gamma^{m-1}) : 1 \leqslant m \leqslant \operatorname{lcm}(d_a, d_b)\}, \tag{3.2.2}$$

$$C = \{(j\gamma^r, k\gamma^r, i\gamma^{r-1}) : 1 \leqslant r \leqslant \operatorname{lcm}(d_a, d_b)\}. \tag{3.2.3}$$

Observe that $|A| = |B| = |C| = \operatorname{lcm}(d_a, d_b)$ and $A \subseteq M_{ab}$, $B \subseteq M_{ca}$, $C \subseteq M_{bc}$. If $|\{a, b, c\}| > 1$ then M_{ab}, M_{ca} and M_{bc} are three different blocks. In this case the length of the orbit is $3\operatorname{lcm}(d_a, d_b)$.

Now suppose i, j, k are from the same cycle of γ and let the length of that cycle be d. In this case $M_{ab} = M_{ca} = M_{bc}$. Viewing A, B, C as orbits of σ^3 it becomes clear that either they all coincide or they are pairwise disjoint. If there exists an integer m satisfying

$k\gamma^m = i$, $i\gamma^{m-1} = j$ and $j\gamma^{m-1} = k$ then $i\gamma^{3m-2} = i$. If $3 \mid d$ then $d \nmid 3m-2$ so A, B, C are disjoint. If $3 \nmid d$ there is a unique m in the range $1 \leqslant m \leqslant d$ such that $d \mid 3m-2$. For that value of m, if $(i, i\gamma^{m-1}, i\gamma^{-m})$ is a triple of L it will have an orbit of length d. □

Example: Suppose $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(L)$ where the cycle structure of γ is $5^2 \cdot 1$. Two orbits of length 5 and 15 are shown in the following figure.

·	·	·	2	·	·	·	·	·	·	·
·	·	·	·	3	·	·	·	·	·	·
4	·	·	·	·	·	·	·	·	·	·
·	5	·	·	·	·	·	·	·	·	·
·	·	1	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·

·	·	6	·	·	·	·	·	3	·	·
·	·	·	7	·	·	·	·	·	4	·
·	·	·	·	8	5	·	·	·	·	·
9	·	·	·	·	·	1	·	·	·	·
·	10	·	·	·	·	·	2	·	·	·
·	·	·	·	2	·	·	·	·	·	·
3	·	·	·	·	·	·	·	·	·	·
·	4	·	·	·	·	·	·	·	·	·
·	·	5	·	·	·	·	·	·	·	·
·	·	·	1	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·

.

We call the cell orbits of length d_t in Lemma 3.2.3(i) and the orbits of length d_a in Lemma 3.2.4 *short orbits*. They will play a crucial role in our subsequent work.

3.2.3 Block diagrams and contours

This subsection defines block diagrams and contours which were introduced in [75] for constructing Latin squares with particular autotopisms.

Suppose $\theta = (\alpha, \beta, \gamma)$ is an autotopism of a Latin Square L, where $\alpha = \alpha_1 \cdots \alpha_a$, $\beta = \beta_1 \cdots \beta_b$ and $\gamma = \gamma_1 \cdots \gamma_c$ are canonical. We define M_{ij} to be the block of L with rows indexed by the points in α_i and columns indexed by the points in β_j. The *block diagram* for θ is a table in which the rows are indexed by α_1 to α_a, and columns are indexed by β_1 to β_b. The cells of the table correspond naturally to the blocks M_{ij} of L. We write $\gamma_k : f_k$ in the cell corresponding to block M_{ij} if every symbol in γ_k appears in M_{ij} precisely $f_k = f_k(i,j)$ times. If $f_k = 0$, we usually omit $\gamma_k : f_k$. A block diagram should satisfy the following properties.

1) $\sum_k o(\gamma_k) f_k(i,j) = o(\alpha_i) o(\beta_j)$ for $1 \leqslant i \leqslant a$ and $1 \leqslant j \leqslant b$.
2) $\sum_j f_k(i,j) = o(\alpha_i)$ for $1 \leqslant i \leqslant a$ and $1 \leqslant k \leqslant c$.
3) $\sum_i f_k(i,j) = o(\beta_j)$ for $1 \leqslant j \leqslant b$ and $1 \leqslant k \leqslant c$.

A *contour* is a tool introduced in [75] to define a Latin square with a particular autotopism. The idea there was to specify the content of exactly one cell in each cell orbit. The whole Latin square can then be recovered from knowledge of the autotopism. We will find it convenient to adapt this idea for autoparatopisms of the form $(\alpha, \beta, \gamma; (12))$. Again, a contour is a partial Latin square containing exactly one filled cell in each cell orbit. It is entirely routine to checking that a contour works, that is, produces a Latin square with the desired autoparatopism. In all cases, we leave this somewhat tedious checking to the reader when we describe a contour.

When constructing contours we always assume that permutations are canonical. For $1 \leqslant i \leqslant c$, let $t_k = 1 + \sum_{j<k} o(\gamma_j)$ be the leading symbol of γ_k. If $o(\gamma_k) > 1$ we specify

an orbit containing symbols from γ_k with the notation $C(i,j) = t_k$, which means that the contour contains symbol t_k in cell (i,j). If $o(\gamma_k) = 1$ we instead write $C(i,j) = \infty_{k'}$ where k' is used to index the fixed points of γ.

3.3 Basic conditions

In this section we determine important necessary conditions known as lcm conditions to find $\mathrm{Par}(n)$. The following lemma in [75] gives a necessary condition for membership in $\mathrm{Atp}(n)$.

Lemma 3.3.1. *Let $\theta = (\alpha, \beta, \gamma)$ be an autotopism of a Latin square L. If $o_\alpha(i) = a$ and $o_\beta(j) = b$, then $o_\gamma(L(i,j)) = c$, where $\mathrm{lcm}(a,b) = \mathrm{lcm}(b,c) = \mathrm{lcm}(a,c) = \mathrm{lcm}(a,b,c)$.*

We now give analogous conditions for autoparatopisms.

Lemma 3.3.2. *Let $\sigma = (\alpha, \beta, \gamma; (12))$ be an autoparatopism of a Latin square L. Suppose (i,j,k) is a triple of L. If $o_{\alpha\beta}(i) = a$ and $o_{\beta\alpha}(j) = b$ and $o_\gamma(k) = c$ then*

$$\mathrm{lcm}(2a, 2b) = \mathrm{lcm}(2a, c) = \mathrm{lcm}(2b, c) = \mathrm{lcm}(2a, 2b, c).$$

Proof. It is clear that $(i,j,k)\sigma^{2p} = (i(\alpha\beta)^p, j(\beta\alpha)^p, k\gamma^{2p})$, for any integer $p \geqslant 0$. Therefore, $(i,j,k)\sigma^{2\,\mathrm{lcm}(a,b)} = (i,j,k\gamma^{2\,\mathrm{lcm}(a,b)}) \in O(L)$. As $(i,j,k) \in O(L)$ we see that $k\gamma^{2\,\mathrm{lcm}(a,b)} = k$, so $c \mid 2\,\mathrm{lcm}(a,b)$. Which means that $\mathrm{lcm}(2a, 2b) = \mathrm{lcm}(2a, 2b, c)$. Similarly,

$$(i,j,k)\sigma^{\mathrm{lcm}(2a,c)} = (i(\alpha\beta)^{\mathrm{lcm}(2a,c)/2}, j(\beta\alpha)^{\mathrm{lcm}(2a,c)/2}, k\gamma^{\mathrm{lcm}(2a,c)}) = (i, j(\beta\alpha)^{\mathrm{lcm}(2a,c)/2}, k).$$

Therefore $b \mid (\mathrm{lcm}(2a,c)/2)$. It follows that $\mathrm{lcm}(2a,c) = \mathrm{lcm}(2a,2b,c)$. A similar argument proves that $\mathrm{lcm}(2b,c) = \mathrm{lcm}(2a,2b,c)$. □

Lemma 3.3.3. *Let $\sigma = (\alpha, \beta, \gamma; (123))$ be an autoparatopism of a Latin square L. Suppose (i,j,k) is a triple of L. If $o_{\alpha\beta\gamma}(i) = a$, $o_{\beta\gamma\alpha}(j) = b$ and $o_{\gamma\alpha\beta}(k) = c$, then*

$$\mathrm{lcm}(a,b) = \mathrm{lcm}(a,c) = \mathrm{lcm}(b,c) = \mathrm{lcm}(a,b,c).$$

Proof. It is clear that $(i,j,k)\sigma^{3p} = (i(\alpha\beta\gamma)^p, j(\beta\gamma\alpha)^p, k(\gamma\alpha\beta)^p)$, for any integer $p \geqslant 0$. Therefore $(i,j,k)\sigma^{3\,\mathrm{lcm}(a,b)} = (i,j,k(\gamma\alpha\beta)^{\mathrm{lcm}(a,b)}) \in O(L)$. Hence $c \mid \mathrm{lcm}(a,b)$, which means that $\mathrm{lcm}(a,b) = \mathrm{lcm}(a,b,c)$. Similarly we can prove that $b \mid \mathrm{lcm}(a,c)$ and $a \mid \mathrm{lcm}(b,c)$. □

Let $\mathscr{D}$ denote the set of ideals in the divisibility lattice of the positive integers. In [75] the elements of $\mathscr{D}$ were called *strongly lcm-closed sets*. This is because elements Λ of $\mathscr{D}$ are characterised by the property that $a, b \in \Lambda$ if and only if $\mathrm{lcm}(a,b) \in \Lambda$. If $\Lambda \in \mathscr{D}$ is finite then Λ is the set of divisors of the maximum element in Λ.

Theorem 3.3.4. *Suppose $\Lambda \in \mathscr{D}$. Let $2\Lambda = \{2x : x \in \Lambda\}$. Take $\Lambda' = \Lambda \cup 2\Lambda$. (It can be proved that $\Lambda' \in \mathscr{D}$). Define $R_\Lambda = C_\Lambda = \{i \in [n] : o_\beta(i) \in \Lambda\}$, and $S_{\Lambda'} = \{i \in [n] : o_\gamma(i) \in \Lambda'\}$. Suppose $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$. If R_Λ is non-empty then $|R_\Lambda| = |C_\Lambda| = |S_{\Lambda'}|$ and L contains a subsquare M on the rows R_Λ, columns C_Λ and symbols $S_{\Lambda'}$.*

Proof. By definition $|R_\Lambda| = |C_\Lambda|$. Let M be the submatrix of L induced by rows R_Λ and columns C_Λ. Let (i, j, k) be any triple in M. Then $o_\beta(i) = a$ for some $a \in \Lambda$, $o_\beta(j) = b$ for some $b \in \Lambda$ and hence $\operatorname{lcm}(2a, 2b) = \operatorname{lcm}(2a, c) = \operatorname{lcm}(2b, c)$. Since $a, b \in \Lambda$ we know that $\operatorname{lcm}(a, b) \in \Lambda$. Therefore $\operatorname{lcm}(2a, 2b) = 2\operatorname{lcm}(a, b) \in 2\Lambda$. Hence $\operatorname{lcm}(2a, c) \in \Lambda'$. Therefore $c \in \Lambda'$ and hence $|R_\Lambda| \leqslant |S_{\Lambda'}|$.

Now consider any triple (i, j, k) of L for which $o_\beta(i) = a \in \Lambda$ and $o_\beta(j) = d \notin \Lambda$. If $o_\gamma(k) = c$ then $\operatorname{lcm}(2a, 2d) = \operatorname{lcm}(2a, c) = \operatorname{lcm}(2d, c)$. Since $\operatorname{lcm}(a, d) \notin \Lambda$, $\operatorname{lcm}(2a, 2d) = 2\operatorname{lcm}(a, d) \notin 2\Lambda$. Therefore $\operatorname{lcm}(2a, 2d) \notin \Lambda'$. Hence $\operatorname{lcm}(2a, c) \notin \Lambda'$. But $2a \in \Lambda'$. Therefore $c \notin \Lambda'$. Hence $k \notin S_{\Lambda'}$. Therefore each element of $S_{\Lambda'}$ in rows R_Λ lies in columns of C_Λ and hence belongs to M. Therefore M is a subsquare. □

For example, consider the paratopism $\sigma = (\varepsilon, \beta, \gamma; (12))$ such that the cycle structure of β is $18{\cdot}6{\cdot}2$ and the cycle structure of γ is $18{\cdot}4^2$. Consider $\Lambda = \{1, 2\} \in \mathscr{D}$. Then $\Lambda' = \Lambda \cup 2\Lambda = \{1, 2, 4\}$. Therefore $|R_\Lambda| = 2$ and $|S_{\Lambda'}| = 8$. Hence by Theorem 3.3.4, $\sigma \notin \mathrm{Par}(26)$.

We now show a more subtle use of Theorem 3.3.4. Suppose $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$ where the cycle structure of β is $4^2{\cdot}2^4$ and the cycle structure of γ is $8{\cdot}2{\cdot}1^6$. Using $\Lambda = \{1, 2\}$, we see that L contains a subsquare on the rows and columns indexed by the 2-cycles of β. As it happens, this subsquare can be constructed on the symbols in $S_{\Lambda'}$. However, this subsquare is half the order of L, which forces a subsquare, also on the symbols in $S_{\Lambda'}$, to lie in the rows and columns indexed by 4-cycles of β. It will follow from Theorem 3.5.4 that this subsquare cannot be built, and hence $\sigma \notin \mathrm{Par}(16)$ after all.

Taking $\Lambda = \{1\}$ in Theorem 3.3.4, we immediately get:

Corollary 3.3.5. Suppose $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$ where $\beta \neq \varepsilon$. If $\mathrm{Fix}(\beta) \neq \emptyset$ then the submatrix M whose rows and columns belong to $\mathrm{Fix}(\beta)$ is a subsquare of L. In particular $|\mathrm{Fix}(\beta)| \leqslant n/2$.

Theorem 3.3.6. *Suppose $\Lambda \in \mathscr{D}$. Define, $R_\Lambda = \{i \in [n] : o_\gamma(i) \in \Lambda\}$. Suppose that $\sigma = (\varepsilon, \varepsilon, \gamma; (123))$ is an autoparatopism of a Latin square L. If R_Λ is non-empty then L contains a subsquare M on the rows R_Λ, columns R_Λ and symbols R_Λ.*

Proof. Let (i, j, k) be a triple of L, with $i, j \in R_\Lambda$. Then $o_\gamma(i) = a$ and $o_\gamma(j) = b$ where $a, b \in \Lambda$. By Lemma 3.3.3, $c = o_\gamma(k)$ satisfies $\operatorname{lcm}(a, c) = \operatorname{lcm}(b, c) = \operatorname{lcm}(a, b) \in \Lambda$, since $a, b \in \Lambda$. Therefore $c \in \Lambda$ and $k \in R_\Lambda$. Hence M is a subsquare. □

Taking $\Lambda = \{1\}$ we immediately get:

Corollary 3.3.7. Let $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathcal{P}_n$ where $\gamma \neq \varepsilon$. If $\sigma \in \mathrm{Par}(L)$ then the submatrix M whose rows and columns belong to $\mathrm{Fix}(\gamma)$ is a subsquare of L. Hence $|\mathrm{Fix}(\gamma)| \leqslant n/2$.

We close this subsection by noting some results which are immediate corollaries of prior work.

Lemma 3.3.8. $(\varepsilon, \varepsilon, \varepsilon; \delta) \in \mathrm{Par}(n)$ *for all $\delta \in \mathcal{S}_3$ and positive integers n.*

Proof. For all n there is a totally symmetric Latin square of order n. For example, we can take $L(i, j) = -i - j$ with rows, columns and symbols indexed by $\mathbb{Z}_n$. □

Consider the following result from [75].

Theorem 3.3.9. *Suppose 2^a is the largest power of 2 dividing n, where $a \geqslant 1$. Suppose $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ is such that the length of each cycle in α, β and γ is divisible by 2^a. Then $\theta \notin \mathrm{Atp}(n)$.*

Corollary 3.3.10. Let 2^a be the largest power of 2 dividing n, where $a \geqslant 1$. If $\sigma = (\alpha, \beta, \gamma; (123))$ and the length of each cycle in $\alpha\beta\gamma$ is divisible by 2^a, then $\sigma \notin \mathrm{Par}(n)$.

Proof. If $\sigma \in \mathrm{Par}(L)$ then $\sigma^3 = (\alpha\beta\gamma, \beta\gamma\alpha, \gamma\alpha\beta) \in \mathrm{Atp}(L)$. By assumption, the length of each cycle in $\alpha\beta\gamma$ is divisible by 2^a. However, $\alpha\beta\gamma \sim \beta\gamma\alpha \sim \gamma\alpha\beta$, so this is a contradiction of Theorem 3.3.9. □

Suppose $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$ where n is even. Let 2^a be the largest power of 2 dividing n. Then γ has at least one cycle whose length is not divisible by 2^a. One application of this is to show that $(\varepsilon, \varepsilon, \gamma; (123)) \notin \mathrm{Par}(n)$ when γ has cycle structure d^m, where d is even and m is odd.

Bryant *et al.* [9] considered Latin squares with cyclic automorphisms and additional conjugate symmetries. Composing the automorphism and conjugate symmetry immediately gives the following:

Theorem 3.3.11. *Suppose $\alpha \in \mathcal{S}_n$ has cycle structure $(n-f)^1 \cdot 1^f$ Then $\sigma = (\alpha, \alpha, \alpha; (12)) \in \mathrm{Par}(n)$ if*

(i) $f = 0$ and n is odd,
(ii) $f = 1$, or
(iii) $f = 2$ and n is even.

Also $\sigma = (\alpha, \alpha, \alpha; (123)) \in \mathrm{Par}(n)$ if

(i) $f = 0$ and $n \equiv 1, 3 \mod 6$,
(ii) $f = 1$ and $n \not\equiv 0 \mod 6$ and $n \neq 10$,
(iii) $f \equiv 2 \mod 3$ and $n \equiv 1, 2 \mod 3$,
(iv) $f \equiv 0 \mod 3, f \geqslant 3$ and $n \equiv 0, 1 \mod 3$, or
(v) $f \equiv 1 \mod 3$ and $f \geqslant 4$.

3.4 Automorphisms

Stones *et al.* [75] characterised $\alpha \in \mathrm{Aut}(n)$ for which α has at most three non-trivial cycles (that is, cycles other than fixed points). A notable feature of this characterisation is that the length of the longest cycle of α is always divisible by the length of every other cycle of α. In this section we first prove a related result for automorphisms with four nontrivial cycles, before showing that no analogue holds for five nontrivial cycles. Finally, we find a sufficient condition for $\alpha \in \mathcal{S}_n$ to be an automorphism when the cycle structure of α is $d_1 \cdot d_2 \cdots d_{p-1} \cdot d_p^a$, for some $a \geqslant 1$.

Theorem 3.4.1. *Let $d_1 d_2 d_3 d_4$ be the cycle structure of $\alpha = \alpha_1\alpha_2\alpha_3\alpha_4 \in \mathcal{S}_n$ such that $d_1 > d_2 > d_3 > d_4$ and $d_4 \nmid d_3$, $d_4 \nmid d_2$ and $d_3 \nmid d_2$. If $\alpha \in \mathrm{Aut}(n)$ then*

$$d_1 = \mathrm{lcm}(d_2, d_3) = \mathrm{lcm}(d_2, d_4) = \mathrm{lcm}(d_3, d_4).$$

Proof. Suppose that $d_2 \nmid d_1$. Consider a cell (i, j) in the M_{12} block of a Latin square L for which $\alpha \in \mathrm{Aut}(L)$. Then $o_\alpha(i) = d_1$ and $o_\alpha(j) = d_2$. By Lemma 3.3.1, $o_\alpha(L(i, j)) = c$, where $\mathrm{lcm}(d_1, d_2) = \mathrm{lcm}(c, d_1) = \mathrm{lcm}(c, d_2)$. Then, $c \neq d_1$ since $d_2 \nmid d_1$ and $c \neq d_2$ since $d_1 > d_2$. Since α_3 or α_4 on its own cannot fill the M_{12} block, symbols from both these cycles must be used in this block. Therefore $\mathrm{lcm}(d_1, d_2) = \mathrm{lcm}(d_1, d_3) = \mathrm{lcm}(d_1, d_4) = \mathrm{lcm}(d_2, d_3) = \mathrm{lcm}(d_2, d_4)$. If $\mathrm{lcm}(d_3, d_4)$ does not equal the lcm of the other pairs then there are no symbols available to fill the M_{34} block. Hence the lcm of all the different pairs are equal. Then the block diagram of L is as follows, where T^a_{bc} is the number of times each symbol in α_a appears in the M_{bc} block.

	α_1	α_2	α_3	α_4
α_1	$\alpha_1 : d_1$	$\alpha_3 : T^3_{12}$ $\alpha_4 : T^4_{12}$	$\alpha_2 : T^2_{13}$ $\alpha_4 : T^4_{13}$	$\alpha_2 : T^2_{14}$ $\alpha_3 : T^3_{14}$
α_2	$\alpha_3 : T^3_{12}$ $\alpha_4 : T^4_{12}$	$\alpha_2 : d_2$	$\alpha_1 : T^1_{23}$ $\alpha_4 : T^4_{23}$	$\alpha_1 : T^1_{24}$ $\alpha_3 : T^3_{24}$
α_3	$\alpha_2 : T^2_{13}$ $\alpha_4 : T^4_{13}$	$\alpha_1 : T^1_{23}$ $\alpha_4 : T^4_{23}$	$\alpha_3 : d_3$	$\alpha_1 : T^1_{34}$ $\alpha_2 : T^2_{34}$
α_4	$\alpha_2 : T^2_{14}$ $\alpha_3 : T^3_{14}$	$\alpha_1 : T^1_{24}$ $\alpha_3 : T^3_{24}$	$\alpha_1 : T^1_{34}$ $\alpha_2 : T^2_{34}$	$\alpha_4 : d_4$

.

Considering the distribution of α_3 in the block diagram, we see that, $T^3_{12} + T^3_{14} = d_1$, $T^3_{21} + T^3_{24} = d_2$ and $T^3_{14} + T^3_{24} = d_4$. Hence $T^3_{12} + T^3_{21} = d_1 + d_2 - d_4$. A similar argument shows that $T^4_{12} + T^4_{21} = d_1 + d_2 - d_3$.

Counting symbols in $M_{12} \cup M_{21}$, we find that $2d_1d_2 = d_3(T^3_{12} + T^3_{21}) + d_4(T^4_{12} + T^4_{21}) = d_3(d_1+d_2-d_4)+d_4(d_1+d_2-d_3)$ which implies that $(d_1-d_4)(d_2-d_3)+(d_1-d_3)(d_2-d_4) = 0$. This is a contradiction since $d_1 > d_2 > d_3 > d_4$. Therefore $d_2 \mid d_1$.

Now consider the M_{23} block. Suppose $o_\alpha(i) = c$ for some symbol i in the M_{23} block. Then by Lemma 3.3.1, $\mathrm{lcm}(d_2, d_3) = \mathrm{lcm}(c, d_2) = \mathrm{lcm}(c, d_3)$. Then, $c \neq d_3$ since $d_2 > d_3$, and $c \neq d_2$ since $d_3 \nmid d_2$. Since α_4 cannot fill the M_{23} block on its own, $T^1_{23} > 0$. Hence $\mathrm{lcm}(d_2, d_3) = \mathrm{lcm}(d_1, d_3) = \mathrm{lcm}(d_1, d_2) = d_1$. Repeating this argument for M_{24} shows that $\mathrm{lcm}(d_2, d_4) = d_1$. Now a similar argument for M_{34} shows that either $T^1_{34} > 0$ or $T^2_{34} > 0$, and either will imply the result we need. □

The argument used to prove Theorem 3.4.1, does not work when α has five non-trivial cycles. We found the following block diagram satisfying Lemma 3.3.1 for $\alpha = \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5$

with lengths $d_1 > d_2 > d_3 > d_4 > d_5$ such that none of d_2, d_3, d_4, d_5 divide d_1:

	α_1	α_2	α_3	α_4	α_5
α_1	$\alpha_1 : 95381$	$\alpha_3 : 4451$ $\alpha_4 : 1776$ $\alpha_5 : 1844$	$\alpha_2 : 4304$ $\alpha_4 : 1370$ $\alpha_5 : 1163$	$\alpha_2 : 2274$ $\alpha_3 : 1591$ $\alpha_5 : 282$	$\alpha_2 : 1793$ $\alpha_3 : 1295$ $\alpha_4 : 201$
α_2	$\alpha_3 : 4451$ $\alpha_4 : 1776$ $\alpha_5 : 1844$	$\alpha_2 : 60697$	$\alpha_1 : 4537$ $\alpha_4 : 63$ $\alpha_5 : 69$	$\alpha_1 : 2267$ $\alpha_3 : 192$ $\alpha_5 : 180$	$\alpha_1 : 1917$ $\alpha_3 : 26$ $\alpha_4 : 0$
α_3	$\alpha_2 : 4304$ $\alpha_4 : 1370$ $\alpha_5 : 1163$	$\alpha_1 : 4537$ $\alpha_4 : 63$ $\alpha_5 : 69$	$\alpha_3 : 51359$	$\alpha_1 : 4304$ $\alpha_4 : 1370$ $\alpha_5 : 1163$	$\alpha_1 : 1171$ $\alpha_2 : 0$ $\alpha_4 : 600$
α_4	$\alpha_2 : 2274$ $\alpha_3 : 1591$ $\alpha_5 : 282$	$\alpha_1 : 2267$ $\alpha_3 : 192$ $\alpha_5 : 180$	$\alpha_1 : 1679$ $\alpha_2 : 65$ $\alpha_5 : 539$	$\alpha_4 : 29029$	$\alpha_1 : 251$ $\alpha_2 : 300$ $\alpha_3 : 450$
α_5	$\alpha_2 : 1793$ $\alpha_3 : 1295$ $\alpha_4 : 201$	$\alpha_1 : 1917$ $\alpha_3 : 26$ $\alpha_4 : 0$	$\alpha_1 : 1171$ $\alpha_2 : 0$ $\alpha_4 : 600$	$\alpha_1 : 251$ $\alpha_2 : 300$ $\alpha_3 : 450$	$\alpha_5 : 23023$

where

$$\begin{aligned} d_1 &= o(\alpha_1) = 11 \times 13 \times 23 \times 29 = 95381, \\ d_2 &= o(\alpha_2) = 7 \times 13 \times 23 \times 29 = 60697, \\ d_3 &= o(\alpha_3) = 7 \times 11 \times 23 \times 29 = 51359, \\ d_4 &= o(\alpha_4) = 7 \times 11 \times 13 \times 29 = 29029, \\ d_5 &= o(\alpha_5) = 7 \times 11 \times 13 \times 23 = 23023. \end{aligned}$$

It is not clear whether this block diagram is realised by any Latin square although we suspect that it is. In any case, McKay et al. [58] have constructed a Latin square with an automorphism consisting of 5 non-trivial cycles, none of which has a length dividing the length of any other cycle. Hence it is clear that such things exist.

Next we look at the opposite scenario, where each cycle length is divisible by the next.

Theorem 3.4.2. *Let $d_1 \cdots d_{p-1} \cdot d_p^a$, where $a = m - p + 1$, be the cycle structure of $\alpha = \alpha_1\alpha_2 \cdots \alpha_m \in \mathcal{S}_n$ such that $d_i < d_{i-1}$ and $d_i \mid d_{i-1}$ for $2 \leqslant i \leqslant p$, and d_1 is odd. Then $\alpha \in \mathrm{Aut}(n)$ if and only if $ad_p \leqslant d_{p-1}$.*

Proof. Suppose that $\alpha \in \mathrm{Aut}(L)$. By [75, Thm 3.7], L has a subsquare induced by the cycles of α of length d_p, inside a subsquare induced by the cycles of lengths d_{p-1} and d_p. It follows that $ad_p \leqslant (ad_p + d_{p-1})/2$ and hence $ad_p \leqslant d_{p-1}$.

Now assume that $ad_p \leqslant d_{p-1}$. By induction on p, we will construct a Latin square L of order n having $\alpha \in \mathrm{Aut}(L)$. The base case is provided by [75, Thm 5.2]. In the general case [75, Thm 3.7] shows that L has a subsquare induced by the cycles of α other than α_1. This subsquare can be built, by the inductive hypothesis. So it suffices to give the following partial contour. Let $e_q = \sum_{j=1}^{q} o(\alpha_j)$ for $0 \leqslant q \leqslant m$. In M_{11} we take,

$$C(i, d_1 + 1 - i) = \begin{cases} t_1, \text{ for } 1 \leqslant i \leqslant 2d_1 - n, \\ t_r, \text{ for } d_1 + e_{r-1} - n + 1 \leqslant i \leqslant d_1 + e_r - n, \text{ and } 2 \leqslant r \leqslant m, \end{cases}$$

In $\bigcup_{r=2}^{m} M_{1,r}$ we take, $C(d_1 + 1 - i, d_1 + i) = t_1$, for $1 \leqslant i \leqslant n - d_1$. In $\bigcup_{r=2}^{m} M_{r,1}$ we take $C(n + 1 - i, i) = t_1$, for $1 \leqslant i \leqslant n - d_1$. □

For example, if $d_1 \cdot d_2 \cdot d_3^3$ is the cycle structure of $\alpha = \alpha_1\alpha_2\alpha_3\alpha_4\alpha_5$ then the block diagram is as in Figure 3.1.

	α_1	α_2	α_3	α_4	α_5
α_1	$\alpha_1 : d_1 - d_2 - 3d_3$ $\alpha_2 : d_2$ $\alpha_3 : d_3$ $\alpha_4 : d_3$ $\alpha_5 : d_3$	$\alpha_1 : d_2$	$\alpha_1 : d_3$	$\alpha_1 : d_3$	$\alpha_1 : d_3$
α_2	$\alpha_2 : d_2$	$\alpha_2 : d_2 - 3d_3$ $\alpha_3 : d_3$ $\alpha_4 : d_3$ $\alpha_5 : d_3$	$\alpha_2 : d_3$	$\alpha_2 : d_3$	$\alpha_2 : d_3$
α_3	$\alpha_1 : d_3$	$\alpha_2 : d_3$	$\alpha_3 : d_3$	$\alpha_4 : d_3$	$\alpha_5 : d_3$
α_4	$\alpha_1 : d_3$	$\alpha_2 : d_3$	$\alpha_4 : d_3$	$\alpha_5 : d_3$	$\alpha_3 : d_3$
α_5	$\alpha_1 : d_3$	$\alpha_2 : d_3$	$\alpha_5 : d_3$	$\alpha_3 : d_3$	$\alpha_4 : d_3$

.

Figure 3.1:

3.5 Autoparatopisms of the form $(\alpha, \beta, \gamma; (12))$

In this section and the next we prove a number of general results which between them are sufficient to determine $\mathrm{Par}(n)$ for $n \leqslant 17$. By 3.2.2, whether $\sigma = (\alpha, \beta, \gamma; (12))$ is in $\mathrm{Par}(n)$ depends only on the cycle structure of $\alpha\beta$ and the cycle structure of γ, so it is enough to study paratopisms of the form $(\varepsilon, \beta, \gamma; (12))$. We start by proving a number of constraints on autoparatopisms of this form. After that we study some special cases in which it is feasible to characterise exactly which paratopisms are autoparatopisms.

Many of the results in this section will employ the same basic technique to bound the number of symbols which are fixed points of γ. We concentrate on one row and consider how many columns in that row may contain fixed symbols. Another technique that we employ repeatedly is to take a triple T, apply some power of a supposed autoparatopism to produce a triple T' that agrees in two places with T, then deduce that $T' = T$. This relies on the fact that distinct triples of a Latin square agree in at most one coordinate.

Theorem 3.5.1. *Suppose that $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$. Let b, c be respectively the orders of β, γ as elements of $\mathcal{S}_n$. Then $c \mid 2b$ and if c is odd then $c = b$.*

Proof. Since $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ we know that $\sigma^{2b} = (\varepsilon, \varepsilon, \gamma^{2b}; \varepsilon) \in \mathrm{Par}(n)$. It follows that $\gamma^{2b} = \varepsilon$, so $c \mid 2b$.

From now on suppose that c is odd. Suppose that d is any cycle length of β. It suffices to show that $d \mid c$. As d was arbitrary this will show that $b \mid c$, which together with $c \mid 2b$ will imply $b = c$, since c is odd.

Consider a row i such that $o_\beta(i) = d$ and let $k = L(i, i\beta^{(c-1)/2})$. As $(i, i\beta^{(c-1)/2}, k) \in O(L)$, we know that $O(L)$ also includes the triple

$$(i, i\beta^{(c-1)/2}, k)\sigma^c = (i\beta^c, i\beta^{(c-1)/2}, k\gamma^c) = (i\beta^c, i\beta^{(c-1)/2}, k).$$

Hence, $i\beta^c = i$ which means that $d \mid c$, as claimed. □

Corollary 3.5.2. $(\alpha, \beta, \varepsilon; (12)) \in \mathrm{Par}(n)$ if and only if $\alpha = \beta^{-1} \in \mathcal{S}_n$.

By Theorem 3.5.1, $(\varepsilon, \beta, \gamma; (12)) \notin \mathrm{Par}(12)$ if β and γ have cycle structures 6^2 and 3^4 respectively. Note that Theorem 3.5.1 does not eliminate the case when β and γ have cycle structures 3^4 and 6^2 respectively. Our next result does rule out that case.

Theorem 3.5.3. *Suppose $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$. If β has a cycle of odd length d then γ has at least one cycle whose length divides d.*

Proof. Any symbol k in the short orbit in the block with rows and columns indexed by the d-cycle of β must satisfy $o_\gamma(k) \mid d$. □

In particular, Theorem 3.5.3 says that if β has fixed points then γ has at least one fixed point. We next consider upper bounds on the number of fixed points that γ may have.

Theorem 3.5.4. *Suppose that $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$. Fix an integer d and let r be the number of cycles of β that have length d. If $r > 0$ and f is the number of fixed points of γ then*

(i) $f \leqslant (r-1)d$ if d is even, and

(ii) $f \leqslant (r-1)d + 1$ if d is odd.

Proof. We assume that $\sigma \in \mathrm{Par}(L)$ for some Latin square L of order n. Fix a row i such that $o_\beta(i) = d$ and suppose that $(i, j, k) \in O(L)$, where $o_\gamma(k) = 1$. By Lemma 3.3.2, $o_\beta(j) = d$, giving us at most rd options for j. Now apply Lemma 3.2.3. When d is even, j cannot be from the same orbit of β as i which means that $f \leqslant (r-1)d$. When d is odd, there is a unique possibility for j in the same orbit of β as i, meaning that $f \leqslant (r-1)d + 1$. □

For example $\sigma = (\varepsilon, \beta, \gamma; (12)) \notin \mathrm{Par}(n)$ when β and γ have respective cycle structures 4^2 and $2^1 1^6$. The same conclusion is reached if β and γ both have cycle structure $3^2 1^5$.

Our next result will improve on Theorem 3.5.4 in some cases when r is odd.

Theorem 3.5.5. *Suppose that $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ where β has precisely r cycles of some length d, and r is odd. Let Γ be the set of all cycles C of γ satisfying*

(i) $o(C)$ is an odd divisor of d,

(ii) β has no cycle C' satisfying $1 < o(C') < d$ and $\mathrm{lcm}(o(C), o(C')) = d$, and

(iii) if $o(C) = d > 1$ then β has an even number of fixed points.

Then $\Gamma = \emptyset$ if d is even and $|\Gamma| \leqslant r$ if d is odd.

Proof. Let A be the submatrix of L containing the cells (i, j) for which $o_\beta(i) = o_\beta(j) = d$, and B be the submatrix of L containing the cells (i, j) for which $o_\beta(i) = d$ and $o_\beta(j) \neq d$. Assume that $C \in \Gamma$ and let $c = o(C)$.

First suppose that some symbol k of C occurs in a column j of B. Let $d' = o_\beta(j)$. Since $c \mid d$ we know that $2d = \mathrm{lcm}(c, 2d) = \mathrm{lcm}(c, 2d')$ by Lemma 3.3.2. So $d = \mathrm{lcm}(c, d')$, as c is odd. Hence $d' = 1$ by (ii), which means that $d = \mathrm{lcm}(c, 1) = c$. Now by (iii), the number f of fixed points of β is even. Suppose that $o_\beta(j') = 1$. By Lemma 3.3.2, each symbol of C occurs in column j' of B, since it cannot occur in column j' of L outside of B. Hence the number of cells of A that contain symbols from C is $crd - fd$. These cells cannot be divided into orbits of length $2d$, since $cr - f$ is odd. Hence, by Lemma 3.2.3, the symbols of C must fill at least one short orbit in A.

Next suppose that no symbol of C occurs in B. In that case the crd cells of A containing symbols of C cannot be partitioned into orbits of length $2d$, since cr is odd. So again, the symbols of C must fill at least one short orbit in A.

The number of short orbits in A is 0 if d is even and r if d is odd. The result follows. □

Theorem 3.5.5 provides an upper bound on the number of fixed points of γ, since Γ automatically contains all such points, and often contains other cycles as well. For example, if β and γ both have cycle structure $3^3 1^2$ then $(\varepsilon, \beta, \gamma; (12)) \notin \mathrm{Par}(11)$.

Theorem 3.5.6. *Let $n = 2^u v$ where v is odd. Suppose that $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ where every cycle of β has length divisible by 2^u. Then*

(i) β has at least as many cycles of odd length as γ has.

(ii) if $u \geqslant 1$ then γ has no cycles of odd length.

Proof. Let L be a Latin square for which $\sigma \in \mathrm{Par}(L)$. Suppose that $(i, j, k) \in O(L)$ where $o_\gamma(k) = c$ and c is odd. If $a = o_\beta(i)$ and $b = o_\beta(j)$ then $2^{u+1} \mid 2\,\mathrm{lcm}(a, b)$ by assumption. The total length of all orbits containing k is cn, which is not divisible by 2^{u+1}. So k must appear in at least one orbit whose length is not divisible by 2^{u+1}. By Lemma 3.2.3, the only possibility is a short orbit. If $u \geqslant 1$ then there are no short orbits. If $u = 0$ then there is a unique short orbit for each cycle of β of odd length. The result follows. □

For example, $(\varepsilon, \beta, \gamma; (12)) \notin \mathrm{Par}(10)$ if β, γ have respective cycle structures $6^1 2^2$ and $4^1 3^2$, or 3^3 and $3^2 1^3$.

To assist in the proof of our next theorem we introduce a well-known concept. For each pair (s, t) of symbols in a Latin square L, there are one or more *symbol cycles* which satisfying the following description and are minimal in the sense that no proper subset also satisfies the conditions. A symbol cycle is a set of cells that each contain either s or t, and such that in any row or column of L the symbol cycle includes either zero or two cells. Symbol cycles are simple examples of trades; a new Latin square can be obtained by switching the symbols s and t throughtout the cycle (see, for example, [82]). Below, we will also need to switch parts of symbol cycles. For this purpose we make two definitions. We call the cells on the main diagonal of L *pivots*. A *section* S of a symbol cycle C can then be defined as follows. We designate a starting point in C, which will be a pivot and will be included in S. We then alternate moving horizontally then vertically, stepping to the other cell that C contains in the same row or column, respectively. Each cell that we visit is included in S. We stop immediately upon including a second pivot in S.

Theorem 3.5.7. *$\sigma = (\varepsilon, \varepsilon, \gamma; (12)) \in \mathrm{Par}(n)$ if and only if the cycle structure of γ is $2^r \cdot 1^f$ for integers $r \geqslant 0$ and $f \geqslant 1$.*

Proof. Suppose that $\sigma = (\varepsilon, \varepsilon, \gamma; (12)) \in \mathrm{Par}(n)$. Then Theorem 3.5.1 shows that $\gamma^2 = \varepsilon$ and Theorem 3.5.3 shows that γ has a fixed point. Hence the cycle structure of γ is as claimed.

Conversely, suppose that γ has cycle structure $2^r \cdot 1^f$, where $r \geqslant 0$ and $f \geqslant 1$. We now explain a process for constructing a Latin square L with $\sigma \in \mathrm{Par}(L)$. Initially, we take L to be the cyclic square $\mathcal{C}_n$, defined by $\mathcal{C}_n(i, j) \equiv i + j - 1 \mod n$, which corresponds to the cyclic group.

Then for $a = 1, 2, \ldots, r$ we undertake the following steps, which will describe as *surgery for a*. We first identify the symbol cycles for the pair of symbols $(a, n - a)$. These will be of two types depending on whether the cycle includes any pivot or not. The symbol cycles that contain no pivot come in pairs that are images of each other under transposition of L. We switch on one entire cycle in each such pair of cycles. Any symbol cycle C that contains a pivot requires more care. We first argue that C contains exactly two pivots. It is clear that the number of pivots in C must be even since there are an even number of cells in C overall, and non-pivots are paired up by tranposition. Also, it is not hard to see that any section and its image under transposition together form a complete symbol cycle. Hence C has two pivots as claimed. We will switch the symbols in one section of C and leave the rest of C unaltered. We then fill both the pivots of C with the symbol n. Doing this will create some duplication within rows and columns that can be fixed with due care. The details are as follows.

Assume that n is odd. Then one pivot in C contains the symbol a and the other has the symbol $n-a$. Suppose the former is cell (i, i) and the latter is cell $(n+1-i, n+1-i)$. We switch the section starting from (i, i) and then put $L(n+1-i, i) = a$ and $L(i, n+1-i) = n - a$.

Now assume that n is even. If a is even then there are no relevant pivots, so assume a is odd. We switch the section starting at $((a+1)/2, (a+1)/2)$ and the section starting at $(n-(a-1)/2, n-(a-1)/2)$. Then we put $L((a+1)/2, n+1-(a+1)/2) = n - a$ and $L(n+1-(a+1)/2, (a+1)/2) = a$. If $n \equiv 0 \mod 4$ then put $L((n+a+1)/2, (n-a+1)/2) = a$ and $L((n-a+1)/2, (n+a+1)/2) = n - a$. Meanwhile, for $n \equiv 2 \mod 4$ we put $L((n+a+1)/2, (n-a+1)/2) = n - a$ and $L((n-a+1)/2, (n+a+1)/2) = a$.

This completes our description of surgery for a. It is now routine to check that it has the following properties. Surgery for a arranges the symbols a and $n - a$ in such a way that if cell (i, j) contains a then cell (j, i) contains $n - a$. Moreover, the only places that L changes are cells containing a, $n - a$ or n. The last of these options only affects cells in the row and column of the pivots that contain a or $n - a$. It follows that if $1 \leqslant a < a' \leqslant r$ then surgery for a affects cells that are distinct from those affected by surgery for a'. Hence we can do surgery for each $a = 1, 2, \ldots, r$ and the result will be a Latin square having σ as an autoparatopism. □

Squares having the symmetry discussed in Theorem 3.5.7 in the particular case $f = 1$ have been called *pairing squares*. Some interesting properties of these squares were proven in [53] and [82].

Examples of the Latin squares built in Theorem 3.5.7 for $n = 10$ and 11 are given below. The cycle structure of γ is $2^4 \cdot 1^2$ when $n = 10$ and $2^3 \cdot 1^5$ when $n = 11$. First we give the cyclic square $\mathcal{C}_n$ with one section marked. Shaded cells represent a section of the symbol cycle (3 7) when $n = 10$ and a section of the symbol cycle (1 10) when $n = 11$. Both these sections are switched in producing the final squares, which are given below.

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

1	2	3	4	5	6	7	8	9	10	11
2	3	4	5	6	7	8	9	10	11	1
3	4	5	6	7	8	9	10	11	1	2
4	5	6	7	8	9	10	11	1	2	3
5	6	7	8	9	10	11	1	2	3	4
6	7	8	9	10	11	1	2	3	4	5
7	8	9	10	11	1	2	3	4	5	6
8	9	10	11	1	2	3	4	5	6	7
9	10	11	1	2	3	4	5	6	7	8
10	11	1	2	8	4	5	6	7	8	9
11	1	2	3	4	5	6	7	8	9	10

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

11	9	3	4	5	6	7	8	2	1	10
2	11	4	5	6	7	3	9	10	8	1
8	4	5	6	7	3	9	1	11	10	2
4	5	6	7	3	2	10	11	1	9	8
5	6	7	8	11	1	2	10	9	3	4
6	7	8	9	10	11	1	2	3	4	5
7	8	2	1	9	10	11	3	4	5	6
3	2	10	11	1	9	8	4	5	6	7
9	1	11	10	2	8	4	5	6	7	3
10	3	1	2	8	4	5	6	7	11	9
1	10	9	3	4	5	6	7	8	2	11

Theorem 3.5.8. *Suppose that $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathcal{P}_n$ and the cycle structure of β is n^1. Then $\sigma \in \mathrm{Par}(n)$ if and only if*

(i) the length of each cycle in γ divides $2n$ and

(ii) at most one cycle of γ has odd length.

Proof. Suppose $\sigma \in \mathrm{Par}(L)$ for some Latin square L and that γ has a cycle of length c. By Lemma 3.2.3, all orbits have length n or $2n$, so $c \mid 2n$. If c is odd then $c \mid n$. By Theorem 3.5.5, there can be no such cycle when n is even, and at most one such cycle when n is odd. Hence (i) and (ii) hold.

It remains to show sufficiency. Assume that (i) and (ii) hold. Suppose that γ has c different cycles, with lengths $d_1, \ldots, d_c$. Since $n = \sum d_i$ we know from (ii) that γ has no cycles of odd length if n is even. Also, if n is odd then γ must have one cycle of odd length. For convenience, we assume that d_1 is odd if n is odd. Define $h = \lceil n/2 \rceil + 1$ and let $e_p = \sum_{j=1}^{p} \lceil d_j/2 \rceil$ for $0 \leqslant p \leqslant c$. Then the contour of a Latin square L such that $\sigma \in \mathrm{Par}(L)$ can be constructed by putting $C(i, h-i) = t_r$ for $1 \leqslant r \leqslant c$ and $e_{r-1} < i \leqslant e_r$. □

Corollary 3.5.9. Suppose that $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathcal{P}_n$, the cycle structure of β is d^r and the cycle structure of γ is $d_1^{ra_1} d_2^{ra_2} \cdots d_p^{ra_p}$. Then $\sigma \in \mathrm{Par}(n)$ if $d_i \mid 2d$ for $1 \leqslant i \leqslant p$, and at most one d_i is odd.

Proof. Theorem 3.5.8 provides a solution L_1 in the case $r = 1$. For larger values of r, simply take the direct product of L_1 with $\mathcal{C}_r$. □

Our next result seems to depart from the principle of only considering paratopisms of the form $(\varepsilon, \beta, \gamma; (12))$. However, it will have several corollaries that deal with paratopisms of that form, so can still be considered part of the same agenda.

Theorem 3.5.10. *Suppose that $\alpha \in \mathcal{S}_n$ has cycle type $d^1 \cdot 1^f$ where $d > 1$ and $f \geqslant 0$. Let $\sigma = (\alpha, \alpha, \alpha; (12)) \in \mathcal{P}_n$. Then $\sigma \in \mathrm{Par}(n)$ if and only if one of the following is satisfied.*

(i) d is odd and $f \in \{0, 1\}$,

(ii) $d \equiv 0 \mod 4$ and $f \leqslant d/2$, or

(iii) $d \equiv 2 \mod 4$ and $1 \leqslant f \leqslant d/2 + 1$.

Proof. Throughout, L will denote a hypothetical Latin square for which $\sigma \in \mathrm{Par}(L)$. We start by showing the necessity of conditions (i) to (iii). Fix a row i such that $o_\alpha(i) = d$ and consider $(i, j, k) \in O(L)$ for which $o_\alpha(k) = 1$. By Lemma 3.3.2 we know that $o_\alpha(j) = d$, so j and i are from the same orbit of α.

For the moment, assume that d is odd. The orbit of the cell (i, j) is

$$\{(i\alpha^{2r}, j\alpha^{2r}) : 0 \leqslant r < d\} \cup \{(j\alpha^{2r+1}, i\alpha^{2r+1}) : 0 \leqslant r < d\}.$$

Since d is odd there is an integer r such that $i = j\alpha^{2r+1}$. For this r it must be the case that $j = i\alpha^{2r+1}$, otherwise the symbol k would occur in two different cells in row i. It follows that $i = i\alpha^{4r+2}$, so $4r + 2$ is divisible by d. As d is odd, it must divide $2r + 1$, but this means that $j = i\alpha^{2r+1} = i$. As there is only one choice for j, we conclude that $f \leqslant 1$.

Next we assume that d is even. In this case the orbit of the cell (i, j) is

$$\{(i\alpha^{2r}, j\alpha^{2r}) : 0 \leqslant r < d/2\} \cup \{(j\alpha^{2r+1}, i\alpha^{2r+1}) : 0 \leqslant r < d/2\}.$$

Suppose that $j = i\alpha^t$ for odd t in the range $0 < t < d$. Then to avoid symbol k being repeated in column j we must have $i = j\alpha^t = i\alpha^{2t}$. Hence d divides $2t$, which can only mean that $t = d/2$. In other words $j \notin \{i\alpha^t : t = 1, 3, 5, \ldots, d - 1\} \setminus \{i\alpha^{d/2}\}$ from which it follows that $f \leqslant d/2$ when $d \equiv 0 \mod 4$, and $f \leqslant d/2 + 1$ when $d \equiv 2 \mod 4$.

To complete the proof of necessity suppose that $d \equiv 2 \mod 4$ and consider the symbol k' for which $(i, i\alpha^{d/2}, k') \in O(L)$. Applying $\sigma^{d/2}$ we find that $(i, i\alpha^{d/2}, k'\alpha^{d/2}) \in O(L)$ which implies that $o_\alpha(k') \mid (d/2)$. The only possibility is that $o_\alpha(k') = 1$. Hence $f \geqslant 1$ when $d \equiv 2 \mod 4$.

It remains to prove sufficiency of conditions (i) to (iii). For (i) we simply invoke Theorem 3.3.11. For (ii) a contour for a Latin square L such that $\sigma \in \mathrm{Par}(L)$ when $f \leqslant d/2$ is as follows.

$$\begin{aligned}
C(d-1, d) &= 1, && \\
C(i, d-i) &= 1, && \text{for } 1 \leqslant i \leqslant d/2 - f, \\
C(d/2 - f + i, d/2 + f - i) &= \infty_i, && \text{for } 1 \leqslant i \leqslant f, \\
C(d/2 - f + i, \infty_i) = C(\infty_i, d/2 + f - i) &= 1, && \text{for } 1 \leqslant i \leqslant f, \\
C(d/2 + 2i - 1, d/2 - 2i) &= 1, && \text{for } 1 \leqslant i \leqslant d/4 - 1, \\
C(d/2 + 2i, d/2 + 1 - 2i) &= 1, && \text{for } 1 \leqslant i \leqslant d/4.
\end{aligned}$$

While for (iii) we have the following contour. Let $q = (d-2)/4$. Take,

$$\begin{aligned} C(q+1, d-q) = C(d-q, q+1) &= \infty_1, \\ C(d+1, q+1) = C(q+1, d+1) &= t_1, \\ C(i, d+1-i) = C(d+1-i, i) &= t_1, && \text{for } 1 \leqslant i \leqslant q, \\ C(q+i, d+i) = C(d+i, d-q+2-i) &= t_1, && \text{for } 2 \leqslant i \leqslant f, \\ C(q+i, d-q+2-i) &= \infty_i, && \text{for } 2 \leqslant i \leqslant f, \\ C(q+i, d-q+2-i) &= t_1, && \text{for } f+1 \leqslant i \leqslant d/2+1, \end{aligned}$$

and add an arbitrary subquasigroup on the fixed points of α. □

Here are examples of the construction in Theorem 3.5.10 for $d = 6$ and $f \in \{1, 4\}$:

4	2	5	∞	3	1	6
2	5	3	6	∞	4	1
5	3	6	4	1	∞	2
∞	6	4	1	5	2	3
3	∞	1	5	2	6	4
1	4	∞	2	6	3	5
6	1	2	3	4	5	∞

∞_3	2	∞_2	∞_1	∞_4	1	6	5	4	3
2	∞_3	3	∞_4	∞_1	∞_2	1	6	5	4
∞_4	3	∞_3	4	∞_2	∞_1	2	1	6	5
∞_1	∞_2	4	∞_3	5	∞_4	3	2	1	6
∞_2	∞_1	∞_4	5	∞_3	6	4	3	2	1
1	∞_4	∞_1	∞_2	6	∞_3	5	4	3	2
6	1	2	3	4	5	∞_1	∞_2	∞_3	∞_4
3	4	5	6	1	2	∞_2	∞_3	∞_4	∞_1
4	5	6	1	2	3	∞_3	∞_4	∞_1	∞_2
5	6	1	2	3	4	∞_4	∞_1	∞_2	∞_3

.

Corollary 3.5.11. Let $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathcal{P}_n$. Then $\sigma \in \mathrm{Par}(n)$ if,

(i) both β and γ have cycle structure n^1, where n is odd.

(ii) both β and γ have cycle structure $(n-1)^1 \cdot 1^1$, where n is even.

(iii) the cycle structure of β is $(d/2)^2 \cdot 1^f$ and the cycle structure of γ is $d^1 \cdot 1^f$ where $d \equiv 0 \mod 4$ and $f \leqslant d/2$.

(iv) the cycle structure of β is $(d/2)^2 \cdot 1^f$ and the cycle structure of γ is $d^1 \cdot 1^f$, where $d \equiv 2 \mod 4$ and $1 \leqslant f \leqslant d/2 + 1$.

Proof. Combine Theorem 3.2.2 and Theorem 3.5.10 when $\beta \sim \alpha^2$ and $\gamma \sim \alpha$. □

Corollary 3.5.12. Suppose $\alpha \in \mathcal{S}_n$ has cycle structure d^r. Then $\sigma = (\alpha, \alpha, \alpha; (12)) \in \mathcal{P}_n$ if and only if $d \not\equiv 2 \mod 4$.

Proof. We first consider the case when $d \equiv 2 \mod 4$. Let $h = d/2$ and $k = L(1\alpha^h, 1)$ where L is a hypothetical Latin square for which $\sigma \in \mathrm{Par}(L)$. Then $(1\alpha^h, 1, k)\sigma^h = (1\alpha^h, 1, k\alpha^h)$ since h is odd, so $k\alpha^h = k$. But this contradicts $o_\alpha(k) = d$, so $\sigma \notin \mathrm{Par}(n)$.

Now suppose that $d \not\equiv 2 \mod 4$. By Theorem 3.5.10 there is a Latin square L with $(\alpha', \alpha', \alpha'; (12)) \in \mathrm{Par}(L)$ where α' has cycle structure d^1. The direct product of L and $\mathcal{C}_r$ has the required autoparatopism σ. □

Corollary 3.5.13. Let $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathcal{P}_n$. Suppose β has cycle structure $d \cdot 1^f$ where $d > 1$. Then $\sigma \in \mathrm{Par}(n)$ if and only if one of the following conditions is satisfied:

(i) d is odd and $f \in \{0, 1\}$, or

(ii) d is even and $f = 0$.

Proof. (i) Suppose d is odd. Then $(\beta, \beta, \beta; (12))$ and $(\varepsilon, \beta, \beta; (12))$ are conjugate, by Theorem 3.2.2. By Theorem 3.5.10, $\sigma \in \mathrm{Par}(n)$ if and only if $f \in \{0, 1\}$.

(ii) Suppose d is even. If $\sigma \in \mathrm{Par}(n)$ then $f = 0$ by Theorem 3.5.5. Conversely, if $f = 0$ then $\mathcal{C}_n$ has σ as an autoparatopism. □

Developing in the direction of Corollary 3.5.13, we now characterise $(\varepsilon, \beta, \beta; (12)) \in \mathrm{Par}(n)$ when β has only two non-trivial cycles. We first do the case when those cycles are equal.

Theorem 3.5.14. *Let $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathcal{P}_n$. Suppose β has cycle structure $d^2 \cdot 1^f$ for some $d > 1$. Then $\sigma \in \mathrm{Par}(n)$ if and only if one of the following is satisfied.*

(i) d is even and $f = 0$, or

(ii) d is odd and $f \leqslant d + 1$.

Proof. Suppose first that $\sigma \in \mathrm{Par}(L)$ and d is even. If $f \geqslant 1$ then there is $(i, j, k) \in O(L)$ with $o_\beta(i) = d$ and $o_\beta(j) = 1$. By Lemma 3.3.2, $o_\beta(k) = 2d$, but β has no cycles of that length, so $f = 0$. Conversely, if $f = 0$ then $\sigma \in \mathrm{Par}(L)$ by Corollary 3.5.9.

Now suppose that d is odd. If $\sigma \in \mathrm{Par}(L)$ then $f \leqslant d + 1$ by Theorem 3.5.4. Let $g = \lfloor f/2 \rfloor$ and $h = (d + 1)/2$. We construct a contour for the subcase $f \leqslant d$ first. For $1 \leqslant i \leqslant h$, take $C(i, h + 1 - i) = t_1$. For $1 \leqslant i \leqslant g$ take

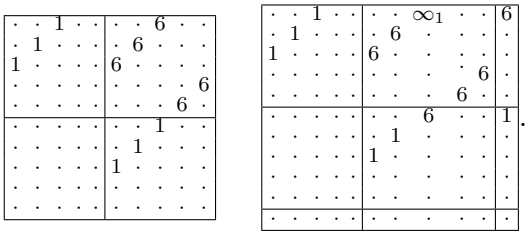
$$\begin{aligned} C(i + 1, 2d + i) = C(d + 1 - i, 2d + g + i) = C(d + 1 + i, d + h - i) &= t_2 \\ C(d + 1 + i, 2d + i) = C(2d + 1 - i, 2d + g + i) &= t_1 \\ C(i + 1, d + h - i) &= \infty_i \\ C(d + 1 - i, d + h + i &= \infty_{i+g}. \end{aligned}$$

For $g + 2 \leqslant i \leqslant h$ take $C(i, d + h + 1 - i) = C(d + 2 - i, d + h - 1 + i) = t_2$ and $C(d+i, d+h+1-i) = t_1$. If f is odd then take $C(1, d+h) = \infty_f$, $C(d+1, d+h) = C(1, n) = t_2$ and $C(d + 1, n) = t_1$ whereas if f is even, take $C(1, d + h) = t_2$ and $C(d + 1, d + h) = t_1$.

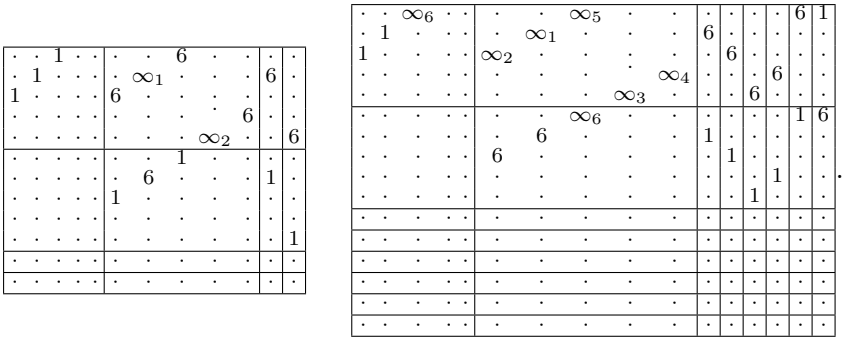
Finally, if $f = d + 1$ then construct the contour for $f = d$ as above, then vary it by taking $C(1, h) = C(d + 1, d + h) = \infty_{d+1}$, $C(1, n) = t_1$ and $C(d + 1, n) = t_2$.

For $1 \leqslant f \leqslant d + 1$, we add an arbitrary subquasigroup on the fixed points of β. □

Examples : (1) $d = 5, f = 0$, (ii) $d = 5, f = 1$.



(iii) $d = 5, f = 2$, (iv) $d = 5, f = 6$.



Next we look at β with two unequal length non-trivial cycles.

Theorem 3.5.15. *Let $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathcal{P}_n$. Let the cycle structure of β be $d_1 \cdot d_2 \cdot 1^f$, where $d_1 > d_2 > 1$. Then $\sigma \in \mathrm{Par}(n)$ if and only if d_1/d_2 is an odd integer and $f = 0$.*

Proof. Suppose σ is an autoparatopism of a Latin square L. Let $(i, j, k) \in O(L)$ be such that $o_\beta(i) = d_1$ and $o_\beta(j) = d_2$. If $o_\beta(k) = c$, then by Lemma 3.3.2,

$$\mathrm{lcm}(2d_1, 2d_2) = \mathrm{lcm}(2d_1, c) = \mathrm{lcm}(2d_2, c).$$

This rules out $c \in \{1, d_2\}$ given that $d_1 > d_2 > 1$. Therefore $c = d_1$ and $\mathrm{lcm}(2d_1, 2d_2) = 2d_1$. Hence $d_2 \mid d_1$. Now suppose that $d_1/d_2 = 2a$ is even. Then

$$(i, j, k)\sigma^{2ad_2} = (i\beta^{ad_2}, j\beta^{ad_2}, k\beta^{2ad_2}) = (i\beta^{ad_2}, j, k)$$

But $i\beta^{ad_2} \neq i$ since $d_1 > ad_2$. This is a contradiction. Hence d_1/d_2 is odd.

Suppose $m \geqslant 1$ and apply Theorem 3.5.5 with $d = d_1$. The set Γ contains all fixed points of γ, so it cannot contain the d_2-cycle. This must be because d_2 is even, from which we conclude that d_1 is even, so $\Gamma = \emptyset$. Therefore $f = 0$ after all.

Conversely suppose d_1/d_2 is an odd integer and $f = 0$. Taking $\Lambda = \{d_2\}$ in Theorem 3.3.4 shows that the d_2-cycles induce a subsquare. This subsquare can be built, by Corollary 3.5.9. For the remainder of the contour, we consider three cases.

(i) When d_1 and d_2 are even, take

$$\begin{aligned} C(i, d_1 + 1 - i) &= t_2, && \text{for } 1 \leqslant i \leqslant d_2/2, \\ C(i, d_1 + 1 - i) &= t_1, && \text{for } d_2/2 + 1 \leqslant i \leqslant d_1/2, \\ C(i, n + 1 - i) = C(d_1 + i, d_1 + 1 - i) &= t_1, && \text{for } 1 \leqslant i \leqslant d_2/2. \end{aligned}$$

(ii) If $d_1 \equiv 1 \mod 4$, take

$$\begin{aligned} C(i, d_1 + 1 - i) &= t_1, && \text{for } (d_1 + 2d_2 + 5)/4 \leqslant i \leqslant (3d_1 + 1)/4, \\ C(i, d_1 + 1 - i) &= t_2, && \text{for } (d_1 + 3)/4 \leqslant i \leqslant (d_1 + 2d_2 + 1)/4, \\ C(i, (5d_1 + 2d_2 + 5)/4 - i) &= t_1, && \text{for } (d_1 - 2d_2 + 5)/4 \leqslant i \leqslant (d_1 + 2d_2 + 1)/4. \end{aligned}$$

(iii) If $d_1 \equiv 3 \mod 4$, take

$$\begin{aligned} C(i, d_1 + 1 - i) &= t_1, && \text{for } (d_1 + 5)/4 \leqslant i \leqslant (3d_1 - 2d_2 + 1)/4, \\ C(i, d_1 + 1 - i) &= t_2, && \text{for } (3d_1 - 2d_2 + 5)/4 \leqslant i \leqslant (3d_1 + 3)/4, \\ C(i, (7d_1 + 2d_2 + 5)/4 - i) &= t_1, && \text{for } (3d_1 - 2d_2 + 5)/4 \leqslant i \leqslant (3d_1 + 2d_2 + 1)/4. \end{aligned}$$

□

Our final result allows the shorter non-trivial cycle length of β to be repeated.

Theorem 3.5.16. *Let $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathcal{P}_n$. Suppose that the cycle structure of β is $d_1 \cdot {d_2}^l$, where d_1 is even, and d_1/d_2 is an odd integer. Then $\sigma \in \mathrm{Par}(n)$ if and only if $0 \leqslant l \leqslant d_1/d_2$.*

Proof. Suppose that L is such that $\sigma \in \mathrm{Par}(L)$. By Theorem 3.3.4, if $l > 0$ then L has a subsquare S induced by the cycles of length d_2. The order of S is at most $n/2$, which means that $ld_2 \leqslant d_1$.

Conversely, suppose that $0 \leqslant l \leqslant d_1/d_2$. The subsquare S can be constructed by Corollary 3.5.9. A contour for the rest of L is as follows. We take

$$\begin{aligned} C(i, d_1 + 1 - i) &= t_{k+1}, && \text{for } 1 \leqslant k \leqslant l, \\ C(i, d_1 + 1 - i) &= t_1, && \text{for } l < k \leqslant d_1/d_2, \\ C(i, d_1 + (3k-1)d_2/2 + 1 - i) &= t_1, && \text{for } 1 \leqslant k \leqslant l, \\ C(d_1 + (k-1)d_2/2 + i, d_1 + 1 - i) &= t_1, && \text{for } 1 \leqslant k \leqslant l, \end{aligned}$$

for $(k-1)d_2/2 + 1 \leqslant i \leqslant kd_2/2$. □

In this section we have demonstrated several conditions that $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ necessarily satisfy. In some of the simpler subcases we were also able to provide sufficient conditions. We have included these as examples of the types of results which may be obtained. However, given the complexities involved, we are not optimistic that $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ can be completely characterised for general n.

3.6 Autoparatopisms of the form $(\alpha, \beta, \gamma; (123))$

By Theorem 3.2.2, whether $\sigma = (\alpha, \beta, \gamma; (123))$ is in $\mathrm{Par}(n)$ depends only on the cycle structure of $\alpha\beta\gamma$. Hence it is enough to study paratopisms of the form $(\varepsilon, \varepsilon, \gamma; (123))$, which is what we do in this section. The approach is very similar to the previous section. We begin by proving some necessary conditions.

Theorem 3.6.1. *Let $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathcal{P}_n$. Fix an integer d and let r be the number of cycles of γ that have length d. Suppose that γ has no two cycles of lengths d', d'' where $d \notin \{d', d''\}$ and $\mathrm{lcm}(d, d') = \mathrm{lcm}(d, d'') = \mathrm{lcm}(d', d'')$. Then $\sigma \notin \mathrm{Par}(n)$ if*

(i) $r = 1$ and $n + d \equiv 1 \mod 3$, or

(ii) $3 \mid d$ and $3 \nmid nr$.

Proof. The result is trivial if $r = 0$, so assume $r \geqslant 1$. Suppose that $\sigma \in \mathrm{Par}(L)$ for a Latin square L. Define $\Omega = \{i \in [n] : o_\gamma(i) = d\}$. Let X be the submatrix of L induced by the rows and columns indexed by Ω. Suppose that $(i, j, k) \in O(L)$ where $i \in \Omega$ and $k \notin \Omega$. Then $j \in \Omega$ by Lemma 3.3.3 and our assumption on cycle lengths of γ. In other words, the $n - rd$ symbols that are not in Ω have to occur in every row of X. This accounts for $rd(n - rd)$ of the $(rd)^2$ entries in X. The remaining entries will all be in orbits of length $3d$ or in short orbits of length d. If $3 \mid d$ then there are no short orbits so we must have $3d \mid rd(2rd - n)$, which implies that $3 \mid rn$. On the other hand, if $r = 1$ there is at most one short orbit. In this case, either $3d \mid d(2d - n)$ or $3d \mid d(2d - n) - d$. Both these conditions imply that $n + d \not\equiv 1 \mod 3$. □

Theorem 3.6.2. *Suppose that $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$, where γ has cycle structure d^r. Then*

(i) if $3 \mid d$ *then* $3 \mid r$ *and*
(ii) if $6 \mid d$ *then* $6 \mid r$.

Proof. Without loss of generality we assume that γ is the canonical permutation with cycle structure d^r. Suppose there exist a Latin square L of order n such that $\sigma \in \mathrm{Par}(L)$. Define $\psi : O(L) \mapsto \mathbb{Z}_d$ by $\psi(i,j,k) \equiv j - i \mod d$. We assume throughout that $3 \mid d$, so that each orbit of σ has length $3d$, by Lemma 3.2.4. Note that ψ is constant on orbits of $\sigma^3 = (\gamma, \gamma, \gamma; \varepsilon)$, by our choice of γ. Define T to be the sum, modulo d, of ψ over one representative from each orbit of σ^3. Observe that

$$\psi(i,j,k) + \psi(k\gamma, i, j) + \psi(j\gamma, k\gamma, i) = j - j\gamma \equiv -1 \mod d.$$

Hence each orbit of σ contributes -1 to T. There are $n^2/(3d) = r^2 d$ orbits of σ, so $T = -r^2 d/3$. Counting the same quantity by taking ψ of each triple in each row indexed by a multiple of d we find that,

$$-\frac{r^2 d}{3} \equiv r \sum_{i=1}^{n} i = \frac{rn(n+1)}{2} = \frac{r^2 d(rd+1)}{2} \equiv \begin{cases} 0, & \text{if } r \text{ is even or } d \text{ is odd,} \\ d/2, & \text{if } r \text{ is odd and } d \text{ is even,} \end{cases}$$

modulo d. Therefore, either $r^2/3$ or $r^2/3 + 1/2$ must be an integer, but the latter option is impossible. We conclude that $3 \mid r$ and either r is even or d is odd. The result follows. □

Theorem 3.6.2 rules out several classes of autoparatopisms $(\varepsilon, \varepsilon, \gamma; (123))$ where γ is semi-regular (has all cycle lengths equal). There is one more case of non-existence where γ is semi-regular, but it seems to be isolated and not part of a family.

Theorem 3.6.3. *If* γ *has cycle structure* 5^2 *then* $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \notin \mathrm{Par}(10)$.

Proof. Suppose $\sigma \in \mathrm{Par}(L)$. There are at most two short orbits of σ and there are $20 \equiv 2 \mod 3$ orbits of σ^3, so both M_{11} and M_{22} must contain a short orbit. The orbits of σ that hit the M_{12} block account for 5 of the remaining 8 orbits of σ^3 in $M_{11} \cup M_{22}$. Hence we may suppose without loss of generality that there is an orbit of σ that is contained entirely within M_{11}. This orbit must hit at least one of the cells $(1,1)$ or $(1,2)$ since it hits 3 cells in the first row, and $(1,4)$ is in the short orbit. However, a straightforward exhaustion of the possibilities shows that no symbol is viable in either $(1,1)$ or $(1,2)$. □

Just as we did in the previous section we now seemingly depart from our agenda in terms of the form of paratopisms we consider. However, the result we prove will have corollaries relevant to our agenda.

Theorem 3.6.4. *Suppose* $\sigma = (\alpha, \alpha, \alpha; (123)) \in \mathcal{P}_n$, *where* $\alpha \in \mathcal{S}_n$ *has cycle structure* $d^1 \cdot 1^f$. *Then* $\sigma \in \mathrm{Par}(n)$ *if and only if*

(i) $f \equiv 0 \mod 3$ *and* $d \not\equiv 2 \mod 3$, *with* d *odd in the case* $f = 0$,
(ii) $f \equiv 1 \mod 3$, *with* $d \not\equiv 5 \mod 6$ *in the case* $f = 1$, *or*
(iii) $f \equiv 2 \mod 3$ *and* $d \not\equiv 1 \mod 3$.

Proof. The following example has an autoparatopism $(\alpha, \alpha, \alpha; (123))$ where α is the canonical permutation with cycle structure $9^1 \cdot 1^1$.

$$\left[\begin{array}{cccccccccc}
8 & 10 & 3 & 7 & 4 & 5 & 2 & 1 & 6 & 9 \\
6 & 9 & 5 & 1 & 8 & 2 & 7 & 3 & 10 & 4 \\
3 & 8 & 7 & 10 & 5 & 9 & 6 & 4 & 1 & 2 \\
5 & 4 & 9 & 2 & 10 & 6 & 1 & 7 & 8 & 3 \\
1 & 6 & 10 & 9 & 3 & 8 & 4 & 2 & 5 & 7 \\
9 & 7 & 4 & 6 & 2 & 1 & 10 & 8 & 3 & 5 \\
4 & 1 & 2 & 8 & 7 & 3 & 5 & 10 & 9 & 6 \\
7 & 5 & 8 & 4 & 9 & 10 & 3 & 6 & 2 & 1 \\
10 & 2 & 6 & 3 & 1 & 7 & 9 & 5 & 4 & 8 \\
2 & 3 & 1 & 5 & 6 & 4 & 8 & 9 & 7 & 10
\end{array}\right]$$

Theorem 3.3.11 shows $\sigma \in \mathrm{Par}(n)$ in all other cases where we are claiming existence.

Now suppose $\sigma \in \mathrm{Par}(L)$. Corollary 3.3.10 shows that d must be odd when $f = 0$.

For the remainder of the proof, assume that $3 \nmid d$. Then, $(i, j, k)\sigma^d = (k, i, j)$ when $d \equiv 1 \mod 3$ and $(i, j, k)\sigma^{2d} = (j, k, i)$ when $d \equiv 2 \mod 3$. Hence, L is semi-symmetric. Also

$$(i, j, k)\sigma^{2d+1} = (i\alpha, j\alpha, k\alpha) \in O(L) \text{ when } d \equiv 1 \mod 3,$$
$$(i, j, k)\sigma^{n+1} = (i\alpha, j\alpha, k\alpha) \in O(L) \text{ when } d \equiv 2 \mod 3.$$

Therefore, $\theta = (\alpha, \alpha, \alpha) \in \mathcal{S}_n^3$ is an autotopism of L. But, by [9, Thrm 2.3], θ is not an autotopism of any semi-symmetric Latin square L in the following cases: $d \equiv 2 \mod 3$ and $f \equiv 0 \mod 3$, or $d \equiv 5 \mod 6$ and $f = 1$, or $d \equiv 1 \mod 3$ and $f \equiv 2 \mod 3$. □

Corollary 3.6.5. Let $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathcal{P}_n$, where γ has cycle structure $d^1 1^f$ and $3 \nmid d$. Then $\sigma \in \mathrm{Par}(n)$ if and only if

(i) $f \equiv 0 \mod 3$ and $d \equiv 1 \mod 3$, with d odd in the case $f = 0$,

(ii) $f \equiv 1 \mod 3$, with $d \not\equiv 5 \mod 6$ in the case $f = 1$, or

(iii) $f \equiv d \equiv 2 \mod 3$.

Proof. As $3 \nmid d$ we see that $\gamma \sim \gamma^3$ so σ is conjugate to $(\gamma, \gamma, \gamma; (123))$ in $\mathcal{P}_n$, by Theorem 3.2.2. The result now follows from Theorem 3.6.4. □

Corollary 3.6.6. Let $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathcal{P}_n$, where γ has cycle structure n^1. Then $\sigma \in \mathrm{Par}(n)$ if and only if $n \equiv 1 \mod 6$.

Proof. If $3 \mid n$ then Theorem 3.6.2 shows that $\sigma \notin \mathrm{Par}(n)$. If $3 \nmid n$ then we apply Corollary 3.6.5. □

Corollary 3.6.7. Let $\sigma = (\varepsilon, \varepsilon, \gamma; (123)) \in \mathcal{P}_n$ where γ has cycle structure d^3. Then $\sigma \in \mathrm{Par}(n)$ if and only if d is odd.

Proof. Let $\alpha \in \mathcal{S}_n$ be a single cycle of length $3d$ so that α^3 has cycle structure d^3. Then $\sigma' = (\alpha, \alpha, \alpha; (123))$ is conjugate to σ in $\mathcal{P}_n$, by Theorem 3.2.2. Now apply Theorem 3.6.4(i). □

We have proved several general necessary conditions for $(\varepsilon, \varepsilon, \gamma; (123))$ to be in $\mathrm{Par}(n)$, and provided complete characterisations of some simple cases. It is time to bring all our results from this section and the previous one together.

$n=2$ β	γ
1^2	1^2
2	2

$n=3$ β	γ
1^3	$1^3, 2{\cdot}1$
3	$2{\cdot}1, 3$

$n=4$ β	γ
1^4	$1^4, 2{\cdot}1^2$
2^2	$2{\cdot}1^2, 2^2, 4$
$3{\cdot}1$	$3{\cdot}1$
4	$2^2, 4$

$n=5$ β	γ
1^5	$1^5, 2{\cdot}1^3, 2^2{\cdot}1$
$2^2{\cdot}1$	$4{\cdot}1$
5	$2^2{\cdot}1, 5$

$n=6$ β	γ
1^6	$1^6, 2{\cdot}1^4, 2^2{\cdot}1^2$
$2^2{\cdot}1^2$	$4{\cdot}1^2$
2^3	$2^3, 4{\cdot}2$
$3{\cdot}1^3$	$3{\cdot}2{\cdot}1$
3^2	$2{\cdot}1^4, 2^2{\cdot}1^2, 3{\cdot}1^3, 3{\cdot}2{\cdot}1, 3^2$
$5{\cdot}1$	$5{\cdot}1$
6	$2^3, 4{\cdot}2, 6$

$n=7$ β	γ
1^7	$1^7, 2{\cdot}1^5, 2^2{\cdot}1^3, 2^3{\cdot}1$
$2^2{\cdot}1^3$	$4{\cdot}2{\cdot}1$
$3^2{\cdot}1$	$3^2{\cdot}1, 6{\cdot}1$
7	$2^3{\cdot}1, 7$

$n=8$ β	γ
1^8	$1^8, 2{\cdot}1^6, 2^2{\cdot}1^4, 2^3{\cdot}1^2$
$2^2{\cdot}1^4$	$4{\cdot}2{\cdot}1^2$
2^4	$2{\cdot}1^6, 2^2{\cdot}1^4, 2^3{\cdot}1^2, 2^4,$ $4{\cdot}1^4, 4{\cdot}2{\cdot}1^2, 4{\cdot}2^2, 4^2$
$3^2{\cdot}1^2$	$3^2{\cdot}1^2, 6{\cdot}1^2$
4^2	$2^2{\cdot}1^4, 2^3{\cdot}1^2, 2^4, 4{\cdot}1^4,$ $4{\cdot}2{\cdot}1^2, 4{\cdot}2^2, 4^2, 8$
$5{\cdot}1^3$	$5{\cdot}2{\cdot}1$
$6{\cdot}2$	$3^2{\cdot}2, 6{\cdot}2$
$7{\cdot}1$	$7{\cdot}1$
8	$2^4, 4{\cdot}2^2, 4^2, 8$

$n=9$ β	γ
1^9	$1^9, 2{\cdot}1^7, 2^2{\cdot}1^5, 2^3{\cdot}1^3, 2^4{\cdot}1$
$2^4{\cdot}1$	$4^2{\cdot}1$
$3^2{\cdot}1^3$	$3^2{\cdot}1^3, 3^2{\cdot}2{\cdot}1, 6{\cdot}1^3, 6{\cdot}2{\cdot}1$
3^3	$2^3{\cdot}1^3, 2^4{\cdot}1, 3{\cdot}2^2{\cdot}1^2, 3{\cdot}2^3,$ $3^2{\cdot}2{\cdot}1, 3^3, 6{\cdot}1^3, 6{\cdot}2{\cdot}1, 6{\cdot}3$
$4^2{\cdot}1$	$8{\cdot}1$
9	$2^4{\cdot}1, 3{\cdot}2^3, 6{\cdot}2{\cdot}1, 6{\cdot}3, 9$

$n=10$ β	γ
1^{10}	$1^{10}, 2{\cdot}1^8, 2^2{\cdot}1^6, 2^3{\cdot}1^4, 2^4{\cdot}1^2$
$2^4{\cdot}1^2$	$4^2{\cdot}1^2$
2^5	$2^5, 4{\cdot}2^3, 4^2{\cdot}2$
$3^2{\cdot}1^4$	$3^2{\cdot}1^4, 3^2{\cdot}2{\cdot}1^2, 6{\cdot}1^4, 6{\cdot}2{\cdot}1^2$
$3^3{\cdot}1$	$3^3{\cdot}1, 6{\cdot}3{\cdot}1$
$4^2{\cdot}1^2$	$8{\cdot}1^2$
$4^2{\cdot}2$	$8{\cdot}2$
$5{\cdot}1^5$	$5{\cdot}2^2{\cdot}1$
5^2	$2^2{\cdot}1^6, 2^3{\cdot}1^4, 2^4{\cdot}1^2, 5{\cdot}1^5, 5{\cdot}2{\cdot}1^3, 5{\cdot}2^2{\cdot}1, 5^2$
$6{\cdot}2^2$	$6{\cdot}2^2, 6{\cdot}4$
$7{\cdot}1^3$	$7{\cdot}2{\cdot}1$
$9{\cdot}1$	$9{\cdot}1$
10	$2^5, 4{\cdot}2^3, 4^2{\cdot}2, 10$

$n=11$ β	γ
1^{11}	$1^{11}, 2{\cdot}1^9, 2^2{\cdot}1^7, 2^3{\cdot}1^5, 2^4{\cdot}1^3, 2^5{\cdot}1$
$2^4{\cdot}1^3$	$4^2{\cdot}1^3, 4^2{\cdot}2{\cdot}1$
$3^2{\cdot}1^5$	$3^2{\cdot}2{\cdot}1^3, 3^2{\cdot}2^2{\cdot}1, 6{\cdot}2{\cdot}1^3, 6{\cdot}2^2{\cdot}1$
$3^3{\cdot}1^2$	$6{\cdot}3{\cdot}1^2$
$4^2{\cdot}1^3$	$8{\cdot}1^3, 8{\cdot}2{\cdot}1$
$5^2{\cdot}1$	$5^2{\cdot}1, 10{\cdot}1$
11	$2^5{\cdot}1, 11$

$n=12$ β	γ
1^{12}	$1^{12}, 2{\cdot}1^{10}, 2^2{\cdot}1^8, 2^3{\cdot}1^6, 2^4{\cdot}1^4, 2^5{\cdot}1^2$
$2^4{\cdot}1^4$	$4^2{\cdot}1^4, 4^2{\cdot}2{\cdot}1^2$
2^6	$2{\cdot}1^{10}, 2^2{\cdot}1^8, 2^3{\cdot}1^6, 2^4{\cdot}1^4, 2^5{\cdot}1^2, 2^6, 4{\cdot}1^8, 4{\cdot}2{\cdot}1^6,$ $4{\cdot}2^2{\cdot}1^4, 4{\cdot}2^3{\cdot}1^2, 4{\cdot}2^4, 4^2{\cdot}1^4, 4^2{\cdot}2{\cdot}1^2, 4^2{\cdot}2^2, 4^3$
$3^2{\cdot}1^6$	$3^2{\cdot}2{\cdot}1^4, 3^2{\cdot}2^2{\cdot}1^2, 6{\cdot}2{\cdot}1^4, 6{\cdot}2^2{\cdot}1^2$
$3^3{\cdot}1^3$	$3^3{\cdot}1^3, 3^3{\cdot}2{\cdot}1, 6{\cdot}3{\cdot}1^3, 6{\cdot}3{\cdot}2{\cdot}1$
3^4	$2{\cdot}1^{10}, 2^2{\cdot}1^8, 2^3{\cdot}1^6, 2^4{\cdot}1^4, 2^5{\cdot}1^2,$ $3{\cdot}1^9, 3{\cdot}2{\cdot}1^7, 3{\cdot}2^2{\cdot}1^5, 3{\cdot}2^3{\cdot}1^3, 3{\cdot}2^4{\cdot}1,$ $3^2{\cdot}1^6, 3^2{\cdot}2{\cdot}1^4, 3^2{\cdot}2^2{\cdot}1^2, 3^2{\cdot}2^3, 3^3{\cdot}1^3, 3^3{\cdot}2{\cdot}1, 3^4,$ $6{\cdot}1^6, 6{\cdot}2{\cdot}1^4, 6{\cdot}2^2{\cdot}1^2, 6{\cdot}3{\cdot}1^3, 6{\cdot}3{\cdot}2{\cdot}1, 6{\cdot}3^2$
$4^2{\cdot}1^4$	$8{\cdot}1^4, 8{\cdot}2{\cdot}1^2$
$4^2{\cdot}2^2$	$8{\cdot}2{\cdot}1^2, 8{\cdot}2^2, 8{\cdot}4$
4^3	$2^6, 4{\cdot}2^4, 4^2{\cdot}2^2, 4^3, 8{\cdot}2^2, 8{\cdot}4$
$5^2{\cdot}1^2$	$5^2{\cdot}1^2, 10{\cdot}1^2$
$6{\cdot}2^3$	$3^2{\cdot}2^3, 4{\cdot}3^2{\cdot}2, 6{\cdot}2^3, 6{\cdot}4{\cdot}2$
6^2	$2^3{\cdot}1^6, 2^4{\cdot}1^4, 2^5{\cdot}1^2, 2^6, 3{\cdot}2^2{\cdot}1^5, 3{\cdot}2^3{\cdot}1^3, 3{\cdot}2^4{\cdot}1,$ $3^2{\cdot}2{\cdot}1^4, 3^2{\cdot}2^2{\cdot}1^2, 3^2{\cdot}2^3, 3^3{\cdot}2{\cdot}1, 4{\cdot}2{\cdot}1^6,$ $4{\cdot}2^2{\cdot}1^4, 4{\cdot}2^3{\cdot}1^2, 4{\cdot}2^4, 4{\cdot}3{\cdot}1^5, 4{\cdot}3{\cdot}2{\cdot}1^3, 4{\cdot}3{\cdot}2^2{\cdot}1,$ $4{\cdot}3^2{\cdot}1^2, 4{\cdot}3^2{\cdot}2, 4^2{\cdot}1^4, 4^2{\cdot}2{\cdot}1^2, 4^2{\cdot}2^2, 4^2{\cdot}3{\cdot}1, 4^3,$ $6{\cdot}1^6, 6{\cdot}2{\cdot}1^4, 6{\cdot}2^2{\cdot}1^2, 6{\cdot}2^3, 6{\cdot}3{\cdot}1^3, 6{\cdot}3{\cdot}2{\cdot}1, 6{\cdot}3^2,$ $6{\cdot}4{\cdot}1^2, 6{\cdot}4{\cdot}2, 6^2, 12$
$7{\cdot}1^5$	$7{\cdot}2^2{\cdot}1$
$9{\cdot}1^3$	$9{\cdot}2{\cdot}1$
$9{\cdot}3$	$9{\cdot}2{\cdot}1, 9{\cdot}3$
$10{\cdot}2$	$5^2{\cdot}2, 10{\cdot}2$
$11{\cdot}1$	$11{\cdot}1$
12	$2^6, 4{\cdot}2^4, 4^2{\cdot}2^2, 4^3, 6{\cdot}2^3, 6{\cdot}4{\cdot}2, 6^2, 8{\cdot}2^2, 8{\cdot}4, 12$

Table 3.1: Cycle structures of β and γ such that $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ for $n \leqslant 12$.

$n = 13$ β	γ
1^{13}	$1^{13}, 2{\cdot}1^{11}, 2^2{\cdot}1^9, 2^3{\cdot}1^7, 2^4{\cdot}1^5, 2^5{\cdot}1^3, 2^6{\cdot}1$
$2^4{\cdot}1^5$	$4^2{\cdot}1^5, 4^2{\cdot}2{\cdot}1^3, 4^2{\cdot}2^2{\cdot}1$
$2^6{\cdot}1$	$4^3{\cdot}1$
$3^3{\cdot}1^4$	$6{\cdot}3{\cdot}2{\cdot}1^2$
$3^4{\cdot}1$	$3^4{\cdot}1, 6{\cdot}3^2{\cdot}1, 6^2{\cdot}1$
$4^2{\cdot}1^5$	$8{\cdot}2{\cdot}1^3, 8{\cdot}2^2{\cdot}1$
$4^2{\cdot}2^2{\cdot}1$	$8{\cdot}4{\cdot}1$
$5^2{\cdot}1^3$	$5^2{\cdot}1^3, 5^2{\cdot}2{\cdot}1, 10{\cdot}1^3, 10{\cdot}2{\cdot}1$
$6^2{\cdot}1$	$12{\cdot}1$
13	$2^6{\cdot}1, 13$

$n = 14$ β	γ
1^{14}	$1^{14}, 2{\cdot}1^{12}, 2^2{\cdot}1^{10}, 2^3{\cdot}1^8, 2^4{\cdot}1^6, 2^5{\cdot}1^4, 2^6{\cdot}1^2$
$2^4{\cdot}1^6$	$4^2{\cdot}1^6, 4^2{\cdot}2{\cdot}1^4, 4^2{\cdot}2^2{\cdot}1^2$
$2^6{\cdot}1^2$	$4^3{\cdot}1^2$
2^7	$2^7, 4{\cdot}2^5, 4^2{\cdot}2^3, 4^3{\cdot}2$
$3^3{\cdot}1^5$	$3^3{\cdot}2{\cdot}1^3, 3^3{\cdot}2^2{\cdot}1, 6{\cdot}3{\cdot}2{\cdot}1^3, 6{\cdot}3{\cdot}2^2{\cdot}1$
$3^4{\cdot}1^2$	$3^4{\cdot}1^2, 6{\cdot}3^2{\cdot}1^2, 6^2{\cdot}1^2$
$4^2{\cdot}1^6$	$8{\cdot}2{\cdot}1^4, 8{\cdot}2^2{\cdot}1^2$
$4^2{\cdot}2^2{\cdot}1^2$	$8{\cdot}4{\cdot}1^2$
$4^2{\cdot}2^3$	$8{\cdot}2^3, 8{\cdot}4{\cdot}2$
$5^2{\cdot}1^4$	$5^2{\cdot}1^4, 5^2{\cdot}2{\cdot}1^2, 10{\cdot}1^4, 10{\cdot}2{\cdot}1^2$
$6^2{\cdot}1^2$	$12{\cdot}1^2$
$6^2{\cdot}2$	$6^2{\cdot}2, 12{\cdot}2$
$7{\cdot}1^7$	$7{\cdot}2^3{\cdot}1$
7^2	$2^3{\cdot}1^8, 2^4{\cdot}1^6, 2^5{\cdot}1^4, 2^6{\cdot}1^2,$ $7{\cdot}1^7, 7{\cdot}2{\cdot}1^5, 7{\cdot}2^2{\cdot}1^3, 7{\cdot}2^3{\cdot}1, 7^2$
$9{\cdot}1^5$	$9{\cdot}2^2{\cdot}1$
$10{\cdot}2^2$	$10{\cdot}2^2, 10{\cdot}4$
$11{\cdot}1^3$	$11{\cdot}2{\cdot}1$
$13{\cdot}1$	$13{\cdot}1$
14	$2^7, 4{\cdot}2^5, 4^2{\cdot}2^3, 4^3{\cdot}2, 14$

$n = 15$ β	γ
1^{15}	$1^{15}, 2{\cdot}1^{13}, 2^2{\cdot}1^{11}, 2^3{\cdot}1^9,$ $2^4{\cdot}1^7, 2^5{\cdot}1^5, 2^6{\cdot}1^3, 2^7{\cdot}1$
$2^4{\cdot}1^7$	$4^2{\cdot}2{\cdot}1^5, 4^2{\cdot}2^2{\cdot}1^3, 4^2{\cdot}2^3{\cdot}1$
$2^6{\cdot}1^3$	$4^3{\cdot}1^3, 4^3{\cdot}2{\cdot}1$
$3^4{\cdot}1^3$	$3^4{\cdot}1^3, 3^4{\cdot}2{\cdot}1, 6{\cdot}3^2{\cdot}1^3, 6{\cdot}3^2{\cdot}2{\cdot}1, 6^2{\cdot}1^3, 6^2{\cdot}2{\cdot}1$
3^5	$2^5{\cdot}1^5, 2^6{\cdot}1^3, 2^7{\cdot}1, 3{\cdot}2^4{\cdot}1^4, 3{\cdot}2^5{\cdot}1^2, 3{\cdot}2^6,$ $3^2{\cdot}2^3{\cdot}1^3, 3^2{\cdot}2^4{\cdot}1, 3^3{\cdot}2^2{\cdot}1^2, 3^3{\cdot}2^3,$ $3^4{\cdot}2{\cdot}1, 3^5, 6{\cdot}2^2{\cdot}1^5, 6{\cdot}2^3{\cdot}1^3, 6{\cdot}2^4{\cdot}1,$ $6{\cdot}3{\cdot}2{\cdot}1^4, 6{\cdot}3{\cdot}2^2{\cdot}1^2, 6{\cdot}3{\cdot}2^3, 6{\cdot}3^2{\cdot}1^3,$ $6{\cdot}3^2{\cdot}2{\cdot}1, 6{\cdot}3^3, 6^2{\cdot}1^3, 6^2{\cdot}2{\cdot}1, 6^2{\cdot}3$
$4^2{\cdot}1^7$	$8{\cdot}2^2{\cdot}1^3, 8{\cdot}2^3{\cdot}1$
$5^2{\cdot}1^5$	$5^2{\cdot}1^5, 5^2{\cdot}2{\cdot}1^3, 5^2{\cdot}2^2{\cdot}1,$ $10{\cdot}1^5, 10{\cdot}2{\cdot}1^3, 10{\cdot}2^2{\cdot}1$
5^3	$2^6{\cdot}1^3, 2^7{\cdot}1, 5{\cdot}2^4{\cdot}1^2, 5{\cdot}2^5, 5^2{\cdot}2^2{\cdot}1, 5^3,$ $10{\cdot}2{\cdot}1^3, 10{\cdot}2^2{\cdot}1, 10{\cdot}5$
$6^2{\cdot}1^3$	$12{\cdot}1^3, 12{\cdot}2{\cdot}1$
$6^2{\cdot}3$	$4^3{\cdot}2{\cdot}1, 4^3{\cdot}3, 12{\cdot}2{\cdot}1, 12{\cdot}3$
$7^2{\cdot}1$	$7^2{\cdot}1, 14{\cdot}1$
15	$2^7{\cdot}1, 3{\cdot}2^6, 5{\cdot}2^5, 6{\cdot}2^4{\cdot}1, 6{\cdot}3{\cdot}2^3, 6{\cdot}5{\cdot}2^2,$ $6^2{\cdot}2{\cdot}1, 6^2{\cdot}3, 10{\cdot}2^2{\cdot}1, 10{\cdot}3{\cdot}2, 10{\cdot}5, 15$

$n = 16$ β	γ
1^{16}	$1^{16}, 2{\cdot}1^{14}, 2^2{\cdot}1^{12}, 2^3{\cdot}1^{10}, 2^4{\cdot}1^8, 2^5{\cdot}1^6, 2^6{\cdot}1^4, 2^7{\cdot}1^2$
$2^4{\cdot}1^8$	$4^2{\cdot}2{\cdot}1^6, 4^2{\cdot}2^2{\cdot}1^4, 4^2{\cdot}2^3{\cdot}1^2$
$2^6{\cdot}1^4$	$4^3{\cdot}1^4, 4^3{\cdot}2{\cdot}1^2$
2^8	$2{\cdot}1^{14}, 2^2{\cdot}1^{12}, 2^3{\cdot}1^{10}, 2^4{\cdot}1^8, 2^5{\cdot}1^6, 2^6{\cdot}1^4, 2^7{\cdot}1^2, 2^8,$ $4{\cdot}1^{12}, 4{\cdot}2{\cdot}1^{10}, 4{\cdot}2^2{\cdot}1^8, 4{\cdot}2^3{\cdot}1^6, 4{\cdot}2^4{\cdot}1^4, 4{\cdot}2^5{\cdot}1^2, 4{\cdot}2^6,$ $4^2{\cdot}1^8, 4^2{\cdot}2{\cdot}1^6, 4^2{\cdot}2^2{\cdot}1^4, 4^2{\cdot}2^3{\cdot}1^2, 4^2{\cdot}2^4,$ $4^3{\cdot}1^4, 4^3{\cdot}2{\cdot}1^2, 4^3{\cdot}2^2, 4^4$
$3^3{\cdot}1^7$	$3^3{\cdot}2^2{\cdot}1^3, 3^3{\cdot}2^3{\cdot}1, 6{\cdot}3{\cdot}2^2{\cdot}1^3, 6{\cdot}3{\cdot}2^3{\cdot}1$
$3^4{\cdot}1^4$	$3^4{\cdot}1^4, 3^4{\cdot}2{\cdot}1^2, 6{\cdot}3^2{\cdot}1^4, 6{\cdot}3^2{\cdot}2{\cdot}1^2, 6^2{\cdot}1^4, 6^2{\cdot}2{\cdot}1^2$
$3^5{\cdot}1$	$3^5{\cdot}1, 6{\cdot}3^3{\cdot}1, 6^2{\cdot}3{\cdot}1$
$4^2{\cdot}1^8$	$8{\cdot}2^2{\cdot}1^4, 8{\cdot}2^3{\cdot}1^2$
$4^2{\cdot}2^4$	$8{\cdot}2^2{\cdot}1^4, 8{\cdot}2^3{\cdot}1^2, 8{\cdot}2^4, 8{\cdot}4{\cdot}1^4, 8{\cdot}4{\cdot}2{\cdot}1^2, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2$
4^4	$2^2{\cdot}1^{12}, 2^3{\cdot}1^{10}, 2^4{\cdot}1^8, 2^5{\cdot}1^6, 2^6{\cdot}1^4, 2^7{\cdot}1^2, 2^8,$ $4{\cdot}1^{12}, 4{\cdot}2{\cdot}1^{10}, 4{\cdot}2^2{\cdot}1^8, 4{\cdot}2^3{\cdot}1^6, 4{\cdot}2^4{\cdot}1^4, 4{\cdot}2^5{\cdot}1^2, 4{\cdot}2^6,$ $4^2{\cdot}1^8, 4^2{\cdot}2{\cdot}1^6, 4^2{\cdot}2^2{\cdot}1^4, 4^2{\cdot}2^3{\cdot}1^2, 4^2{\cdot}2^4,$ $4^3{\cdot}1^4, 4^3{\cdot}2{\cdot}1^2, 4^3{\cdot}2^2, 4^4, 8{\cdot}1^8, 8{\cdot}2{\cdot}1^6, 8{\cdot}2^2{\cdot}1^4,$ $8{\cdot}2^3{\cdot}1^2, 8{\cdot}2^4, 8{\cdot}4{\cdot}1^4, 8{\cdot}4{\cdot}2{\cdot}1^2, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2$
$5^2{\cdot}1^6$	$5^2{\cdot}1^6, 5^2{\cdot}2{\cdot}1^4, 5^2{\cdot}2^2{\cdot}1^2, 10{\cdot}1^6, 10{\cdot}2{\cdot}1^4, 10{\cdot}2^2{\cdot}1^2$
$5^3{\cdot}1$	$5^3{\cdot}1, 10{\cdot}5{\cdot}1$
$6^2{\cdot}1^4$	$12{\cdot}1^4, 12{\cdot}2{\cdot}1^2$
$6^2{\cdot}2^2$	$3^4{\cdot}2{\cdot}1^2, 3^4{\cdot}2^2, 4{\cdot}3^4, 6{\cdot}3^2{\cdot}2{\cdot}1^2, 6{\cdot}3^2{\cdot}2^2, 6{\cdot}4{\cdot}3^2,$ $6^2{\cdot}2{\cdot}1^2, 6^2{\cdot}2^2, 6^2{\cdot}4, 12{\cdot}2{\cdot}1^2, 12{\cdot}2^2, 12{\cdot}4$
$7^2{\cdot}1^2$	$7^2{\cdot}1^2, 14{\cdot}1^2$
8^2	$2^4{\cdot}1^8, 2^5{\cdot}1^6, 2^6{\cdot}1^4, 2^7{\cdot}1^2, 2^8, 4{\cdot}2^2{\cdot}1^8, 4{\cdot}2^3{\cdot}1^6, 4{\cdot}2^4{\cdot}1^4,$ $4{\cdot}2^5{\cdot}1^2, 4{\cdot}2^6, 4^2{\cdot}1^8, 4^2{\cdot}2{\cdot}1^6, 4^2{\cdot}2^2{\cdot}1^4, 4^2{\cdot}2^3{\cdot}1^2, 4^2{\cdot}2^4,$ $4^3{\cdot}1^4, 4^3{\cdot}2{\cdot}1^2, 4^3{\cdot}2^2, 8{\cdot}4{\cdot}1^4, 8{\cdot}4{\cdot}2{\cdot}1^2, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2, 16$
$10{\cdot}2^3$	$5^2{\cdot}2^3, 5^2{\cdot}4{\cdot}2, 10{\cdot}2^3, 10{\cdot}4{\cdot}2$
$12{\cdot}4$	$3^4{\cdot}2^2, 4{\cdot}3^4, 6{\cdot}3^2{\cdot}2^2, 6{\cdot}4{\cdot}3^2, 6^2{\cdot}2^2, 6^2{\cdot}4, 12{\cdot}2^2, 12{\cdot}4$
$14{\cdot}2$	$7^2{\cdot}2, 14{\cdot}2$
16	$2^8, 4{\cdot}2^6, 4^2{\cdot}2^4, 4^3{\cdot}2^2, 4^4, 8{\cdot}2^4, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2, 16$

$n = 17$ β	γ
1^{17}	$1^{17}, 2{\cdot}1^{15}, 2^2{\cdot}1^{13}, 2^3{\cdot}1^{11}, 2^4{\cdot}1^9, 2^5{\cdot}1^7, 2^6{\cdot}1^5, 2^7{\cdot}1^3, 2^8{\cdot}1$
$2^6{\cdot}1^5$	$4^3{\cdot}1^5, 4^3{\cdot}2{\cdot}1^3, 4^3{\cdot}2^2{\cdot}1$
$3^4{\cdot}1^5$	$3^4{\cdot}1^5, 3^4{\cdot}2{\cdot}1^3, 3^4{\cdot}2^2{\cdot}1,$ $6{\cdot}3^2{\cdot}1^5, 6{\cdot}3^2{\cdot}2{\cdot}1^3, 6{\cdot}3^2{\cdot}2^2{\cdot}1, 6^2{\cdot}1^5, 6^2{\cdot}2{\cdot}1^3, 6^2{\cdot}2^2{\cdot}1$
$3^5{\cdot}1^2$	$6{\cdot}3^3{\cdot}1^2, 6^2{\cdot}3{\cdot}1^2$
$5^2{\cdot}1^7$	$5^2{\cdot}2{\cdot}1^5, 5^2{\cdot}2^2{\cdot}1^3, 5^2{\cdot}2^3{\cdot}1, 10{\cdot}2{\cdot}1^5, 10{\cdot}2^2{\cdot}1^3, 10{\cdot}2^3{\cdot}1$
$6^2{\cdot}1^5$	$12{\cdot}1^5, 12{\cdot}2{\cdot}1^3, 12{\cdot}2^2{\cdot}1$
$7^2{\cdot}1^3$	$7^2{\cdot}1^3, 7^2{\cdot}2{\cdot}1, 14{\cdot}1^3, 14{\cdot}2{\cdot}1$
17	$2^8{\cdot}1, 17$

Table 3.2: Cycle structures of β and γ such that $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ for $13 \leqslant n \leqslant 17$.

$n = 2$ γ
1^2

$n = 3$ γ
$1^3, 2{\cdot}1$

$n = 4$ γ
$1^4, 2{\cdot}1^2, 2^2$

$n = 5$ γ
$1^5, 2^2{\cdot}1, 4{\cdot}1$

$n = 6$ γ
$1^6, 2^2{\cdot}1^2, 3{\cdot}1^3$

$n = 7$ γ
$1^7, 2^2{\cdot}1^3, 2^3{\cdot}1,$ $4{\cdot}1^3, 4{\cdot}2{\cdot}1, 5{\cdot}1^2, 7$

$n = 8$ γ
$1^8, 2^2{\cdot}1^4, 2^3{\cdot}1^2,$ $2^4, 4{\cdot}1^4, 4{\cdot}2{\cdot}1^2,$ $4{\cdot}2^2, 4^2, 7{\cdot}1$

$n = 9$ γ
$1^9, 2^3{\cdot}1^3, 2^4{\cdot}1,$ $3^2{\cdot}1^3, 3^3, 4^2{\cdot}1, 5{\cdot}1^4,$ $6{\cdot}1^3, 6{\cdot}2{\cdot}1, 8{\cdot}1$

$n = 10$ γ
$1^{10}, 2^3{\cdot}1^4, 2^4{\cdot}1^2, 3^3{\cdot}1,$ $4^2{\cdot}1^2, 5{\cdot}1^5, 7{\cdot}1^3, 8{\cdot}1^2$

$n = 11$ γ
$1^{11}, 2^3{\cdot}1^5, 2^4{\cdot}1^3, 2^5{\cdot}1, 3^3{\cdot}1^2,$ $4^2{\cdot}1^3, 4^2{\cdot}2{\cdot}1, 5^2{\cdot}1, 7{\cdot}1^4, 10{\cdot}1$

$n = 12$ γ
$1^{12}, 2^3{\cdot}1^6, 2^4{\cdot}1^4, 2^5{\cdot}1^2, 2^6,$ $3^2{\cdot}1^6, 3^3{\cdot}1^3, 4^2{\cdot}1^4, 4^2{\cdot}2{\cdot}1^2, 4^2{\cdot}2^2,$ $5^2{\cdot}1^2, 6{\cdot}1^6, 6{\cdot}2^2{\cdot}1^2, 6{\cdot}3{\cdot}1^3,$ $8{\cdot}1^4, 8{\cdot}2{\cdot}1^2, 8{\cdot}2^2, 9{\cdot}1^3$

$n = 13$ γ
$1^{13}, 2^4{\cdot}1^5, 2^5{\cdot}1^3, 2^6{\cdot}1, 3^3{\cdot}1^4,$ $4^2{\cdot}1^5, 4^2{\cdot}2^2{\cdot}1, 4^3{\cdot}1, 5^2{\cdot}1^3, 7{\cdot}1^6,$ $8{\cdot}1^5, 8{\cdot}2^2{\cdot}1, 8{\cdot}4{\cdot}1, 10{\cdot}1^3, 10{\cdot}2{\cdot}1,$ $11{\cdot}1^2, 13$

$n = 14$ γ
$1^{14}, 2^4{\cdot}1^6, 2^5{\cdot}1^4, 2^6{\cdot}1^2, 3^3{\cdot}1^5,$ $4^2{\cdot}1^6, 4^2{\cdot}2^2{\cdot}1^2, 4^3{\cdot}1^2, 5^2{\cdot}1^4,$ $7{\cdot}1^7, 7^2, 10{\cdot}1^4, 10{\cdot}2{\cdot}1^2, 13{\cdot}1$

$n = 15$ γ
$1^{15}, 2^4{\cdot}1^7, 2^5{\cdot}1^5, 2^6{\cdot}1^3, 2^7{\cdot}1, 3^3{\cdot}1^6, 3^4{\cdot}1^3,$ $4^2{\cdot}1^7, 4^2{\cdot}2^2{\cdot}1^3, 4^2{\cdot}2^3{\cdot}1, 4^3{\cdot}1^3, 4^3{\cdot}2{\cdot}1,$ $5^2{\cdot}1^5, 5^3, 6^2{\cdot}1^3, 6^2{\cdot}2{\cdot}1, 7^2{\cdot}1,$ $8{\cdot}1^7, 8{\cdot}2^2{\cdot}1^3, 8{\cdot}2^3{\cdot}1, 8{\cdot}4{\cdot}1^3, 8{\cdot}4{\cdot}2{\cdot}1,$ $9{\cdot}1^6, 9{\cdot}3{\cdot}1^3, 11{\cdot}1^4, 12{\cdot}1^3, 12{\cdot}2{\cdot}1, 14{\cdot}1$

$n = 16$ γ
$1^{16}, 2^4{\cdot}1^8, 2^5{\cdot}1^6, 2^6{\cdot}1^4, 2^7{\cdot}1^2, 2^8, 3^3{\cdot}1^7,$ $4^2{\cdot}1^8, 4^2{\cdot}2^2{\cdot}1^4, 4^2{\cdot}2^3{\cdot}1^2, 4^2{\cdot}2^4,$ $4^3{\cdot}1^4, 4^3{\cdot}2{\cdot}1^2, 4^3{\cdot}2^2, 4^4, 5^2{\cdot}1^6, 5^3{\cdot}1,$ $6{\cdot}3{\cdot}2^2{\cdot}1^3, 7^2{\cdot}1^2, 8{\cdot}1^8, 8{\cdot}2^2{\cdot}1^4, 8{\cdot}2^3{\cdot}1^2, 8{\cdot}2^4,$ $8{\cdot}4{\cdot}1^4, 8{\cdot}4{\cdot}2{\cdot}1^2, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2,$ $10{\cdot}1^6, 10{\cdot}2^2{\cdot}1^2, 11{\cdot}1^5, 13{\cdot}1^3, 14{\cdot}1^2$

$n = 17$ γ
$1^{17}, 2^5{\cdot}1^7, 2^6{\cdot}1^5, 2^7{\cdot}1^3, 2^8{\cdot}1, 3^3{\cdot}1^8,$ $4^3{\cdot}1^5, 4^3{\cdot}2^2{\cdot}1, 4^4{\cdot}1, 5^2{\cdot}1^7, 5^3{\cdot}1^2, 7^2{\cdot}1^3, 8^2{\cdot}1,$ $10{\cdot}1^7, 10{\cdot}2^2{\cdot}1^3, 10{\cdot}2^3{\cdot}1, 10{\cdot}5{\cdot}1^2, 13{\cdot}1^4, 16{\cdot}1$

Table 3.3: Cycle structures of γ such that $(\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$ for $n \leqslant 17$.

3.7 Wrapping up

We now describe how we used the preceding results to establish exactly what $\mathrm{Par}(n)$ is when $n \leqslant 17$. For each possible cycle structure of β and γ we first considered whether any of our results showed that $(\varepsilon, \beta, \gamma; (12)) \notin \mathrm{Par}(n)$ or $(\varepsilon, \varepsilon, \gamma; (123)) \notin \mathrm{Par}(n)$. If not, we used a simple backtracking algorithm to construct a Latin square L with $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(L)$ or $(\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(L)$ as appropriate.

When applying Lemma 3.3.2 and Lemma 3.3.3 we checked for each block that there were sufficient symbols available to fill it. When applying Theorem 3.3.4 and Theorem 3.3.6 we chose Λ to be the set of divisors of the length of some cycle of β and γ, respectively. This guaranteed that we would find a (not necessarily proper) subsquare, of order say s. If $n/2 < s < n$ this is an immediate contradiction. If $s \leqslant n/2$ the subsquare has an induced autoparatopism, and we checked with a recursive call that it was plausible. If $s = n/2$ we also considered the complementary subsquare, as described in the example after Theorem 3.3.4.

Thus, by combining Lemma 3.3.2 and Theorems 3.3.4, 3.5.1, 3.5.3, 3.5.4, 3.5.5 and 3.5.6 we found a catalogue of all possible cycle structures for $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ for $n \leqslant 17$. The results are given in Table 3.1 and Table 3.2.

Similarly, by combining Lemma 3.3.3 and Theorem 3.3.6 with the results in Section 3.6 we found a catalogue of all possible cycle structures for $(\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$ for $n \leqslant 17$. The results are given in Table 3.3. By Theorems 3.2.1 and 3.2.2, it is possible to deduce from Tables 3.1, 3.2 and 3.3 a list of all $(\alpha, \beta, \gamma; \delta) \in \mathrm{Par}(n)$ for $n \leqslant 17$, where $\delta \neq \varepsilon$. The

$\delta = \varepsilon$ case was already solved in [75].

We end with an interesting comparison with the following theorem by McKay *et al.* [58] on autotopisms.

Theorem 3.7.1. *For almost all $\alpha \in \mathcal{S}_n$, there are no $\beta, \gamma \in \mathcal{S}_n$ such that $(\alpha, \beta, \gamma) \in \mathrm{Atp}(n)$.*

In the same vein we have:

Theorem 3.7.2. *For almost all $\gamma \in \mathcal{S}_n$, there are no $\alpha, \beta \in \mathcal{S}_n$ such that $(\alpha, \beta, \gamma; (12)) \in \mathrm{Par}(n)$.*

Proof. If $\sigma = (\alpha, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ then $\sigma^2 = (\alpha\beta, \beta\alpha, \gamma^2; \varepsilon) \in \mathrm{Par}(n)$. In turn this implies that γ^2 has order at most $n^2/4$, by [58, Thm 2], so γ has order at most $n^2/2$. However by [23], almost all $\gamma \in \mathcal{S}_n$ have order at least $n^{(1/2+o(1))\log n}$, from which the result follows. □

These results contrast starkly with our final two results on autoparatopisms:

Theorem 3.7.3. *For all $\alpha \in \mathcal{S}_n$ there exist $\beta, \gamma \in \mathcal{S}_n$ such that $\sigma = (\alpha, \beta, \gamma; (12)) \in \mathrm{Par}(n)$.*

Proof. For $\alpha \in \mathcal{S}_n$ take $\gamma = (1\,2 \cdots n)$ and $\beta = \alpha^{-1}\gamma$. Then $\sigma' = (\varepsilon, \alpha\beta, \gamma; (12)) \in \mathrm{Par}(n)$, by Corollary 3.5.13. Hence $\sigma \in \mathrm{Par}(n)$, since σ and σ' are conjugate by Theorem 3.2.2. □

Theorem 3.7.4. *For all $\alpha, \beta \in \mathcal{S}_n$ there exist $\gamma \in \mathcal{S}_n$ such that $\sigma = (\alpha, \beta, \gamma; (123)) \in \mathrm{Par}(n)$.*

Proof. For $\alpha, \beta \in \mathcal{S}_n$ take $\gamma = (\beta\alpha)^{-1}$. Then $\gamma\beta\alpha = \varepsilon$ and hence $\sigma = (\alpha, \beta, \gamma; (123))$ and $\sigma' = (\varepsilon, \varepsilon, \varepsilon; (123))$ are conjugate. Hence the result, by Lemma 3.3.8. □

Chapter 4

Near-Autoparatopisms

4.1 Introduction

A $2 \times \ell$ Latin subrectangle R of some Latin square L is said to be a *row cycle* of length ℓ (or simply an ℓ-*cycle*) if R is minimal in that it contains no $2 \times \ell'$ Latin subrectangle for $\ell' \in [2, \ell - 1]$. Column cycles are defined similarly, as $\ell \times 2$ submatrices that are mapped to row cycles by transposition. The importance of row cycles and column cycles for our work hinges on the following elementary result, whose proof is omitted.

Theorem 4.1.1. *If a subsquare contains at least one entry from each row of some row cycle then it contains every entry of the row cycle. Similarly, if a subsquare contains at least one entry from each column of some column cycle then it contains every entry of the column cycle.*

Another way to view row cycles is to define a *row permutation* $\rho_{i,j}$ by $L(i,k) \mapsto L(j,k)$ for each k. Each cycle (in the usual permutation sense) γ of $\rho_{i,j}$ corresponds to a row cycle Γ in L between rows i and j. Moreover, γ and Γ have the same length and contain exactly the same symbols; we simply take Γ to contain any entry in row i or row j of L where the symbol is one of those moved by γ.

As discussed in Chapter 2, by turning intercalates, Norton [62] found 146 of the 147 species of Latin squares of order 7. Sade then found the missing species containing the Latin square $\mathscr{L}$ given in (2.4.1). Sade noted that $\mathscr{L}$ has a unique intercalate M, and that if we turn M we get $\mathscr{L}^\sigma$, where $\sigma = (\varepsilon, \varepsilon, (12); (12)) \in \mathcal{P}_n$. In particular, $\mathscr{L}$ and $\mathscr{L}^\sigma$ belong to the same species, meaning that $\mathscr{L}$ is a *self-switching square* in the terminology of [82]. These are Latin squares which contain intercalates but which cannot produce any Latin square from a different species by turning intercalates. In [82] it was found that self-switching squares exist for orders $5, 7, 8$ and 9, but existence for larger orders was left open. An interesting counterpoint is in 1-factorisations of complete graphs, where potentially there is an analogue of self-switching squares but they do not exist for small orders [42].

One of our main goals in this chapter is to construct the first infinite family of self-switching squares generalising the square 2.4.1 that Sade discovered.

Example 1. Let $\alpha = (1\,2)(3\,4 \cdots 10)$. The following Latin square has α as a near-automorphism, with the intercalate in the top left-hand corner being the one that turns

when α is applied.

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

Indeed, since it is totally symmetric (that is, its triples are invariant under uniform permutation), it has $(\alpha, \alpha, \alpha; \delta)$ as a near-autoparatopism for all $\delta \in \mathcal{S}_3$. This shows that near-autoparatopisms can have any of the six possibilities for their last component.

A goal of this chapter is to determine a family of Latin squares which admit a near-autoparatopism and have a unique intercalate.

Let $\mathcal{U}_{n,s}$ denote the set of order n Latin squares that contain a unique proper subsquare, with that subsquare having order s. This set was studied in [79] where it was noted that $n = 7$ is the smallest n for which $\mathcal{U}_{n,2} \neq \emptyset$, and that all members of $\mathcal{U}_{7,2}$ belong to the species represented by 2.4.1. Also, the following conjecture was made.

Conjecture 4.1.2. *$\mathcal{U}_{n,2}$ is non-empty for all large enough n.*

We give a partial solution to this conjecture, showing that it is true for $n \equiv \pm 1 \mod 6$. For prime $p \equiv 1 \mod 4$ and for $p = 3$, Theorems 4 and 5 in [79] show that there are arbitrarily large n for which $\mathcal{U}_{n,p} \neq \emptyset$. However, a similar statement had not previously been shown for $p = 2$.

The structure of the chapter is as follows. In Section 4.2 we prove some basic properties of near-autoparatopisms. In Section 4.3 we construct the family $\{L_n\}$ of Latin squares which is the main focus of the chapter, and demonstrate some of their basic properties. In Section 4.4 we show that L_n has a unique intercalate and no other subsquares of order less than 5. In Section 4.5 we show that L_n has no proper subsquares of order 5 or greater. In the final section we make some concluding comments.

4.2 Near-autoparatopisms

In this section we prove some basic results that provide a foundation for the study of near-autoparatopisms. We start with a simple generalisation of a result from [15], where the near-automorphism case of the following result was observed.

Theorem 4.2.1. *Suppose σ_1 and σ_2 are conjugate in $\mathcal{P}_n$. If σ_1 is a near-autoparatopism of some Latin square then σ_2 is a near-autoparatopism of a (potentially) different Latin square.*

Proof. By assumption there exist $\tau \in \mathcal{P}_n$ such that $\sigma_2 = \tau^{-1}\sigma_1\tau$ and there is some Latin square L such that $\text{dist}(L^{\sigma_1}, L) = 4$. Then,

$$\text{dist}(L^{\tau\sigma_2}, L^\tau) = \text{dist}(L^{\tau(\tau^{-1}\sigma_1\tau)}, L^\tau) = \text{dist}(L^{\sigma_1\tau}, L^\tau) = \text{dist}(L^{\sigma_1}, L) = 4.$$

Hence σ_2 is a near-autoparatopism of L^τ. □

The above proof is almost identical to that of Theorem 3.2.1.

Theorem 4.2.2. *Let L be a Latin square with a near-autoparatopism $\sigma = (\alpha, \beta, \gamma; \delta) \in \mathcal{P}_n$. Let I be the intercalate with triples $O(L) \setminus O(L^\sigma)$ and let I' be the intercalate with triples $O(L^\sigma) \setminus O(L)$. If the triples of I are mapped to those of I' by σ then σ^2 is an autoparatopism of L.*

Proof. Since σ maps $O(I)$ to $O(I')$ it must map $O(L) \setminus O(I)$ to triples outside $O(I')$. But σ is a near-autoparatopism so it must fix $O(L) \setminus O(I)$ setwise. Thus σ^2 also fixes $O(L) \setminus O(I)$ setwise. There are precisely two ways to complete $O(L) \setminus O(I)$ to a Latin square, meaning that σ^2 must send $O(I)$ to either $O(I)$ or $O(I')$. The latter option is untenable because it would mean that σ^{-1} maps $O(I')$ to $O(I')$, but we know it maps $O(I')$ to $O(I)$. Hence σ^2 fixes $O(I)$ as well as $O(L) \setminus O(I)$, and we are done. □

Note that the hypothesis in Theorem 4.2.2 that σ maps $O(I)$ to $O(I')$ is satisfied by the near-autoparatopisms discussed in Example 1. However, the hypothesis is not satisfied by all near-autoparatopisms. Indeed there are Latin squares L with a near-autoparatopism σ such that σ^2 is not an autoparatopism of L. For a concrete example, see [15]. Nevertheless, we do have the following:

Theorem 4.2.3. *If σ is a near-autoparatopism of a Latin square L then σ is a near-autoparatopism of L^{σ^k} for all integers $k \geqslant 0$.*

Proof. It suffices to prove the case $k = 1$ since the result will then follow by induction. Suppose L has order n. Applying σ to the $n^2 - 4$ triples in $O(L^\sigma) \cap O(L)$ we get $n^2 - 4$ triples in $O(L^{\sigma^2}) \cap O(L^\sigma)$. Hence $\text{dist}(L^{\sigma^2}, L^\sigma) \leqslant 4$. If $\text{dist}(L^{\sigma^2}, L^\sigma) = 0$ then σ^{-1} is an autoparatopism of L^{σ^2} which means that $L^{\sigma^2} = L^\sigma = L$, and we know that is not the case. It follows that $\text{dist}(L^{\sigma^2}, L^\sigma) = 4$, and we are done. □

We stress that Theorem 4.2.3 does not imply that σ^k is a near-autoparatopism of L for each $k \geqslant 0$ (indeed, such a statement is clearly false).

4.3 The construction

In this section we construct the Latin squares that are the main focus of this chapter.

Our construction will only work if $n \equiv \pm 1 \mod 6$ and $n \geqslant 7$, so for the remainder of the chapter we assume these conditions. Let $n' = n - 2$ and $h = (n-1)/2$. Define an n'-cycle $\beta = (0\,1 \cdots n{-}3)$. We define L_n to be an order n Latin square with rows, columns and symbols indexed by $\mathbb{Z}_{n'} \cup \{\star, \diamond\}$. The symbols $\star, \diamond$ will be referred to as *infinity symbols*.

$\star$	2	3	4	5	$\diamond$	6	7	8	0	1
1	$\star$	4	5	6	7	$\diamond$	8	0	2	3
2	3	$\star$	6	7	8	0	$\diamond$	1	4	5
3	4	5	$\star$	8	0	1	2	$\diamond$	6	7
$\diamond$	5	6	7	$\star$	1	2	3	4	8	0
6	$\diamond$	7	8	0	$\star$	3	4	5	1	2
7	8	$\diamond$	0	1	2	$\star$	5	6	3	4
8	0	1	$\diamond$	2	3	4	$\star$	7	5	6
0	1	2	3	$\diamond$	4	5	6	$\star$	7	8
4	6	8	1	3	5	7	0	2	$\star$	$\diamond$
5	7	0	2	4	6	8	1	3	$\diamond$	$\star$

Figure 4.1: The construction for $n = 11$.

The Latin square L_n has autotopism $\theta_* = (\beta, \beta, \beta^2)$ and can be generated from the following triples (orbit representatives under the group generated by θ_*):

$$(0, 0, \star), (0, h, \diamond) \tag{4.3.1}$$
$$(0, i, i+1) \text{ for } 1 \leqslant i \leqslant h-1 \tag{4.3.2}$$
$$(0, i, i) \text{ for } h+1 \leqslant i \leqslant n'-1 \tag{4.3.3}$$
$$(0, \star, 0), (0, \diamond, 1) \tag{4.3.4}$$
$$(\star, 0, h-1), (\diamond, 0, h) \tag{4.3.5}$$
$$(\star, \star, \star), (\star, \diamond, \diamond), (\diamond, \star, \diamond), (\diamond, \diamond, \star). \tag{4.3.6}$$

Entries of L_n will be classified as belonging to *Subregions* A_0, A_1, A_2 or *Regions* B, C and D depending on whether they belong to an orbit from (4.3.1) to (4.3.6) respectively. We define Region A to be the union of Subregions A_0, A_1, A_2. We will also find it useful to define $\mathcal{D}[c]$ to be the orbit of the triple $(0, c, L_n[0, c])$ under the group generated by θ_*, for each $c \in \mathbb{Z}_{n'} \cup \{\star, \diamond\}$. Note that L_n divides into four blocks

A	B
C	D

.

Here, A is the $n' \times n'$ submatrix of L_n with rows and columns indexed by $\mathbb{Z}_{n'}$ and D is the 2×2 submatrix with rows and columns indexed by infinity symbols. Noting that D is an intercalate, we will also be interested in the Latin square L'_n which is obtained from L_n by turning the intercalate D. It is routinely verified that L_n is mapped to L'_n by the near-autoparatopism $\sigma_* = (\varepsilon, \beta^{(n-3)/2}, \beta^{(n-3)/2}(\star\diamond); (12))$. As an illustration of Theorem 4.2.2, it shows that $\sigma_*^2 = (\beta^{(n-3)/2}, \beta^{(n-3)/2}, \beta^{n-3}; \varepsilon) = \theta_*^{(n-3)/2}$ is an autotopism of L_n (a fact that is immediate, given that θ_* is an autotopism).

We note that the orbits (4.3.4) in Region B require n to be odd, otherwise they will cause duplication of symbols within a column. The construction works when $n \equiv 3 \mod 6$ in the sense that it would build a Latin square. However, that square would have more than one intercalate, as we will see in the next section. This is why we have assumed $n \equiv \pm 1 \mod 6$. An example of our construction, for the case $n = 11$, is given in Figure 4.1.

For the remainder of the chapter, S will be a hypothetical proper subsquare of L_n other than the intercalate D. We may also assume that S has no proper subsquares except possibly the intercalate D, since if it had such a subsquare we could use it in place of S. By exhausting all possibilities we will show that S does not exist. Let s denote the order of S. The proof of the next result will reveal why we assume that $n \geqslant 7$.

Lemma 4.3.1. *There is no intercalate S consisting of one triple from each region A, B, C, D of L_n.*

Proof. Let (i, j, ∞) be a triple of S, where $i, j \in \mathbb{Z}_{n'}$ and $\infty \in \{\star, \diamond\}$. Then $L_n(i, \star) = 2i$, $L_n(i, \diamond) = 2i + 1$, $L_n(\star, j) = h - 1 + 2j$ and $L_n(\diamond, j) = h + 2j$. For S to be an intercalate hitting all four regions we would need $2i - 2j \mod n'$ to be one of $h - 2$, $h - 1$, h. But by (4.3.1) we know $2i-2j \mod n'$ is either 0 or $n'-1$. As $n \geqslant 7$ we have $0 < h-2 < h < n'-1$, completing the proof. □

In the next lemma we will say that S has consecutive rows if there is some $x \in \mathbb{Z}_{n'}$ such that S meets both row x and row $x+1$ of L_n. Consecutive columns and consecutive symbols are defined similarly. Note that infinity elements are excluded from these definitions.

Lemma 4.3.2. *The subsquare S does not have consecutive rows, consecutive columns or consecutive symbols.*

Proof. The row permutation $\rho_{0,1}$ is

$$(\star, 1, 3, 4, \ldots, h, h + 1, \diamond, h + 2, h + 3, \ldots, n' - 2, n' - 1, 0, 2).$$

In particular, this row permutation is a single (Hamiltonian) cycle. Since L admits the autotopism θ_*, the row permutation between any pair of consecutive rows is Hamiltonian. Hence S does not have consecutive rows, given Theorem 4.1.1.

Since L admits the near-autoparatopism σ_*, the column permutation between any two consecutive columns is also Hamiltonian. Hence S does not have consecutive columns.

It remains to rule out the possibility that S contains consecutive symbols, say k and $k + 1$. First suppose that S includes some triple (i, j, k) in Region A. By construction, L_n includes one or both of the triples $(i, j + 1, k + 1)$ and $(i + 1, j, k + 1)$. However, S cannot contain either triple since we have established that S does not have consecutive rows or columns. Hence, S cannot contain the symbol $k + 1$, contradicting our assumption. A similar argument works if S includes any occurrence of symbol $k + 1$ in Region A.

The only occurrences of k and $k + 1$ that remain available are in Regions B and C. Suppose S includes (i, ∞, μ) where ∞ is either of the infinity symbols and $\mu \in \{k, k + 1\}$. Then S must include both k and $k + 1$ in row i, and these can only occur in Region B. Thus S meets both columns of Region B, and must include k and $k + 1$ in both. Also, in every row of S in Region B, both k and $k + 1$ occur. We conclude that S includes an intercalate on symbols k and $k + 1$ in Region B. But Region B contains no intercalates (this can be seen many ways; one way is to note that Region B is isotopic to two columns of the addition table of $\mathbb{Z}_{n'}$ and n' is odd). We conclude that S cannot meet Region B. A similar argument works for Region C. Hence S cannot contain consecutive symbols. □

Lemma 4.3.3. *The subsquare S does not include either infinity symbol. Also S does not intersect both rows in Region C or both columns in Region B.*

Proof. By hypothesis $S \neq D$. If S intersects both rows in Region C or both columns in Region B then S contains consecutive symbols. This contradicts Lemma 4.3.2.

By Lemma 4.3.1 we may assume that S has at least two rows with indices in $\mathbb{Z}_{n'}$. Since the autotopism θ_* is transitive on such rows, we may assume that S intersects row zero and row d.

If $\star$ is a symbol in S then $(0, 0, \star) \in S$ and $(d, d, \star) \in S$. Then $(0, d, x) \in S$ and $(d, 0, y) \in S$ for some symbols x, y of S. If $d \notin \{h-1, h\}$, then x, y are consecutive symbols, contradicting Lemma 4.3.2. If $d \in \{h-1, h\}$ then $\diamond$ is a symbol in S. Hence $(h-1, 0, \diamond), (0, h, \diamond) \in S$, which means that $(h-1, h-1, \star), (h, h, \star) \in S$, contradicting Lemma 4.3.2. Therefore $\star$ is not a symbol in S. A similar proof shows that $\diamond$ is not a symbol in S. □

4.4 Small subsquares

The aim of this section is to rule out L_n having any subsquare $S \neq D$ of order $s < 5$. By Lemma 4.3.3 we may assume that S does not intersect Subregion A_0 or Region D, but does intersect region A. As S does not meet Region D, it cannot meet both Regions B and C. Also, S^{σ_*} must be a subsquare in L_n. Hence, by replacing S by S^{σ_*} if necessary, we may assume that S does not meet Region C.

Suppose for a moment that S does not intersect Region B. Replacing each entry $(i, j, L_n[i, j])$ of S by $(i, j-1, L_n[i, j]-1)$ yields another subsquare of order s, unless S already included an entry in $\mathcal{D}[1]$ or $\mathcal{D}[h+1]$. By applying this observation repeatedly, we may assume that S includes an entry in $\mathcal{D}[1], \mathcal{D}[h+1], \mathcal{D}[\star]$ or $\mathcal{D}[\diamond]$. Finally, using the autotopism θ_* we may assume that S intersects row zero and row r, where $r \in \mathbb{Z}_{n'}$. Also, by Lemma 4.3.2 we may assume that $2 \leqslant r \leqslant n'-2$.

In summary, if there is a proper subsquare of some order s, then there is a subsquare of order s that includes one of the triples

$$(0, 1, 2), (0, h+1, h+1), (0, \star, 0), (0, \diamond, 1). \tag{4.4.1}$$

We choose this subsquare to be S.

We will follow a row cycle $\mathcal{C}$ between rows 0 and r, inductively defining (column,symbol) pairs e_i and f_i by the following rules. We will begin at some $e_0 = (x_0, y_0)$ such that $(0, x_0, y_0) \in L_n$. To move from row 0 to row r, we define $f_i = (x_i, z_i)$ if $(r, x_i, z_i) \in L_n$ and $e_i = (x_i, y_i)$. To move from row r to row 0, we define $e_{i+1} = (x_{i+1}, z_i)$ if $(0, x_{i+1}, z_i) \in L_n$ and $f_i = (x_i, z_i)$. For $\mathcal{C}$ to be a cycle of length ℓ, a necessary condition is that $e_\ell = e_0$.

We will seek short row cycles by calculating values for e_i and f_i, for various starting points e_0. In the process, we will use the following result repeatedly.

Lemma 4.4.1. *Suppose that $e_i = (y, z)$ where y, z are not infinity elements. Then either*

(a) The symbol in e_{i+1} is congruent to $z + r + x \mod n'$ where $x \in \{-1, 0, 1\}$, or

(b) The symbol in e_{i+1} is an infinity symbol.

Proof. The hypotheses ensure that e_i lies in Subregion A_1 or A_2. Let $f_i = (y, w)$. If w is an infinity symbol then we have condition (b), so we may assume that f_i lies in Subregion A_1 or A_2. If both e_i and f_i lie in the same subregion then $w = z + r$, while if they lie in different subregions then $w = z + r \pm 1$. Either way, we have condition (a). □

By Lemma 4.3.3, we may stop searching any time that case (b) arises in Lemma 4.4.1.

Theorem 4.4.2. *Region D is the only intercalate in L_n.*

Proof. For simplicity, throughout this proof we will assume that $n > 15$. For smaller n the same arguments work, but some minor details differ from the general argument. In any case, it is easy to establish that the theorem holds for $n \leqslant 15$ by direct computation.

Suppose $S \neq D$ is an intercalate in L_n. There must be a pair $e_0 = (x, y)$ such that $(0, x, y)$ is an entry from (4.4.1) that is included in S. Starting with this e_0 we must find a row cycle of length 2; in other words $e_2 = e_0$. We distinguish two cases.

Case (i): All entries of S occur in Region A.

In this case e_0 is either $(1, 2)$ or $(h + 1, h + 1)$. The symbol in f_1 must equal the symbol in e_0. By Lemma 4.4.1 we have $2r + x \equiv 0 \mod n'$ for some $-2 \leqslant x \leqslant 2$. Given that $2 \leqslant r \leqslant n' - 2$, the only possibilities are $r = (n' - 1)/2$ and $r = (n' + 1)/2$.

When $r = (n' - 1)/2$ we have

$$\begin{array}{llll} e_0 = (1, 2), & e_1 = (r, r + 1), & & e_0 = (r + 2, r + 2), \quad e_1 = (1, 2), \\ f_0 = (1, r + 1), & f_1 = (r, \star). & \text{or} & f_0 = (r + 2, 2), \qquad f_1 = (1, r + 1). \end{array}$$

When $r = (n' + 1)/2$ we have

$$\begin{array}{lll} e_0 = (1, 2), & & e_0 = (r + 1, r + 1), \quad e_1 = (2, 3), \\ f_0 = (1, \diamond). & \text{or} & f_0 = (r + 1, 3), \qquad f_1 = (2, r + 2). \end{array}$$

There is no instance where the symbol in e_0 equals the symbol in f_1 (and the row cycle avoids meeting an infinity symbol).

Case (ii): One column of S occurs in Region B and the other column in Region A.

In this case, we can select e_0 to be either $(\star, 0)$ or $(\diamond, 1)$. If $e_0 = (\star, 0)$ then $f_0 = (\star, 2r)$. Hence, $e_1 = (x_1, 2r)$ and $f_1 = (x_1, 3r + x)$ where $x_1 \in \mathbb{Z}_{n'}$ and $-1 \leqslant x \leqslant 1$. Thus, to have a 2-cycle we must have $3r + x \equiv 0 \mod n'$ where $-1 \leqslant x \leqslant 1$. Since $2 \leqslant r \leqslant n' - 2$ we know that $3r + x \in \{n', 2n'\}$. The same restrictions on r apply if we start with $e_0 = (\diamond, 1)$.

When $r = (n' - x)/3$, we have

$$\begin{array}{llll} e_0 = (\star, 0), & e_1 = (2r, 2r), & & e_0 = (\diamond, 1), \qquad e_1 = (2r + 1, 2r + 1), \\ f_0 = (\star, 2r), & f_1 = (2r, 1 - x) & \text{or} & f_0 = (\diamond, 2r + 1), \quad f_1 = (2r + 1, 2 - x). \end{array}$$

We find an intercalate if and only if $x = 1$. However, if $x = 1$ then $n' \equiv 1 \mod 3$ which means $n \equiv 0 \mod 3$ (a possibility that we excluded, and this situation shows why).

When $r = (2n' - x)/3$, we have

$$\begin{array}{llll} e_0 = (\star, 0), & e_1 = (2r-1, 2r), & & e_0 = (\diamond, 1), \quad e_1 = (2r, 2r+1), \\ f_0 = (\star, 2r), & f_1 = (2r-1, -1-x) & \text{or} & f_0 = (\diamond, 2r+1), \quad f_1 = (2r, -x). \end{array}$$

An intercalate arises if and only if $x = -1$. This again corresponds to $n \equiv 0 \mod 3$. Hence there are no intercalates other than Region D. □

Since every Latin square of order 4 contains at least 8 intercalates, we have an immediate corollary:

Corollary 4.4.3. There are no subsquares of order 4 in L_n.

To complete the goal for this section, it remains to show:

Theorem 4.4.4. *There are no subsquares of order* 3 *in* L_n.

Proof. As we did in Theorem 4.4.2, we note that the small cases can be handled by exhaustive computation. Hence, for simplicity, we assume that $n \geqslant 25$ in the remainder of the proof.

Suppose S is a subsquare of order 3. We consider two cases.

Case (i): All entries of S occur in Region A.

As before, we may assume that e_0 is either $(1, 2)$ or $(h+1, h+1)$. To have a 3-cycle it is necessary that $e_0 = e_3$. By Lemma 4.4.1, this requires that $3r + x \equiv 0 \mod n'$, where $-3 \leqslant x \leqslant 3$. Again, we know that $3r + x \in \{n', 2n'\}$.

When $r = (n' - x)/3$ we have

$$\begin{array}{ll} e_0 = (1, 2), & e_1 = (r, r+1), \\ f_0 = (1, r+1), & f_1 = (r, \star) \end{array}$$

or

$$\begin{array}{lll} e_0 = (h+1, h+1), & e_1 = (h+r+2, h+r+2), & e_2 = (h+2r+1, h+2r+2), \\ f_0 = (h+1, h+r+2), & f_1 = (h+r+2, h+2r+2), & f_2 = (h+2r+1, h+1-x). \end{array}$$

Hence the only relevant 3-cycle that we find is when $x = 0$ and $e_0 = (h+1, h+1)$.

[As an aside, the next description fails when $n = 23$, which is why we have assumed that $n \geqslant 25$]. When $r = (2n' - x)/3$ we have

$$\begin{array}{lll} e_0 = (1, 2), & e_1 = (r+2, r+2), & e_2 = (2r+2, 2r+3), \\ f_0 = (1, r+2), & f_1 = (r+2, 2r+3), & f_2 = (2r+2, 2-x), \end{array}$$

giving a 3-cycle only if $x = 0$ and $e_0 = (1, 2)$; or

$$\begin{array}{ll} e_0 = (h+1, h+1), & e_1 = (h+r, h+r+1) \\ f_0 = (h+1, h+r+1) & f_1 = (h+r, \diamond). \end{array}$$

From the above we deduce that each cell is in at most one 3-cycle, whereas in would need to be in two 3-cycles if it was in a subsquare of order 3.

Case (ii): One column of S is in Region B and the other two columns are in Region A.

Starting with $e_0 = (\infty, y)$ where ∞ is either of the infinity elements and $y \in \mathbb{Z}_{n'}$, we will find that the symbol in e_1 is $y + 2r$. Lemma 4.4.1 then shows that to have $e_3 = e_0$ requires $4r + x \equiv 0 \mod n'$ for some $-2 \leqslant x \leqslant 2$. Given that $2 \leqslant r \leqslant n' - 2$, the only possible values for r are $(n'-1)/4$, $(n'+1)/4$, $(n'-1)/2$, $(n'+1)/2$, $(3n'-1)/4$ and $(3n'+1)/4$.

When $r = (n'-1)/4$, we have

$$\begin{array}{lll} e_0 = (\star, 0), & e_1 = (2r-1, 2r), & e_2 = (3r, 3r), \\ f_0 = (\star, 2r), & f_1 = (2r-1, 3r), & f_2 = (3r, 0), \end{array} \tag{4.4.2}$$

or

$$\begin{array}{lll} e_0 = (\diamond, 1), & e_1 = (2r, 2r+1), & e_2 = (3r+1, 3r+1), \\ f_0 = (\diamond, 2r+1), & f_1 = (2r, 3r+1), & f_2 = (3r+1, \diamond). \end{array}$$

The first option gives a 3-cycle while the second does not.

When $r = (n'+1)/4$, we have

$$\begin{array}{lll} e_0 = (\star, 0), & e_1 = (2r-1, 2r), & e_2 = (3r, 3r), \\ f_0 = (\star, 2r), & f_1 = (2r-1, 3r), & f_2 = (3r, \diamond) \end{array}$$

or

$$\begin{array}{lll} e_0 = (\diamond, 1), & e_1 = (2r+1, 2r+1), & e_2 = (3r+2, 3r+2), \\ f_0 = (\diamond, 2r+1), & f_1 = (2r+1, 3r+2), & f_2 = (3r+2, 3). \end{array}$$

Neither option gives a 3-cycle.

When $r = (n'-1)/2$ the two columns indexed by the infinity symbols are in the same row cycle, beginning $e_0 = (\diamond, 1),\ f_0 = (\diamond, 0),\ e_1 = (\star, 0)$. Likewise, when $r = (n'+1)/2$, we find $e_0 = (\star, 0),\ f_0 = (\star, 1),\ e_1 = (\diamond, 1)$. Lemma 4.3.3 tells us that we can ignore these cases.

When $r = (3n'-1)/4$, we have

$$\begin{array}{lll} e_0 = (\star, 0), & e_1 = (2r-1, 2r), & e_2 = (3r-2, 3r-1), \\ f_0 = (\star, 2r), & f_1 = (2r-1, 3r-1), & f_2 = (3r-2, -2). \end{array}$$

or

$$\begin{array}{lll} e_0 = (\diamond, 1), & e_1 = (2r, 2r+1), & e_2 = (3r-1, 3r), \\ f_0 = (\diamond, 2r+1), & f_1 = (2r, 3r), & f_2 = (3r-1, -1). \end{array}$$

Neither option gives a 3-cycle.

When $r = (3n'+1)/4$, we have

$$\begin{array}{lll} e_0 = (\star, 0), & e_1 = (2r-1, 2r), & e_2 = (3r-2, 3r-1), \\ f_0 = (\star, 2r), & f_1 = (2r-1, 3r-1), & f_2 = (3r-2, 0). \end{array} \tag{4.4.3}$$

or

$$\begin{array}{lll} e_0 = (\diamond, 1), & e_1 = (2r+1, 2r+1), & e_2 = (3r, 3r+1), \\ f_0 = (\diamond, 2r+1), & f_1 = (2r+1, 3r+1), & f_2 = (3r, \diamond). \end{array}$$

The first option gives a 3-cycle while the second does not.

For S to be a subsquare of order 3 we would have to find two separate 3-cycles that include e_0. The only plausible combination is (4.4.2) and (4.4.3). However, in (4.4.2) the symbol in f_0 is $(n'-1)/2$, while in (4.4.3) the symbol in f_0 is $(n'+1)/2$. By Lemma 4.3.2 these two symbols cannot both be in S, so we are done. □

4.5 Non existence of large subsquares

The aim of this section is to prove that L_n has no subsquares of order $s \geqslant 5$. We assume to the contrary and deduce properties of such a subsquare S.

Lemma 4.5.1. *If $d \in [1, h-2]$ then $S^{\theta_*^d} \neq S$.*

Proof. All calculations in this proof will be modulo n'. There is at least one column of S indexed by some $z \in \mathbb{Z}_{n'}$. Assuming that $S^{\theta_*^d} = S$, we must also have the columns indexed $z+d, z+2d, z+3d, \ldots$ in S. Since $d \leqslant h-2$ there must be columns $x \in [1, h-1]$ and $y \in [h+1, n'-1]$ and symbols a, b such that $(0, x, a) \in S$ and $(0, y, b) \in S$ with $y - x = \lambda d$, for some integer λ. Also $a = x+1$ and $b = y$. Hence $b - a = y - x - 1 = \lambda d - 1$. Now n' is odd and S is invariant under $\theta_*^{d\lambda(n'+1)/2}$, so $a + 2d\lambda(n'+1)/2 = a + \lambda d$ is a symbol of S. But this contradicts Lemma 4.3.2, since $b = a + \lambda d - 1$ is a symbol of S. □

We now introduce the notion of a diagonal pair which is used in the remainder of the chapter. Two entries (a, b, c) and $(a, b, c)^{\theta_*^d}$ are said to be a diagonal pair provided that neither of them lies in Region D.

Lemma 4.5.2. *The subsquare S does not contain two distinct diagonal pairs.*

Proof. Suppose that S contains the following two diagonal pairs:

$$\{(a_1, b_1, c_1), (a_1, b_1, c_1)^{\theta_*^d}\} \text{ and } \{(a_2, b_2, c_2), (a_2, b_2, c_2)^{\theta_*^d}\}.$$

Then the subsquare $S^{\theta_*^d}$ contains the two entries

$$(a_1, b_1, c_1)^{\theta_*^d} \text{ and } (a_2, b_2, c_2)^{\theta_*^d}$$

from S. Since the intersection of two subsquares is again a subsquare, $S \cap S^{\theta_*^d}$ is a subsquare. But S contains no proper subsquare by Lemma 4.3.3 and our choice of S. Therefore, $S^{\theta_*^d} = S$, contradicting Lemma 4.5.1. □

Theorem 4.5.3. *There is no proper subsquare S of order $s \geqslant 5$ in the Latin square L_n.*

Proof. Let d_r be the minimum absolute difference between the indices of two rows of S that have indices in $\mathbb{Z}_{n'}$. Let d_c be the corresponding quantity for column indices of S, and let $d = \min(d_r, d_c)$. Note that $d \leqslant n'/4 \leqslant h-2$ since S has at least 4 columns with indices in $\mathbb{Z}_{n'}$. By Lemma 4.3.3 we know that S avoids Region D, so S^{σ_*} is also a subsquare of L_n. By replacing S by S^{σ_*} if necessary, we may assume that $d = d_r$. Finally, using the autotopism θ_* we may assume that S intersects row zero and row d.

By Lemma 4.3.2, Lemma 4.3.3 and our choice of d, we know that S can contain at most one column from the interval $[0, d]$, at most one column from the interval $[h, h+d]$, and at most one column in Region B. Hence there must be a column

$$c \in \mathbb{Z}_{n'} \setminus \big([0, d] \cup [h, h+d]\big)$$

in S. Hence $(0, c, x), (d, c, x+d) \in S$ for some x.

Let $r \in \mathbb{Z}_{n'}$ be a row of L_n in which both x and $x+d$ occur in Region A. Define $\Delta(r) \in \mathbb{Z}_{n'}$ by $\Delta(r) \equiv j - i \mod n'$ where $(r,i,x),(r,j,x+d) \in L_n$. By construction, $\Delta(r) \in \{d-1, d, d+1\}$ for all choices of r. However, by our choice of d we know that S does not include any rows r for which $\Delta(r) = d-1$.

Now consider a row r for which $\Delta(r) = d+1$. By the construction of L_n we know that in row r symbol x must occur in $\mathcal{D}[c]$, for some $c \in \{h-d, \ldots, h-1\}$. Define I_1 (respectively I_2) to be the set of d consecutive rows starting with the row in which symbol x occurs in $\mathcal{D}[h-1]$ (respectively $\mathcal{D}[h-2]$). All rows r for which $\Delta(r) = d+1$ lie in either I_1 or I_2. However, each of these two sets contains at most one row of S, by our choice of d. Hence there exist 3 rows r_1, r_2, r_3 of S that do not come from I_1 or I_2.

Case 1: S does not intersect Region B.

By Lemma 4.3.3, at most one row of S may be in Region C. So, without loss of generality, we may suppose that $r_1, r_2 \in \mathbb{Z}_{n'}$ and hence $\Delta(r_1) = \Delta(r_2) = d$. Let c_1, c_2 be the columns in which symbol x occurs in rows r_1, r_2 respectively. The cells $(0, c_1)$, $(d, c_1 + d)$, $(0, c_2)$ and $(d, c_2 + d)$ must all be in S, but this violates Lemma 4.5.2.

Case 2: S does intersect Region B.

By Lemma 4.3.3, S does not intersect Region C and has only one column, say column ∞, in Region B. At most two of r_1, r_2, r_3 contain x or $x+d$ in column ∞, so S must include at least one row r for which $\Delta(r) = d$. This gives one diagonal pair (by the same argument as in Case 1), and we get another from the fact that cells $(0, \infty)$ and (d, ∞) are both in S. Again, Lemma 4.5.2 yields a contradiction. □

Corollary 4.5.4. The only proper subsquare of L_n is the intercalate D.

The following theorem gives another near-autoparatopism of a Latin square L.

Theorem 4.5.5. *Let $\sigma = (\varepsilon, \beta, \gamma : (12)) \in \mathcal{P}_n$ and $d = (n-2)/2$. Suppose the cycle structure of β, γ are $d^2 \cdot 1^2$, $d^2 \cdot 2$ respectively. Then, σ is a near-autoparatopism of a Latin square L when d is odd.*

Proof. Consider the following contour of a Latin square L.

$$\begin{aligned}
C(1,1) &= d+1,\\
C(1,t) &= t-1, \text{ for } 2 \leqslant t \leqslant (d+1)/2,\\
C(1,t) &= t+1, \text{ for } d+1 \leqslant t \leqslant 2(d-1),\\
C(1,2d-1) &= \star, C(1,2d) = \diamond,\\
C(1,2d+1) &= d-1, C(1,2d+2) = d,\\
C(d+1,d+t) &= t, \text{ for } 1 \leqslant t \leqslant (d+1)/3,\\
C(d+1,2d+1) &= d+2, C(d+1,2d+2) = d+3,\\
C(\star,\star) &= \star, \quad C(\star,\diamond) = \diamond,\\
C(\diamond,\star) &= \diamond, \quad C(\diamond,\diamond) = \star.
\end{aligned}$$

Example :

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

.

□

Chapter 5

Conclusion

Automorphisms, autotopisms, autoparatopisms and near-autoparatopisms of Latin squares have been investigated in this thesis. Also we established a family of Latin squares with a unique intercalate and no larger subsquares.

5.1 Autoparatopisms

By combining Lemma 3.3.2 and Theorems 3.3.4, 3.5.1, 3.5.3, 3.5.4, 3.5.5 and 3.5.6 we found a catalogue of all possible cycle structures for $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ for $n \leqslant 17$. The results are given in Table 3.1 and Table 3.2.

Similarly, by combining Lemma 3.3.3 and Theorem 3.3.6 with the results in Section 3.6 we found a catalogue of all possible cycle structures for $(\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$ for $n \leqslant 17$. The results are given in Table 3.3. By Theorems 3.2.1 and 3.2.2, it is possible to deduce from Tables 3.1, 3.2 and 3.3 a list of all $(\alpha, \beta, \gamma; \delta) \in \mathrm{Par}(n)$ for $n \leqslant 17$, where $\delta \neq \varepsilon$. The $\delta = \varepsilon$ case was already solved in [75].

5.2 Near-autoparatopisms

We constructed a family $\{L_n\}$ of Latin squares, where $n \equiv \pm 1 \mod 6$ and $n \geqslant 7$. We showed that L_n has no proper subsquare of order more than 2, and has a unique intercalate. This is known [56] to be a very rare property among Latin squares of large order, and provides a partial proof of Conjecture 4.1.2.

We also showed that by turning the intercalate in L_n we reach a Latin square L'_n from the same species as L_n. This makes $\{L_n\}$ the first known infinite family of self-switching Latin squares, which lead to isolated vertices in switching graphs such as those constructed in [82]. It also means that L_n possesses a near-autoparatopism. Cavenagh and Stones [15] raised the question of whether Sade's square 2.4.1 could be generalised to produce Latin squares with a unique intercalate and a near-automorphism. Our result is very much in the spirit of their question.

The theory of near-autoparatopisms remains largely undeveloped, although we did demonstrate some basic properties in Section 4.2. We found (just as [15] did) some ways that near-autoparatopisms behave like autoparatopisms and some ways in which they differ.

This theme deserves further exploration. We suggest some possible lines of inquiry in the next subsection.

5.3 Future research

In 3.4, we gave a plausible block diagram for a Latin square with an automorphism consisting of 5 non-trivial cycles, none of which has a length dividing the length of any other cycle. McKay et al. [58] have constructed such a Latin square. Hence we suggest these two problems.

Problem 5.3.1. *What is the smallest $k > 1$ for which there is an automorphism with cycle structure $d_1^{a_1} d_2^{a_2} \dots d_k^{a_k}$ such that $d_i \nmid d_j$ for $i \neq j$?*

Problem 5.3.2. *What is the smallest $k > 1$ for which there is an automorphism with cycle structure $d_1 \cdot d_2 \cdots d_k \cdot 1^f$ with $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_k > 1$, $f \geqslant 0$, and $d_j \nmid d_i$ whenever $d_j \neq d_i$.*

For both questions we know the answer is at most 5.

From the case when no cycle length divides any other, we next turn to the opposite extreme. In Theorem 3.4.2 we found a sufficient condition for $\alpha \in \mathcal{S}_n$ to be an automorphism when the cycle structure of α is $d_1 \cdot d_2 \cdots d_{p-1} \cdot d_p^a$, for some $a \geqslant 1$. More generally we might try to characterise all automorphisms where each cycle length divides the next shortest cycle length.

Problem 5.3.3. *Find all positive integers k, $a_1, \dots, a_k$ and $d_1, \dots, d_k$ such that there is an automorphism with cycle structure $d_1^{a_1} \cdot d_2^{a_2} \cdots d_k^{a_k}$, where $d_p \mid d_{p-1}$ and $d_{p-1} > d_p$ for $2 \leqslant p \leqslant k$.*

We can ask similar questions for autoparatopisms. Consider the following example. Let $d_1 = 18, d_2 = 6, d_3 = 2$. It is clear $d_1 > d_2 > d_3$ and $d_1/d_2, d_2/d_3$ are odd integers. Suppose the cycle structure of β is 18·6·2. The following Latin square L admits autoparatopism $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathcal{P}_n$.

·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	19	·	·	·	·	·	·	·	1
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	19	·	·	·	·	·	·	1	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	19	·	·	·	·	·	·	1	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	25	·	·	·	·	·	1	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	25	·	19
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	19	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	19	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	·	·	·	·	·	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	1	·	·	·	·	·	19	25	·
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·

Considering the above example and Theorem 3.5.15, it would be interesting to try the following problem.

Problem 5.3.4. *Find necessary and sufficient conditions for* $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathrm{Par}(n)$ *when the cycle structure of* β *is* $d_1 d_2 \dots d_m$*, where* $d_i > d_{i+1}$ *and* d_i/d_{i+1} *is an odd integer for* $i \in 1, \dots, m-1$*.*

Harder yet, we might try to build on the work of Corollary 3.5.13 and Theorems 3.5.15, 3.5.16, to:

Problem 5.3.5. *Characterise* β *for which* $\sigma = (\varepsilon, \beta, \beta; (12)) \in \mathrm{Par}(n)$*.*

By Theorems 3.5.7, 3.5.8, all possible cycle structures of γ such that $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ can be determined when $\beta = \varepsilon$ or β consists of a single cycle.

Problem 5.3.6. *Generalise Theorems 3.5.7 and 3.5.8 to the case when* β *has cycle structure* d^m *for some integers* m, d*.*

Problems 5.3.4 to 5.3.6 are all specific instances of the more general problem of trying to characterise all autoparatopisms.

Problem 5.3.7. *Find a general pattern for the cycle structure of* β *and* γ *satisfying* $(\varepsilon, \beta, \gamma; (12)) \in \mathrm{Par}(n)$ *or* $(\varepsilon, \varepsilon, \gamma; (123)) \in \mathrm{Par}(n)$ *for large* n*.*

A large part of this thesis has been devoted to this problem, nevertheless it seems a distant goal.

Next consider the following example. Let $\sigma = (\alpha, \beta, \gamma; (12))$ be a paratopism, where $\alpha = (1234)(567)$, $\beta = (1234)(576)$ and $\gamma = (1234)(56)(7)$. Suppose L is a Latin square

4	5	7	6	1	2	3
6	1	5	7	2	3	4
7	6	2	5	3	4	1
5	7	6	3	4	1	2
2	3	4	1	5	6	7
3	4	1	2	7	5	6
1	2	3	4	6	7	5

.

Then L^σ is

4	5	7	6	1	2	3
6	1	5	7	2	3	4
7	6	2	5	3	4	1
5	7	6	3	4	1	2
2	3	4	1	7	5	6
3	4	1	2	6	7	5
1	2	3	4	5	6	7

.

Note that $\mathrm{dist}(L, L^\sigma) = 9$. Also we can observe that we can get the Latin square L^σ from L by combining two symbol cycle switchings.

Let σ be a paratopism and $\text{dist}(L, L^\sigma) = k$ for some integer k. Already we have studied when $k \in \{0, 4\}$. When $k = 0$, σ is known as an autoparatopism of the Latin square L and when $k = 4$, σ is a near autoparatopism of L. Motivated by the above example we suggest a new area of research looking for σ and L such that $\text{dist}(L, L^\sigma) = k$, where k is some positive integer other than 4.

Problem 5.3.8. *For a given n what are the possible values of* $\text{dist}(L, L^\sigma)$ *where L is allowed to be any Latin square of order n, and $\sigma \in \mathcal{P}_n$?*

In Chapter 4, we found near-autoparatopisms $\sigma = (\varepsilon, \beta, \gamma; (12)) \in \mathcal{P}_n$ when the cycle structures of β and γ are $(n-2) \cdot 1^2$ and $(n-2) \cdot 2^1$; or $((n-2)/2)^2 \cdot 1^2$ and $((n-2)/2)^2 \cdot 2^1$. These are just the beginning of the investigation:

Problem 5.3.9. *Characterise $\sigma \in \mathcal{P}_n$ that are a near-autoparatopism of some Latin square of order n.*

In Chapter 4, We were successful in giving a partial solution to Conjecture 4.1.2, showing that it is true for large $n \equiv 1, 5 \mod 6$. Four cases mod 6 remain open:

Problem 5.3.10. *Is $\mathcal{U}_{n,2} \neq \emptyset$ for large $n \equiv 0, 2, 3, 4 \mod 6$?*

Also the Latin squares that we found in $\mathcal{U}_{n,2}$ are self-switching, but the existence of self-switching squares for other orders remains open.

Problem 5.3.11. *Is there a self-switching Latin square for all large orders $n \equiv 0, 2, 3, 4 \mod 6$?*

McKay *et al.* [58] showed that almost all paratopisms are not autoparatopisms. This raises an obvious question:

Problem 5.3.12. *Are almost all paratopisms not near-autoparatopisms?*

One way to prove this would be to find a polynomial bound on the order of a near-autoparatopism, which is how McKay *et al.* [58] obtained their result.

Finally, McKay and Wanless [57] showed that almost all Latin squares possess no non-trivial autoparatopism.

Problem 5.3.13. *Do almost all Latin squares have no near-autoparatopism?*

Bibliography

[1] L.D. Andersen, Factorizations of graphs, In: C.J.Colbourn & J.H.Dinitz (ed.), *Handbook of combinatorial designs*, 2nd Ed., CRC Press, Boca Raton, (2007), 740–755.

[2] L.D. Andersen, E. Mendelsohn, A direct construction for Latin squares without proper subsquares. *Annals of Discrete Math.*, **15** (1982), 27–53.

[3] V.D. Belousov, Extensions of quasigroups. Bull. Akad. Stince RSS Moldoven (1967).

[4] E.J. Billington, Combinatorial trades: a survey of recent results, in W.D.Wallis(Ed). Designs 2002:Further computational and constructive design theory, Kluwer, Boston, (2003), 47–67.

[5] A.E. Brouwer, Steiner triple systems without forbidden subconfigurations, Mathematisch Centrum, Amsterdam, ZW, (1977), 77–104.

[6] 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), 41–56.

[7] J. Browning, D. S. Stones and I. M. Wanless, Bounds on the number of autotopisms and subsquares of a Latin square, *Combinatorica* **33** (2013), 11–22.

[8] J.M. Browning, P.J. Cameron, I.M. Wanless, Bounds on the number of small Latin subsquares, *J. Combin. Theory Ser.A.*, **124** (2014), 41–56.

[9] D. Bryant, M. Buchanan and I. M. Wanless, The spectrum for quasigroups with cyclic automorphisms and additional symmetries, *Discrete Math.*, **304** (2009), 821–833.

[10] 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), 328–342.

[11] D. Bryant, B. Maenhaut and I. M. Wanless, New families of atomic Latin squares and perfect one-factorisations, *J. Combin. Theory Ser. A*, **113** (2006), 608–624.

[12] P. J. Cameron, Permutation Groups, Cambridge University Press, (1999).

[13] N. J. Cavenagh, The theory and application of Latin bitrades: a survey, *Math Slovaca.*, **58** (2008), 691–718.

[14] 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), 286–309.

[15] N. J. Cavenagh, D. S. Stones, Near-automorphisms of Latin squares, *J. Combin. Designs.*, **19** (2011), 365–377.

[16] J. Dénes, A.D. Keedwell, Latin squares and their applications, Akademiai Kiado, Budapest, (1974).

[17] J. Dénes, A.D. Keedwell, Latin squares: New developments in the theory and applications, *Ann. Discrete Math.*, 46, North-Holland, Amsterdam: (1991).

[18] J. Dénes, E.-né. Pásztor, (1963) A kvázicsoportok néhány problémájáról. Magyar Tud. Akad. Mat. Fiz. Oszt. Közl. 13, 109-118. (Hungarian). [Some problems on quasigroups.]

[19] R. H. F. Denniston, Remarks on Latin squares with no subsquares of order two, *Utilitas. Math.*, **13** (1978), 299–302.

[20] R.H.F. Denniston, Enumeration of symmetric designs (25,9,3), *Ann. Discrete. Math.*, **15** (1982), 111–127.

[21] A.A. Drisko, On the number of even and odd Latin squares of order $p+1$, *Adv. Math.*, **128** (1997), 20–35.

[22] J.R. Elliott, P.B. Gibbons, The construction of subsquare free Latin squares by simulated annealing, *Australas. J. Combin*, **5** (1992), 209–228.

[23] P. Erdős and P. Turán, On some problems of a statistical group theory III, *Acta Math. Acad. Sci. Hungar.* **18** (1967), 309–320.

[24] L. Euler, Recherches sur une nouvelle espèce de quarrés magiques, *Verh. Zeeuwsch. Gennot. Weten. Vliss.*, **9** (1782), 85–239. Eneström E530, Opera Omnia OI7, 291–392.

[25] J. Egan, I. M. Wanless, Enumeration of MOLS of small order, *Math. Comp.*, to appear.

[26] R. M. Falcón, Cycle structures of autotopisms of the Latin squares of order up to 11, *Ars. Combin.*, **103** (2012), 239–256.

[27] R. M. Falcón and J. Martín-Morales, Gröbner bases and the number of Latin squares related to autotopisms of order $\leqslant 7$, *J. Symbolic Comput.*, **42** (2007), 1142–1154.

[28] R.A Fisher, An examination of the different possible solutions of a problem in incomplete blocks, *Ann. Eugenics*, **10** (1940), 52–75.

[29] R. M. F. Ganfornina, Latin squares associated to principal autotopisms of long cycles, in Proc. Transgressive Computing, Granada, Spain, (2006) 24–26, 213–230. `http://www.orcca.on.ca/conferences/tc2006/TC2006-Proceedings.pdf`

[30] M.J. Grannel, T.S. Griggs, J.P. Murphy, Twin Steiner triple systems, *Discrete Math.*, **167-168** (1997), 341–352.

[31] M.J. Grannel, T.S. Griggs, C.A. Whitehead, The resolution of the anti-Pasch conjecture, *J.Combin. Des.*, **8** (2000), 300–309.

[32] M.J. Grannel, T.S. Griggs, J.P. Murphy, Switching cycles in Steiner triple systems, *Util. Math.*, **56** (1999), 3–21.

[33] T.S Griggs, J. Murphy, J.S Phelan, Anti-Pasch Steiner triple systems, *J.Comb. Inf. Syst. Sci.*, **15** (1990), 79–84.

[34] K. Heinrich, Latin squares with no proper subsquares, *J.Combin. Theory Ser, A.*, **29** (1980), 36–353.

[35] K. Heinrich, Latin squares with and without subsquares of prescribed type, in "Latin squares: New developments in the theory and applications," Ann. *Discrete. Math.*, **46** (1991), 101–147.

[36] K. Heinrich and W. D. Wallis, The maximum number of intercalates in a Latin square, *Combinatorial mathematics VIII*, Lecture Notes in Math. 884 (1981), 221–233.

[37] A. Hulpke, P. Kaski and P. R. J. Östergård, The number of Latin squares of order 11, *Math. Comp.*, **80** (2011), 1197–1219.

[38] M.T. Jacobson, P. Matthews, Generating uniformly distributed random Latin squares *J.Comb. Des.*, **4** (1996), 405–437.

[39] D. Jungnickel, V.D. Tonchev, Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound, *Des. Codes Cryptogr.*, **1** (1991), 247–253.

[40] D. Jungnickel, V.D. Tonchev, On symmetric and quasi-symmetric designs with the symmetric difference property and their codes, *J.Combin. Theory Ser, A.*, **59** (1992), 40–50.

[41] P. Kaski, V. Makinen, P.R.J. Östergaård, The cycle switching graph of the Steiner triple system of order 19 is connected, *Graph Combin*, **27** (2011), 539–546.

[42] P. Kaski, A. D. S. Medeiros, P. R. J. Östergård and I. M. Wanless, Switching in one-factorisations of complete graphs, *Electron. J. Comb.* **21**(2) (2014), #P2.49.

[43] P. Kaski, P.R.J. Östergaård, The Steiner triple system of order 19, *Math. Comp.*, **73** (2004), 2075–2092.

[44] A.D. Keedwell, Critical sets in Latin squares and related matters: an update, *Util. Math.*, **65** (2004), 97–131.

[45] B. Kerby and J. D. H. Smith, Quasigroup automorphisms and symmetric group characters, *Comment. Math. Univ. Carol.*, **51** (2010), 279–286.

[46] B. L. Kerby and J. D. H. Smith, Quasigroup automorphisms and the Norton-Stein complex, *Proc. Amer. Math. Soc.*, **138** (2010), 3079–3088.

[47] H. Kharaghani, B. Tayfeh-Rezaie, Hadamard matrices of order 32, *J.Combin. Des.*, **21** (2013), 212–221.

[48] D. Kotlar, Parity Types, Cycles structures and autotopisms of Latin squares, *Electron. J. Combin.* **19(3)** (2012), #P10.

[49] D. Kotlar, Computing the autotopy group of a Latin square by cycle structure, *Discrete Math.* **331** (2014), 74–82.

[50] 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), 287-294.

[51] A. Kotzig, J. Turgeon, On certain constructions for Latin squares with no Latin subsquares of order two, *Discrete Math.*, (1976), 263–270.

[52] C. Laywine, An expression for the number of equivalence classes of Latin squares under row and column permutations, *J. Combin. Theory Ser. A*, **30** (1981), 317–320.

[53] B.M. Maenhaut, I.M. Wanless, Atomic Latin squares of order eleven, *J. Combin.Des.*, **12** (2004), 12–34.

[54] B. Maenhaut, I.M. Wanless, B.S. Webb, Subsquare-free Latin squares of odd order, *Euro. J. Combin.*, **28** (2007), 322-336. (2007) 322–336.

[55] B. D. McKay, A. Meynert and W. Myrvold, Small Latin squares, quasigroups and loops, *J. Combin. Des.*, **15** (2007), 98–119.

[56] B.D. McKay, I.M. Wanless, Most Latin squares have many subsquares, *J.Combin. Theory Ser. A.*, **86** (1999) 323–347.

[57] B. D. McKay and I. M. Wanless, On the number of Latin squares, *Ann. Comb.* **9** (2005), 335–344.

[58] B. D. McKay, I. M. Wanless and X. Zhang, The order of automorphisms of quasigroups, *J. Combin. Designs*, to appear.

[59] M. McLeish, On the existence of Latin squares with no subsquares of order two, *Utilitas Math.*, **8** (1975), 41–53.

[60] M. McLeish, A direct construction of Latin squares with no subsquares of order two, *Ars. Combin.*, **10** (1980), 179–186.

[61] R.C.Mullin, H.-D.O.F. Gronau, PBDs and GDDs: the basics, in: C.J.Colbourn, J.H.Dinitz(Eds), Handbook of combinatorial Designs, 2nd ed, Chapman and Hall, Boca Raton, (2007), 231–236.

[62] H. W. Norton, The 7×7 squares, *Ann. Eugenics*, **9** (1939), 269–307.

[63] P.Ó Catháin, I. M. Wanless, Trades in complex Hadamard matrices, Springer Proc. Math. Stat., Algebraic Design Theory and Hadamard Matrices, to appear.

[64] J.M. Osborn, New loops from old geometries, *Amer. Monthly*, **68** (1961), 103–107.

[65] P.R.J. Östergård, Switching codes and designs, *Discrete Mathematics*, **312** (2012), 621–632.

[66] W.P Orrick, On the enumeration of some D-optimal designs, *J. Statist.Plann.Inference*, **138** (2008), 286–293.

[67] W.P Orrick, Switching operations for Hadamard matrices, *SIAM. J.Discrete Math.*, **22** (2008), 31–50.

[68] E.T. Parker, Computer investigation of orthogonal Latin squares of order ten, *Proc. Symp. Appl. Math.*, **15** (1963), 73–81.

[69] A.O. Pittenger, Mappings of Latin squares, *Linear Algebra Appl.*, **261** (1997), 251–268.

[70] A. Sade, An omission in Norton's list of 7×7 squares, *Ann. Math. Statist.*, **22** (1951), 306–307.

[71] A. A. Sade, Autotopies des quasigroupes et des systèmes associatifs, *Arch. Math. (Brno)*, **4** (1968), 1–23.

[72] E. Seah, and D.R. Stinson, A perfect one-factorization for K_{40}, *Congr. Numer.*, **68** (1989), 211–213.

[73] D. S. Stones, The parity of the number of quasigroups. *Discrete Math.*, **310** (2010), 3033–3039.

[74] D.S. Stones, On the number of Latin rectangles, Ph.D. Thesis, Monash University, (2010).

[75] D. S. Stones, P. Vojtěchovský and I. M. Wanless, Cycle structure of autotopisms of quasigroups and Latin Squares, *J.Combin. Designs*, **20** (2012), 227-263.

[76] W. D. Wallis, *One-factorizations*, Kluwer Academic, Dordrecht, Netherlands, 1997.

[77] I.M. Wanless, Permanents, matchings and Latin rectangles, Ph.D. thesis, Australian National University, (1997).

[78] I. M. Wanless, Perfect factorisations of bipartite graphs and Latin squares without proper subrectangles, *Elect. J. Combin.*, **6** (1999), R9.

[79] I.M. Wanless, Latin squares with one subsquare, *J. Combin. Des.*, **9** (2001), 128–146.

[80] I.M Wanless, On McLeish's construction for Latin squares without intercalates, *Ars. Combin.*, **58**(2001), 313-317.

[81] I.M. Wanless, Cycle switches in Latin squares, *Graphs Combin.*, **20** (2004), 545–570.

[82] I. M. Wanless, Diagonally cyclic Latin squares, *European J. Combin.*, **25** (2004), 393–413.

[83] I. M. Wanless, Atomic Latin squares based on cyclotomic orthomorphisms, *Elect. J. Combin.*, **12** (2005), R22.

[84] I.M. Wanless, A computer enumeration of small Latin trades, *Australas.J.Combin*, **39** (2007), 247-258.

[85] I.M. Wanless, New perfect 1-factorisations, `http://users.monash.edu.au/~iwanless/data/P1F/newP1F.html`.

[86] I. M. Wanless and E. C. Ihrig, Symmetries that Latin Squares Inherit from 1-Factorizations, *J. Combin. Designs*, **13** (2005), 157–172.

[87] A.J. Wolfe, A perfect one-factorization of K_{52}, *J. Combin. Designs*, **17** (2009), 190–196.

[88] A.J. Wolfe, A.C.H. Ling, J.H. Dinitz, The existence of N_2 resolvable Latin squares, SIAM, *J.Combin. Des.*, **23** (2009), 1217–1237.