Cycle structure of autotopisms of quasigroups and Latin squares*

Douglas S. Stones[1,2], Petr Vojtěchovský[3] and Ian M. Wanless[1]

[1] School of Mathematical Sciences and
[2] Clayton School of Information Technology
Monash University
VIC 3800 Australia

the_empty_element@yahoo.com (D. S. Stones) and ian.wanless@monash.edu (I. M. Wanless)

[3] Department of Mathematics
University of Denver
2360 S Gaylord St, Denver, CO 80208, USA

petr@math.du.edu

Abstract

An autotopism of a Latin square is a triple (α, β, γ) of permutations such that the Latin square is mapped to itself by permuting its rows by α, columns by β, and symbols by γ. Let $\mathrm{Atp}(n)$ be the set of all autotopisms of Latin squares of order n. Whether a triple (α, β, γ) of permutations belongs to $\mathrm{Atp}(n)$ depends only on the cycle structures of α, β and γ. We establish a number of necessary conditions for (α, β, γ) to be in $\mathrm{Atp}(n)$, and use them to determine $\mathrm{Atp}(n)$ for $n \leqslant 17$. For general n we determine if $(\alpha, \alpha, \alpha) \in \mathrm{Atp}(n)$ (that is, if α is an automorphism of some quasigroup of order 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.

AMS Subject Classification: 05B15, 20N05, 20D45
Keywords: automorphism; autotopism; cycle structure; diagonally cyclic Latin square; Latin square; quasigroup.

1 Introduction

A *Latin square* of order n is an $n \times n$ array $L = L(i, j)$ of n symbols such that the symbols in every row and in every column are distinct. We will usually index the rows and columns of L by elements of $[n] = \{1, 2, \ldots, n\}$ and take the symbol set to be $[n]$. A *quasigroup* Q is a nonempty set with one binary operation such that for every a, $b \in Q$ there is a unique

*Research supported by ARC grants DP0662946 and DP1093320. P. Vojtěchovský thanks Monash University for hospitality and financial support during his sabbatical stay.

$x \in Q$ and a unique $y \in Q$ satisfying $ax = b$, $ya = b$. Since multiplication tables of finite quasigroups are precisely Latin squares, all results obtained in this paper for Latin squares can be interpreted in the setting of finite quasigroups.

Let $\mathcal{I}_n = S_n \times S_n \times S_n$, where S_n is the symmetric group acting on $[n]$. Then $\mathcal{I}_n$ acts on the set of Latin squares indexed by $[n]$ as follows: For each $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ we define $\theta(L)$ to be the Latin square formed from L by permuting the rows according to α, permuting the columns according to β, and permuting the symbols according to γ. More precisely, $\theta(L) = L'$ is the Latin square defined by

$$L'(i,j) = \gamma\big(L(\alpha^{-1}(i), \beta^{-1}(j))\big). \tag{1.1}$$

The elements θ of $\mathcal{I}_n$ are called *isotopisms*, and the Latin squares L and $\theta(L)$ are said to be *isotopic*. If $\theta \in \mathcal{I}_n$ is of the form $\theta = (\alpha, \alpha, \alpha)$, then α is an *isomorphism*.

If $\theta \in \mathcal{I}_n$ satisfies $\theta(L) = L$, then θ is an *autotopism* of L. By (1.1), $\theta \in \mathcal{I}_n$ is an autotopism of L if and only if

$$\gamma\big(L(i,j)\big) = L\big(\alpha(i), \beta(j)\big) \tag{1.2}$$

for all $i, j \in [n]$. We use id to denote the identity permutation, and we call $(\mathrm{id}, \mathrm{id}, \mathrm{id}) \in \mathcal{I}_n$ the *trivial* autotopism. The group of all autotopisms of L will be denoted by $\mathrm{Atp}(L)$.

We will be particularly interested in the case where $(\alpha, \alpha, \alpha) \in \mathrm{Atp}(L)$, when we call α an *automorphism* of L. The group of all automorphisms of L will be denoted by $\mathrm{Aut}(L)$.

Autotopisms and automorphisms are natural classes of symmetries of Latin squares and quasigroups, motivating the question

"Which isotopisms are autotopisms of Latin squares?" (Q)

and also its specialization "Which isomorphisms are automorphisms of Latin squares?". In this paper we give a partial answer to these questions.

1.1 Overview

Let $n \geqslant 1$. For $\theta \in \mathcal{I}_n$, let $\Delta(\theta)$ be the number of Latin squares L of order n for which $\theta \in \mathrm{Atp}(L)$. Let $\mathrm{Atp}(n) = \{\theta \in \mathcal{I}_n : \Delta(\theta) > 0\}$ and $\mathrm{Aut}(n) = \{\alpha \in S_n : (\alpha, \alpha, \alpha) \in \mathrm{Atp}(n)\}$. Hence (Q) can be rephrased as "What is $\mathrm{Atp}(n)$?"

We show in Section 2 that the value of $\Delta(\theta)$ depends only on the cycle structures of the components α, β and γ of $\theta = (\alpha, \beta, \gamma)$. In Section 3 we establish several necessary conditions for an isotopism to be an autotopism. These conditions go a long way toward describing $\mathrm{Atp}(n)$ for all $n \leqslant 17$, with only a few *ad hoc* computations needed.

To demonstrate that $\theta \in \mathrm{Atp}(n)$, it is usually necessary to give an explicit construction of a Latin square L with $\theta \in \mathrm{Atp}(L)$. In Section 4 we present two visual tools, called block diagrams and contours, that allow us to describe the required Latin squares without impenetrable notation. Additionally, more specialized means of constructing contours of Latin squares are given in Section 6.

We call a cycle of a permutation *nontrivial* if it has length greater than one. In Theorem 5.2 we characterize all automorphisms whose nontrivial cycles are of the same length.

In Theorem 7.1 we characterize all automorphisms that contain precisely two nontrivial cycles. In Theorem 8.1 we characterize all automorphisms that contain precisely three nontrivial cycles.

Our computational results are summarized in Section 9 and Appendix A, where we determine $\mathrm{Atp}(n)$ for $12 \leqslant n \leqslant 17$. Combined with the previous results of Falcón [17] (which we verify), this identifies $\mathrm{Atp}(n)$ for all $n \leqslant 17$.

Open problems and conjectures are presented in the final section.

1.2 Motivation and literature review

For a notion as pervasive as symmetry it is infeasible to survey all the relevant results within the vast literature on Latin squares and quasigroups. The problem is exacerbated by the fact that results may be proved about symmetries of other objects that implicitly imply results about symmetries of Latin squares. For instance, Colbourn and Rosa [8, Section 7.4] asked which permutations are automorphisms of Steiner triple systems, hence addressing our question (Q) for Steiner quasigroups (i.e. Latin squares that are idempotent and totally symmetric). To give another example, autotopisms of Latin squares inherited from one-factorizations of graphs were studied in [52].

There are quite a few recent results on Latin squares where understanding of autotopisms has been critical. In [3, 37, 45, 46, 47], autotopisms were used to establish congruences that the number of Latin squares of given order must satisfy (see also [44]). Similar ideas were used by Drisko [14] to prove a special case of the Alon-Tarsi Conjecture (see also [48]). It was shown in [37] that the autotopism group of almost all Latin squares is trivial, thereby revealing that the asymptotic ratio of the number of Latin squares to the number of isotopism classes of Latin squares of order n is $(n!)^3$. Imposing a large autotopism group can make it feasible to look for Latin squares with desirable properties in search spaces that would otherwise be too large [50], and also to show that certain properties hold in a Latin square [34, 50]. Ganfornina [19, 20] suggested using Latin squares that admit certain autotopisms for secret sharing schemes. During the course of resolving the existence question for near-automorphisms, [7] classified when a Latin rectangle completes to a Latin square that admits an autotopism with a trivial first component.

There are also many results concerning autotopisms of quasigroups and *loops*, that is, quasigroups with a neutral element. In loop theory, autotopisms have been useful in the study of specific varieties of loops, particularly those in which the defining identities can be expressed autotopically. For example, a loop is *Moufang* [33] if it satisfies the identity $(xy)(zx) = x((yz)x)$. This is equivalent to the assertion that for each x the triple (L_x, R_x, L_xR_x) is an autotopism, where $L_x(y) = xy$ and $R_x(y) = yx$ for all y. Thus Moufang loops can be studied by considering these and other autotopisms [1, Chapter V], a point of view that culminates in the theory of groups with triality [10]. Other varieties of loops in which the defining identities have autotopic characterizations include conjugacy closed loops [22], extra loops [29], and Buchsteiner loops [9]. A new, systematic look at the basic theory of loops defined in this way can be found in [11]. Automorphisms have not played quite the same role in loop theory as they do in group theory, primarily due to the fact that inner mappings (stabilizers of the neutral element in the permutation group generated by all L_x and R_x) are generally not automorphisms. Worth mentioning is the study of loops

with transitive automorphism groups [12, 13], and of loops in which every inner mapping is actually an automorphism [2, 25, 26].

We conclude the literature review with a summary of some results specifically concerning (Q). The first result was obtained by Euler [16] in 1782. He answered (Q) when α, β and γ are all n-cycles. This was generalized by Wanless [49] in 2004, who answered (Q) for isomorphisms containing a single nontrivial cycle. Bryant, Buchanan and Wanless [5] later extended the results in [49] to include quasigroups with additional properties, such as semisymmetry or idempotency.

In 1968, Sade [41] answered (Q) for an isotopism θ with a trivial component; a condition that was rediscovered in [20, 30]. Actually, these papers proved only the necessity of the condition, but the sufficiency is easy to show, cf. Theorem 3.4.

In 2007, McKay, Meynert and Myrvold [36] derived an important necessary condition for $\theta \in \mathcal{I}_n$ to belong to $\mathrm{Atp}(n)$ (see Theorem 3.3) in the course of enumerating quasigroups and loops up to isomorphism for orders $\leqslant 10$. Recently, Hulpke, Kaski and Östergård [24] gave a detailed account of the symmetries of Latin squares of order 11.

McKay, Meynert and Myrvold [36] also identified graphs whose automorphism groups are isomorphic to $\mathrm{Atp}(L)$ and $\mathrm{Aut}(L)$. This enabled them to use the graph isomorphism software `nauty` [35] to efficiently calculate the autotopism groups of Latin squares. A different procedure for finding the automorphism group of L, based on equational invariants, was implemented in the `LOOPS` [39, 40] package for `GAP` [21].

Also in 2007, Falcón and Martín-Morales [18] gave the nonzero values of $\Delta(\theta)$ for all $\theta \in \mathcal{I}_n$ with $n \leqslant 7$. Later, Falcón [17] determined $\mathrm{Atp}(n)$ for all $n \leqslant 11$, and he gave several results of general nature.

Kerby and Smith [27, 28] considered (Q) for isomorphisms from an algebraic point of view. The divisors of $\Delta(\theta)$, for isomorphisms θ, were discussed in [42] and were used to determine the parity of the number of quasigroups for small orders.

2 Cycle structure

We begin by identifying an equivalence relation on isotopisms that preserves the value of Δ. Given a Latin square $L = L(i, j)$ of order n we can construct a set of n^2 ordered triples

$$O(L) = \big\{\big(i, j, L(i, j)\big) : i, j \in [n]\big\}$$

called the *orthogonal array representation* of L. We will call the elements of $O(L)$ *entries* of L. Conversely, if O is a set of n^2 triples $\big(i, j, L(i, j)\big) \in [n] \times [n] \times [n]$ such that distinct triples differ in at least two coordinates, then O gives rise to a Latin square of order n.

The symmetric group S_3 has a natural action on $O(L)$. If $\lambda \in S_3$, 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 S_3 also acts on $\mathcal{I}_n = S_n \times S_n \times S_n$ by permuting the coordinates of $\mathcal{I}_n$. Given $\theta \in \mathcal{I}_n$ and $\lambda \in S_3$, we denote the resulting isotopism by θ^λ.

Lemma 2.1. *Let $\lambda \in S_3$, let $\theta, \varphi \in \mathcal{I}_n$, and let L be a Latin square of order n. Then*

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

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

Proof. To prove the first claim, observe that the following conditions are equivalent: $\varphi\theta\varphi^{-1} \in \mathrm{Atp}(\varphi(L))$, $\varphi\theta\varphi^{-1}\varphi(L) = \varphi(L)$, $\varphi\theta(L) = \varphi(L)$, $\theta(L) = L$, $\theta \in \mathrm{Atp}(L)$. The second claim is even more straightforward. □

Every $\alpha \in S_n$ 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 $c_1 > c_2 > \cdots > c_m \geqslant 1$ and there are λ_i cycles of length c_i in the unique cycle decomposition of α. Hence $c_1\lambda_1 + c_2\lambda_2 + \cdots + c_m\lambda_m = n$. If $\lambda_i = 1$, we usually write c_i instead of c_i^1 in the cycle structure.

We define the *cycle structure* of $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ to be the ordered triple of cycle structures of α, β and γ.

Since two permutations in S_n are conjugate if and only if they have the same cycle structure [6, p. 25], we deduce from Lemma 2.1 that the value of $\Delta(\theta)$ depends only on the (unordered) cycle structure of θ. In particular, if α, β and γ have the same cycle structures then $\Delta((\alpha, \beta, \gamma)) = \Delta((\alpha, \alpha, \alpha))$.

We say that a permutation in 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 $i < j$. The purpose of this definition is to establish a unique way of writing a representative permutation with a given cycle structure. For instance, if we consider permutations with the cycle structure $3{\cdot}2{\cdot}1^2$, then $(123)(45)(6)(7) \in S_7$ is canonical, whereas $(357)(41)(2)(6)$, $(132)(45)(6)(7)$ and $(123)(45)(7)(6)$ are not.

By Lemma 2.1, while studying the value of $\Delta((\alpha, \beta, \gamma))$, we may assume that the permutations α, β and γ are canonical.

Finally, we deduce from Lemma 2.1 that for $\varphi \in \mathcal{I}_n$ the autotopism groups $\mathrm{Atp}(L)$ and $\mathrm{Atp}(\varphi(L))$ are conjugate in $\mathcal{I}_n$, and thus they are isomorphic. We will therefore study isotopisms modulo the equivalence induced by conjugation and parastrophy.

3 Conditions on isotopisms to be autotopisms

In this section we review and extend some important conditions for membership in $\mathrm{Atp}(n)$.

3.1 Previously known conditions

The following two lemmas are easy to observe. A submatrix of a Latin square L is called a *subsquare* of L if it is a Latin square.

Lemma 3.1. *Let L be a Latin square of order n that contains a subsquare of order m. Then either $m = n$ or $m \leqslant \lfloor \frac{1}{2}n \rfloor$.*

The *direct product* of two Latin squares L and L' of orders n and n', respectively, is a Latin square $K = L \times L'$ of order nn' defined by $K((i, i'), (j, j')) = (L(i, j), L'(i', j'))$.

The *direct product* of two permutations α of $[n]$ and α' of $[n']$ is defined by $(\alpha \times \alpha')(i, i') = (\alpha(i), \alpha'(i'))$.

Lemma 3.2. *Let L and L' be Latin squares such that $\theta = (\alpha, \beta, \gamma) \in \mathrm{Atp}(L)$ and $\theta' = (\alpha', \beta', \gamma') \in \mathrm{Atp}(L')$. Then $\theta \times \theta' \in \mathrm{Atp}(L \times L')$, where $\theta \times \theta' = (\alpha \times \alpha', \beta \times \beta', \gamma \times \gamma')$.*

We will only need Lemma 3.2 in the special case when $\theta' = (\mathrm{id}, \mathrm{id}, \mathrm{id})$ is the trivial autotopism. If the order of L' is n', then the cycle structure of $(\alpha, \beta, \gamma) \times (\mathrm{id}, \mathrm{id}, \mathrm{id})$ is the cycle structure of (α, β, γ) with the multiplicity of each cycle multiplied by n'.

Note that it is possible to have $\theta \times (\mathrm{id}, \mathrm{id}, \mathrm{id}) \in \mathrm{Atp}(nn')$ while $\theta \notin \mathrm{Atp}(n)$. For example, in Theorem 5.2 we will find that $(\alpha, \alpha, \alpha) \notin \mathrm{Atp}(n)$ if n is even and α is an n-cycle, but if $n' = 2$ (for example) then $(\alpha, \alpha, \alpha) \times (\mathrm{id}, \mathrm{id}, \mathrm{id}) \in \mathrm{Atp}(nn')$.

We begin our list of conditions for membership in $\mathrm{Atp}(n)$ with the aforementioned theorem of McKay, Meynert and Myrvold [36].

Theorem 3.3. *Let L be a Latin square of order n and let (α, β, γ) be a nontrivial autotopism of L. Then either*

(a) α, β and γ have the same cycle structure with at least 1 and at most $\lfloor \frac{1}{2}n \rfloor$ fixed points, or

(b) 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

(c) 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. Lemma 2.1 implies that the following theorem characterizes all nontrivial autotopisms with one trivial component.

Theorem 3.4 (Autotopisms with a trivial component)**.** *Let $\theta = (\alpha, \beta, \mathrm{id}) \in \mathcal{I}_n$. 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. The necessity was proved by Sade [41] and rediscovered in [20, 30]; a proof also appears in [17]. Let $L = L(i, j)$ be a Latin square with $\theta \in \mathrm{Atp}(L)$. If i belongs to a c-cycle of α and j belongs to a d-cycle in β, then the entry $(i, j, L(i, j))$ maps to $(i, \beta^c(j), L(i, j))$ by θ^c. Hence d divides c. A similar argument shows c divides d, so $c = d$. Thus α and β must contain only d-cycles.

To prove the converse, let $L = L(i, j)$ be the Latin square on the symbol set $[n]$ that satisfies $L(i, j) \equiv i + j \pmod{n}$. Now observe that $((12 \cdots n), (12 \cdots n)^{-1}, \mathrm{id})^{n/d} \in \mathrm{Atp}(L)$ and consists of n/d cycles of length d. □

Note that the proof of Theorem 3.4 implies that the full spectrum of possible cycle structures of autotopisms with a trivial component is displayed by Cayley tables of cyclic groups.

Remark 3.5. Let $\theta = (\alpha, \alpha, \mathrm{id})$. The evaluation of $\Delta(\theta)$ was studied by Laywine [30] and Ganfornina [20]. Unfortunately, [30] contained some errors (later corrected in [31]). Ganfornina [20] gave an explicit formula for $\Delta(\theta)$ if α consists of n/d cycles of length $d \leqslant 3$.

3.2 New conditions

We begin with the following necessary condition for membership in $\mathrm{Atp}(n)$.

Lemma 3.6. *Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be an autotopism of a Latin square L. If i belongs to an a-cycle of α and j belongs to a b-cycle of β, then $L(i,j)$ belongs to a c-cycle of γ, where $\mathrm{lcm}(a,b) = \mathrm{lcm}(b,c) = \mathrm{lcm}(a,c) = \mathrm{lcm}(a,b,c)$.*

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 $\lambda \in S_3$ by Lemma 2.1. □

Lemma 3.6 precludes many isotopisms from being autotopisms. For example, there is no autotopism with cycle structure $(3^2{\cdot}2^3, 3^4, 2^6)$.

For our next lemma, we will need to introduce the notion of a strongly lcm-closed set. Let $\mathbb{N} = \{1, 2, \ldots\}$. A nonempty subset Λ of $\mathbb{N}$ is *strongly lcm-closed* if for every $a, b \in \mathbb{N}$ we have $\mathrm{lcm}(a,b) \in \Lambda$ if and only if $a \in \Lambda$ and $b \in \Lambda$. Strongly lcm-closed sets are precisely the ideals in the divisibility lattice on the set of positive integers. If Λ is a finite strongly lcm-closed set, then Λ is the set of divisors of $\max \Lambda$. However, we wish to also consider infinite strongly lcm-closed sets.

For $i \geqslant 1$, let p_i be the i-th prime. For any map $f : \mathbb{N} \to \mathbb{N} \cup \{0, \infty\}$, the set

$$\Lambda(f) = \Big\{ \prod_{i \in I} p_i^{k_i} : \ I \text{ is a finite subset of } \mathbb{N} \text{ and each } k_i \in \mathbb{N} \cup \{0\} \text{ where } k_i \leqslant f(i) \Big\}$$

is strongly lcm-closed. Moreover, it is not hard to see that every strongly lcm-closed set can be obtained in this way for some suitable f.

We will now show 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 $S = \{L(i,j) : i \in R \text{ and } j \in C\}$, so $|R| = |C| = |S|$. We will say M is *closed* under the action of θ (more formally, under the action of the subgroup generated by 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

$$\begin{aligned} R_\Lambda &= \{i \in [n] : \ i \text{ belongs to an } a\text{-cycle in } \alpha \text{ and } a \in \Lambda\}, \\ C_\Lambda &= \{i \in [n] : \ i \text{ belongs to a } b\text{-cycle in } \beta \text{ and } b \in \Lambda\}, \\ S_\Lambda &= \{i \in [n] : \ i \text{ belongs to a } c\text{-cycle in } \gamma \text{ and } c \in \Lambda\}. \end{aligned}$$

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

Theorem 3.7. *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 $|R_\Lambda| = |C_\Lambda| = |S_\Lambda| = \frac{1}{2}n$ *then* L *has four subsquares, each with autotopisms induced by* θ*. The subsquares are on the rows, columns and symbols* $(R_\Lambda, C_\Lambda, S_\Lambda)$*,* $(R_\Lambda, \overline{C_\Lambda}, \overline{S_\Lambda})$*,* $(\overline{R_\Lambda}, C_\Lambda, \overline{S_\Lambda})$ *and* $(\overline{R_\Lambda}, \overline{C_\Lambda}, S_\Lambda)$*.*

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.

Pick an entry $(i, j, L(i, j))$ in M. Then i belongs to an a-cycle of α for some $a \in \Lambda$ and j belongs to a b-cycle of β for some $b \in \Lambda$. Suppose $L(i, j)$ belongs to a c-cycle of γ. By Lemma 3.6, $\operatorname{lcm}(a, c) = \operatorname{lcm}(a, b)$. Since Λ is a strongly lcm-closed set, we deduce that $\operatorname{lcm}(a, c) \in \Lambda$ and $c \in \Lambda$. Therefore, every symbol in M belongs to S_Λ and so $|S_\Lambda| \geqslant |R_\Lambda|$. Hence $|R_\Lambda| = |C_\Lambda| = |S_\Lambda|$ and M is a subsquare of L.

To prove that θ_M is indeed an autotopism of M, we merely note that R_Λ, C_Λ and S_Λ are closed under the action of $\langle\alpha\rangle$, $\langle\beta\rangle$ and $\langle\gamma\rangle$, respectively.

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. □

For instance, by considering the strongly lcm-closed set $\Lambda = \{1, 2\}$, Theorem 3.7 implies that there is no autotopism (α, β, γ) such that α has cycle structure $4{\cdot}2^2$ and β has cycle structure 2^4. A square with such an autotopism would contain a 4×8 "subsquare", which is impossible.

The next necessary condition for membership in $\operatorname{Atp}(n)$ checks whether we can find enough room in a Latin square L with $\theta \in \operatorname{Atp}(L)$ to place all n copies of each symbol so that Lemma 3.6 is satisfied.

The *permanent* of an $n \times n$ square matrix $X = X(i, j)$ is defined as

$$\textsc{per}(X) = \sum_{\sigma \in S_n} \prod_{i \in [n]} X\big(i, \sigma(i)\big).$$

In particular, if X is an $n \times n$ $(0, 1)$-matrix, then $\textsc{per}(X)$ counts the number of $n \times n$ permutation matrices that embed into X. We direct the reader to [38] for more information on permanents.

Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ and suppose $s \in [n]$ belongs to a c-cycle in γ. We define $X_s = X_s(i, j)$ to be the $(0, 1)$-matrix with $X_s(i, j) = 1$ if i belongs to an a-cycle of α and j belongs to a b-cycle of β such that $\operatorname{lcm}(a, b) = \operatorname{lcm}(b, c) = \operatorname{lcm}(a, c) = \operatorname{lcm}(a, b, c)$, and $X_s(i, j) = 0$ otherwise. Informally, the zeroes in X_s mark the positions where Lemma 3.6 says a symbol s cannot be placed in a Latin square L of order n with $\theta \in \operatorname{Atp}(L)$.

If $\theta \in \operatorname{Atp}(L)$ for some Latin square L of order n, then the copies of the symbol s in L identify a permutation matrix embedded in X_s. Hence we have just proved the following result.

Lemma 3.8. *Let* $\theta \in \mathcal{I}_n$*. If* $\theta \in \operatorname{Atp}(n)$ *then* $\textsc{per}(X_s) > 0$ *for all* $s \in [n]$*.*

To illustrate, let $n = 6 + 3k + 2\ell$ for some integers $k \geqslant 1$ and $\ell \geqslant 4$, and suppose that $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ is such that α, β and γ have cycle structure $6{\cdot}3^k{\cdot}2^\ell$. Consider the $(0, 1)$-matrix X_s for some s that belongs to a 3-cycle in γ. Note that $X_s(i, j) = 0$ when i belongs to a 2-cycle in α and j belongs to either a 2-cycle or 3-cycle in β. In particular, X_s has a

$(2\ell) \times (n-6)$ zero submatrix, and $2\ell + n - 6 > n$ so $\text{PER}(X_s) = 0$ (by the Frobenius-König Theorem [38, p.31]). Hence, Lemma 3.8 implies that $\theta \notin \text{Atp}(n)$.

We will establish additional conditions on the cycle structure of autotopisms in Section 5, but first we need to develop some visual tools.

4 Block diagrams and contours

In this section we introduce two visual tools for constructing Latin squares with a prescribed automorphism: block diagrams and contours. We start by looking at orbits of cells of Latin squares under the action induced by an autotopism.

Suppose that $\theta = (\alpha, \beta, \gamma)$ is an autotopism of a Latin square L, where α and β are canonical. If i is a leading symbol in a cycle of α, j is a leading symbol in a cycle of β, and $L(i,j) = k$, the orbit of the entry $(i,j,k) \in O(L)$ under the action of θ will look like

	j	$j+1$	$j+2$	$\cdots$
i	k			
$i+1$		$\gamma(k)$		
$i+2$			$\gamma^2(k)$	
$\vdots$				$\ddots$

.

The set of cells $\{(\alpha^r(i), \beta^r(j)) : r \geqslant 0\}$ is called a *cell orbit*. Of course, the "shape" of the orbit depends on the lengths of the cycles of α and β containing i and j, respectively. For instance, if i is in a 2-cycle of α and j is in a 6-cycle of β, the orbit of (i,j,k) looks like

	j	$j+1$	$j+2$	$j+3$	$j+4$	$j+5$
i	k		$\gamma^2(k)$		$\gamma^4(k)$	
$i+1$		$\gamma(k)$		$\gamma^3(k)$		$\gamma^5(k)$

.

This forces γ to behave in a certain way, as described in Lemma 3.6.

Note the special shape of the orbit when either i is a fixed point of α or j is a fixed point of β.

Although it is possible to continue the discussion for general autotopisms, we will mostly deal only with automorphisms.

4.1 Block diagrams

As we are going to see in Section 4.2, constructing a Latin square L with a prescribed automorphism α can be reduced to a careful placement of leading symbols of α into L. We would therefore like to know how the leading symbols of α are distributed in L.

For the rest of this paper, let $\alpha_1, \alpha_2, \ldots, \alpha_m$ be the nontrivial cycles of $\alpha \in S_n$ with lengths $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_m$, respectively. For $1 \leqslant i \leqslant m$, let $t_i = 1 + \sum_{j<i} d_j$ be the non-fixed leading symbols of α. Let α_∞ be the set of all fixed points of α, and let $d_\infty = |\alpha_\infty|$. Let $[m]^* = [m] \cup \{\infty\}$. For any $i, j \in [m]^*$, let M_{ij} be the *block* of L formed by the rows whose indices are in the cycle α_i and columns whose indices are in the cycle α_j.

Blocks will be our basic "unit of construction". In Lemma 4.1, we will give conditions that can be used to diagnose whether or not a given collection of blocks determines a Latin square with a specific automorphism. Previous efforts to construct or enumerate Latin squares with a given autotopism (e.g. [18, 36, 42]) have tended to build the squares block by block, although the terminology and notation has varied.

We write $\alpha_k : f_k$ in a block M_{ij} if every symbol in α_k (equivalently, the leading symbol of α_k) appears in M_{ij} precisely $f_k = f_k(i,j)$ times. If $f_k = 0$, we usually omit $\alpha_k : f_k$. The result is the *block diagram* of L according to the cycles of α.

Although there are situations when the block diagram depends only on α (that is, every Latin square L with $\alpha \in \mathrm{Aut}(L)$ has the same block diagram), generally this is not the case. For example, here are two Latin squares with distinct block diagrams for the automorphism (123)(456):

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

$\rightarrow$

	α_1	α_2
α_1	$\alpha_1 : 3$ $\alpha_2 : 0$	$\alpha_1 : 0$ $\alpha_2 : 3$
α_2	$\alpha_1 : 0$ $\alpha_2 : 3$	$\alpha_1 : 3$ $\alpha_2 : 0$

and

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

$\rightarrow$

	α_1	α_2
α_1	$\alpha_1 : 2$ $\alpha_2 : 1$	$\alpha_1 : 1$ $\alpha_2 : 2$
α_2	$\alpha_1 : 1$ $\alpha_2 : 2$	$\alpha_1 : 2$ $\alpha_2 : 1$

While constructing a block diagram, it is helpful to keep in mind that in every block M_{ij} we must have $d_1 f_1(i,j) + d_2 f_2(i,j) + \cdots + d_m f_m(i,j) + d_\infty f_\infty(i,j) = d_i d_j$. In addition, for any $i \in [m]^*$ the $d_i \times n$ submatrix $\bigcup_{j \in [m]^*} M_{ij}$ contains exactly d_i copies of each symbol in $[n]$. Hence

$$\sum_{j \in [m]^*} f_k(i,j) = d_i \tag{4.1}$$

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

To further illustrate the concept of a block diagram, let us determine the block diagram of any Latin square L with $\alpha \in \mathrm{Aut}(L)$, where α has cycle structure $d_1 \cdot d_2 \cdot 1^{d_\infty}$ with $d_1 > d_2 > 1$, which is depicted in Figure 1. The $M_{\infty\infty}$ block contains only fixed points by Lemma 3.6 and hence it contains each fixed point d_∞ times. Similarly, for $1 \leqslant i \leqslant 2$, the blocks $M_{i\infty}$ and $M_{\infty i}$ contain only symbols of α_i, each d_∞ times. Since $d_1 > d_2$, the blocks M_{12} and M_{21} must contain only symbols of α_1, each d_2 times. The structure of the remaining blocks M_{11} and M_{22} follows from (4.1). So, in this case, the block diagram is determined by α. In Theorem 7.1 we will give necessary and sufficient conditions for the existence of a Latin square L having this α as an automorphism.

4.2 Contours

Consider $\alpha = (123)(4)(5)$, and observe that $\alpha \in \mathrm{Aut}(5)$, since it is an automorphism of the Latin square

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

. (4.2)

	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_∞	$\alpha_1 : d_\infty$	$\alpha_2 : d_\infty$	$\alpha_\infty : d_\infty$

Figure 1: Block diagram of L with $d_1 > d_2$ the only nontrivial cycle lengths.

Note that the placement of the horizontal (or vertical) lines in (4.2) determines α, since α is canonical. Moreover, the Latin square (4.2) and α can be reconstructed from the knowledge of

1	4	5	·	·
·	·	·	·	1
·	·	·	1	·
·	·	1	4	5
·	1	·	5	4

.

We call such a diagram a *contour* $\mathcal{C}$ of α, provided it only contains leading symbols, each cell orbit contains precisely one leading symbol, and the diagram determines a Latin square L with $\alpha \in \mathrm{Aut}(L)$.

The following lemma describes what needs to be checked in a purported contour to ensure that it is indeed a contour.

Lemma 4.1. *Consider a canonical $\alpha \in S_n$. Let T be the set of all leading symbols of α. Then a partial matrix $\mathcal{C}$ of order n, divided into blocks according to the cycle structure of α, is a contour of α if and only if all of the following conditions are satisfied:*

(a) $\mathcal{C}$ is a partial Latin square (that is, any symbol occurs at most once in each row and each column) and every symbol of $\mathcal{C}$ is from T.

(b) Let B be an $a \times b$ block of $\mathcal{C}$. Then B contains precisely $\gcd(a, b)$ symbols from T, all in distinct cell orbits of B.

(c) If $z \in T$ is a symbol in an $a \times b$ block, then z belongs to a c-cycle of α such that $\mathrm{lcm}(a, b) = \mathrm{lcm}(b, c) = \mathrm{lcm}(a, c) = \mathrm{lcm}(a, b, c)$.

(d) Let $z \in T$ be in a c-cycle of α. If two distinct rows i and i' both contain a copy of z and belong to the same a-cycle of α, then $i \not\equiv i' \pmod{\gcd(a, c)}$.

(e) Let $z \in T$ be in a c-cycle of α. If two distinct columns j and j' both contain a copy of z and belong to the same b-cycle of α, then $j \not\equiv j' \pmod{\gcd(b, c)}$.

Proof. A detailed proof of this result can be found in [43, pp. 111–112]. Here we offer some guiding observations. Remaining details are direct consequences of our definitions or are otherwise routine to complete. Let (i, j, k) be an entry in an $a \times b$ block and suppose

k belongs to a c-cycle of α. There are $ab/\operatorname{lcm}(a,b) = \gcd(a,b)$ distinct cell orbits in the block containing the entry (i,j,k). This explains condition (b). The cell orbit through (i,j,k) contains $\operatorname{lcm}(a,b)$ entries. The symbol k will therefore appear $\operatorname{lcm}(a,b)/c$ times in the cell orbit, spaced evenly in rows with increments of $a/(\operatorname{lcm}(a,b)/c) = ac/\operatorname{lcm}(a,b) = ac/\operatorname{lcm}(a,c) = \gcd(a,c)$ rows, and similarly spaced evenly in columns with increments of $\gcd(b,c)$ columns. Hence (d) and (e) are required to prevent repeated symbols within rows and columns respectively. Condition (c) is necessary by Lemma 3.6. □

As well as contours we will talk of *partial contours*, which we define to be the restriction of a contour to a block or union of blocks. A partial contour should be such that it does not result in any violation of the conditions in Lemma 4.1 within the blocks on which it is defined.

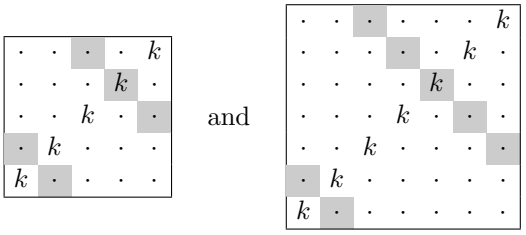
We will now develop techniques that allow us to check most of the conditions of Lemma 4.1 visually. For instance, conditions (d) and (e) can be fulfilled by placing identical leading symbols into consecutive rows and consecutive columns in a given block. The building blocks of contours introduced in Section 4.3 will help with conditions (a) and (b), while the block diagrams of Section 4.1 are designed to cope with condition (c).

4.3 Basic block patterns

A contour of α decomposes into partial contours according to the blocks determined by the cycles of α. We collect here several constructions for partial contours. The action of α on the cells of a block M_{ij} partitions it into $g = \gcd(d_i, d_j)$ disjoint cell orbits. Each of these cell orbits should contain exactly one leading symbol. The action of α can then be used to fill the remaining cells in each cell orbit, thereby completing the block.

The patterns in this section are intended to be an informal guide only. They represent configurations that occur many times in our specific constructions in later sections. Those sections should be consulted for concrete examples. Our aim here is just to present the intuition behind what we do later.

The odd pattern If g is odd, then by the *odd pattern* we refer to a partial contour where the cells on the main antidiagonal of some $g \times g$ contiguous submatrix of M_{ij} are filled, such as in

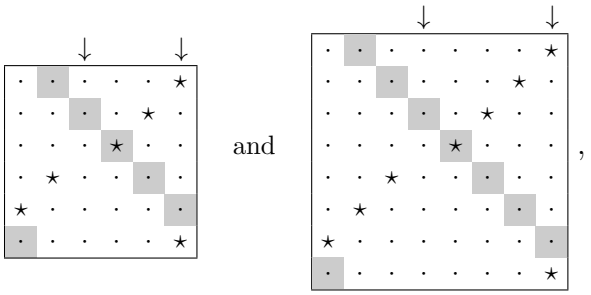


(4.3)

The shaded cells highlight a cell orbit and k is a leading symbol from an $\operatorname{lcm}(d_i, d_j)$-cycle. Any pattern obtained from the odd pattern by cyclically permuting its rows or columns can also be thought of as an odd pattern.

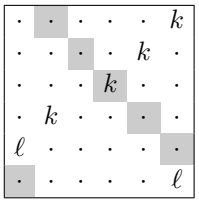
The even pattern Now consider a $g \times g$ contiguous submatrix when g is even. We can see (cf. Theorem 5.1) that a partial contour containing a unique cell from each row, column,

and cell orbit cannot be realized. Consequently, in most of the constructions in this paper, the cycles of even length will be more difficult to handle than cycles of odd length. However, the *even pattern*



comes close, with one cell in each row, each cell orbit, and all but two of the columns (marked by arrows). In general, an even pattern is formed by starting with the main antidiagonal and (cyclically) shifting half of the occupied cells by one position.

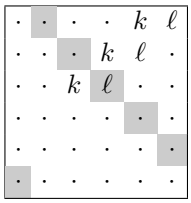
If k is a leading symbol from an $\operatorname{lcm}(d_i, d_j)$-cycle and ℓ is a leading symbol from a c-cycle (where c divides $\operatorname{lcm}(d_i, d_j)$, as required by Lemma 3.6), we can find a partial contour for M_{ij}, such as in



(4.4)

for example. Conditions (a)–(c) of Lemma 4.1 are then satisfied within the block M_{ij}, and we also observe that conditions (d) and (e) of Lemma 4.1 are satisfied for the symbol k within M_{ij}. Provided there are not too many copies of ℓ, we can observe that conditions (d) and (e) of Lemma 4.1 are also satisfied for the symbol ℓ within M_{ij}, since the symbols are located in consecutive rows and columns. In this case, (4.4) is a partial contour.

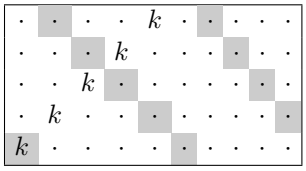
The staircase pattern Again with g even, if k and ℓ are leading symbols of two $\operatorname{lcm}(d_i, d_j)$-cycles in α, then we can use a partial contour that embeds in a $g \times g$ contiguous submatrix, such as



which we call the *staircase pattern*.

Rectangular blocks The above block patterns can also be used to fill rectangular blocks. For instance, if a is an odd divisor of b, we can place leading symbols k from a b-cycle into

an $a \times b$ block by filling an $a \times a$ submatrix with an odd pattern, as in



.

Additional block patterns will be given in Section 6.

4.4 Notation in contours

To save space and improve legibility, we will from now on reserve certain symbols to denote leading symbols of cycles in contours.

As usual, we assume α has cycles $\alpha_1, \alpha_2, \alpha_3, \ldots$ of lengths $d_1 \geqslant d_2 \geqslant d_3 \geqslant \cdots$, respectively. We use

$$\begin{aligned} \star &\text{ to denote the leading symbol of } \alpha_1, \\ \circ &\text{ to denote the leading symbol of } \alpha_2, \\ \bullet &\text{ to denote the leading symbol of } \alpha_3, \text{ and} \\ \infty &\text{ to denote a fixed point.} \end{aligned}$$

Hence the numerical equivalents of $\star$, $\circ$, and $\bullet$ are $t_1 = 1$, $t_2 = d_1 + 1$, and $t_3 = d_1 + d_2 + 1$, respectively.

Since we also wish to construct contours in proofs without regard to the parity of d_1, we define offsets $\mathcal{O}_{1,i}$ for $1 \leqslant i \leqslant d_1$ by

$$\mathcal{O}_{1,i} = \begin{cases} 1 & \text{if } d_1 \text{ is even and } \frac{1}{2}d_1 < i < d_1, \\ 1 - d_1 & \text{if } d_1 \text{ is even and } i = d_1, \\ 0 & \text{otherwise.} \end{cases}$$

The cells in the block M_{11} with coordinates $(i, d_1 + 1 - i - \mathcal{O}_{1,i})$ for $1 \leqslant i \leqslant d_1$ then define an odd or even pattern in accordance with the parity of d_1.

5 Automorphisms with all nontrivial cycles of the same length

In this section we characterize all automorphisms of Latin squares whose nontrivial cycles have the same length. We begin with the following theorem from [49].

Theorem 5.1. *If $\alpha \in S_n$ 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 $\lceil \frac{1}{2}n \rceil \leqslant d < n$.*

We will now prove a generalization of Theorem 5.1, when α consists of an arbitrary number of cycles of the same length. We remark that in 1782 Euler [16] proved a result equivalent to the special case of Theorem 5.1 with $d = n$ and no fixed points.

Theorem 5.2 (Automorphisms with all nontrivial cycles of the same length)**.** *Suppose that $\alpha \in S_n$ 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.*

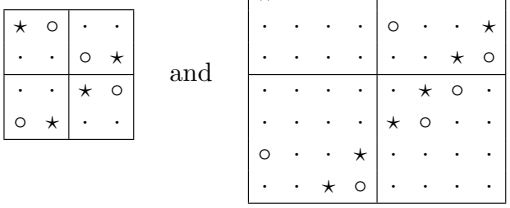
Proof. We begin with Case I, where we assume α has no fixed points.

Case I(a): d is odd (m may be even or odd). Theorem 5.1 and Lemma 3.2 imply that there exists a Latin square L with $\alpha \in \mathrm{Aut}(L) \subseteq \mathrm{Aut}(n)$.

Case I(b): both d and m are even. It is sufficient to show that $\alpha \in \mathrm{Aut}(n)$ when $m = 2$, since the rest of this case then follows from Lemma 3.2. When $m = 2$, we identify a contour $\mathcal{C}$ comprising of four identical staircase patterns, suitably shifted. We define M_{11} and M_{12} respectively by

$$\begin{aligned} \mathcal{C}(i, d/2+1-i) &= t_1 \quad \text{for } 1 \leqslant i \leqslant d/2, \\ \mathcal{C}(i, d/2+2-i) &= t_2 \quad \text{for } 1 \leqslant i \leqslant d/2, \\ \mathcal{C}(d/2+1, d+1) &= t_2, \\ \mathcal{C}(d/2+i, 2d+1-i) &= t_1 \quad \text{for } 1 \leqslant i \leqslant d/2, \\ \mathcal{C}(d/2+1+i, 2d+1-i) &= t_2 \quad \text{for } 1 \leqslant i \leqslant d/2-1, \end{aligned}$$

then let $M_{11} = M_{22}$ and $M_{12} = M_{21}$. For example, the contours for $d \in \{2, 4\}$ are



The conditions of Lemma 4.1 can be readily verified. Conditions (a) and (b) are immediate from the construction. Since both cycles of α have the same length, condition (c) is satisfied. The staircase pattern ensures conditions (d)–(e) are satisfied. Hence we have indeed constructed a contour $\mathcal{C}$. (In later constructions we will not explicitly describe how Lemma 4.1 is satisfied.)

Case I(c): d is even and m is odd, whence

$$\alpha = (12 \cdots d)(d+1 \cdots 2d) \cdots ((m-1)d+1 \cdots md).$$

Suppose, seeking a contradiction, that $L = L(i, j)$ is a Latin square of order n such that $\alpha \in \mathrm{Aut}(L)$.

Consider the first row of the $d \times d$ block of L with top left corner $(dr+1, ds+1)$, for some r and s satisfying $0 \leqslant r \leqslant m-1$ and $0 \leqslant s \leqslant m-1$. Then, calculating modulo d,

since α is an automorphism of L, we have

$$\sum_{t=1}^{d} L(dr+t, ds+1) = \sum_{t=0}^{d-1} L(dr+d-t, ds+1) = \sum_{t=0}^{d-1} L\big(\alpha^{-t}(dr+d), \alpha^{-t}(ds+1+t)\big)$$
$$= \sum_{t=0}^{d-1} \alpha^t\big(L(dr+d, ds+1+t)\big) \equiv \sum_{t=0}^{d-1} \Big(L(dr+d, ds+1+t)+t\Big).$$

Using this congruence and the fact that every row and column sums to $n(n+1)/2$, we obtain

$$m\frac{n(n+1)}{2} = \sum_{s=0}^{m-1}\sum_{i=1}^{n} L(i, ds+1) = \sum_{r=0}^{m-1}\sum_{s=0}^{m-1}\sum_{t=1}^{d} L(dr+t, ds+1)$$
$$\equiv \sum_{r=0}^{m-1}\sum_{s=0}^{m-1}\sum_{t=0}^{d-1} \big(L(dr+d, ds+1+t)+t\big) = m^2\sum_{t=0}^{d-1} t + \sum_{r=0}^{m-1}\sum_{j=1}^{n} L(dr+d, j)$$
$$= m^2\frac{(d-1)d}{2} + m\frac{n(n+1)}{2},$$

and hence $\frac{1}{2}m^2(d-1)d \equiv 0 \pmod{d}$. This contradicts our assumption that d is even and m is odd.

Case II: α has at least one fixed point, so $n > md$. If $n > 2md$ then $\alpha \notin \mathrm{Aut}(n)$ by Theorem 3.3. If $n \leqslant 2md$, Theorem 5.1 guarantees the existence of a Latin square of order n that admits the automorphism $\omega = (12\cdots(md))(md+1)\cdots(2md)$ and so $\omega^m \in \mathrm{Aut}(n)$. Since ω^m has the same cycle structure as α, Lemma 2.1 implies $\alpha \in \mathrm{Aut}(n)$. □

Corollary 5.3. *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 L is a Latin square of order n that admits the autotopism θ. Define the strongly lcm-closed set $S = \{s \in \mathbb{N} : 2^{a+1} \text{ does not divide } s\}$. Theorem 3.7 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 indivisible by 2^{a+1}. Hence the order of θ_M is $2^a x$ for some odd $x \geqslant 1$.

The order of M is $2^a b$ for some odd $b \geqslant 1$ (otherwise 2^{a+1} divides n). 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 5.2 implies that $(\theta_M)^x \notin \mathrm{Atp}(2^a b)$, giving a contradiction. □

Kerby and Smith [28] independently obtained the case of Corollary 5.3 when θ is an automorphism. The special case when all cycles have length two can be found in the proof of [36, Lemma 4].

6 Some useful partial contours

There are several situations that arise repeatedly while constructing a Latin square with a prescribed automorphism. We now give a sequence of lemmas that handle these situations.

As usual, we assume that $\alpha \in S_n$ is canonical and has nontrivial cycles of lengths $d_1 \geqslant d_2 \geqslant \cdots \geqslant d_m$ and $d_\infty \geqslant 0$ fixed points.

First we look at adding fixed points to an existing construction.

Lemma 6.1. *Suppose $\alpha \in \mathrm{Aut}(L)$ for some Latin square L of order n. Let μ be the minimum, over $k \in [m]$, of the number of occurrences of the leading symbol t_k in block M_{kk}. Then for $0 \leqslant \nu \leqslant \mu$ there exists a Latin square L' of order $n + \nu$ that admits an automorphism α' with cycles of lengths $d_1, d_2, \ldots, d_m$ and $d_\infty + \nu$ fixed points.*

Proof. We use a procedure known as *prolongation* to construct L' from L. We assume $\nu = 1$; the remainder of the lemma follows by induction. We may also assume that α and α' are canonical. We use M_{ij} to denote a block of L and M'_{ij} to denote a block of L'.

For each $k \in [m]$, pick an entry (i, j, t_k) in the block M_{kk}. Define $L'(\alpha^r(i), n+1) = L'(n+1, \alpha^r(j)) = \alpha^r(t_k)$ and $L'(\alpha^r(i), \alpha^r(j)) = n+1$ for $0 \leqslant r \leqslant d_k - 1$. Then $M'_{\infty\infty}$ can be chosen arbitrarily from the Latin squares of order $d_\infty + 1$ on the symbols $\alpha_\infty \cup \{n+1\}$. The remainder of L' is the same as L. □

When attempting to construct a contour $\mathcal{C}$ for a Latin square that admits the automorphism α, Lemma 4.1 implies that we may proceed block-by-block, in any order. We imagine that we build $\mathcal{C}$ from a series of partial contours, such that at each stage we introduce a new block M_{ij}. It is sufficient to check that, at each stage, the introduced block M_{ij} does not contradict conditions (a)–(e) of Lemma 4.1 with respect to itself and the other extant blocks in those rows and columns.

For the next lemma, we consider the case of when the nontrivial cycles of α have distinct lengths, and give sufficient conditions for the existence of blocks M_{ij} satisfying the conditions of Lemma 4.1, when either $i = \infty$ or $j = \infty$.

Lemma 6.2. *Suppose that no two nontrivial cycles of α have the same length.*

(i) If $\alpha \in \mathrm{Aut}(L)$ and $i \in [m]$, then the block $M_{i\infty}$ contains one copy of the leading symbol t_i in each column and no other leading symbols.

(ii) While constructing L such that $\alpha \in \mathrm{Aut}(L)$, if the region $\bigcup_{j\in[m]} M_{ij}$ for some $i \in [m]$ has been successfully completed and contains exactly $d_i - d_\infty$ copies of t_i, then $M_{i\infty}$ can also be completed.

Similar statements (transposed) hold for the blocks $M_{\infty i}$.

Proof. Assume that $\alpha \in \mathrm{Aut}(L)$. Then each column of $M_{i\infty}$ is a cell orbit and each must contain a leading symbol from a cycle of length $\mathrm{lcm}(d_i, 1) = d_i$, by Lemma 3.6. By assumption t_i is the only such leading symbol.

Now assume that L is under construction and we wish to achieve $\alpha \in \mathrm{Aut}(L)$. If there are $d_i - d_\infty$ copies of t_i in $\bigcup_{j\in[m]} M_{ij}$ then there are d_∞ rows where t_i does not occur in any of these blocks. We can place t_i in each of these rows within $M_{i\infty}$, with one copy of t_i per column and per row, but otherwise arbitrarily. It is easy to check that the conditions of Lemma 4.1 will continue to be satisfied. The transpose argument works for $M_{\infty i}$. □

The next result shows when it is possible to fill several subsquares at once, provided they only overlap in the block $M_{\infty\infty}$. Conditions for the existence of Latin squares with overlapping subsquares of various sizes were given in [4].

Lemma 6.3. *For $i \in [m]$, let λ_i be the number of cycles in α that have length d_i. Let $I = \{i \in [m];$ there is no $j \in [m]$ such that d_j is a proper divisor of $d_i\}$. For all $i \in I$, let $\mathcal{S}_i = \bigcup_{a,b} M_{ab}$ over all $a, b \in \{c \in [m] : d_c = d_i\} \cup \{\infty\}$.*

(i) If $\alpha \in \mathrm{Aut}(L)$, then $\mathcal{S}_i$ is a subsquare of L for every $i \in I$. Hence the region $\bigcup_{i\in I} \mathcal{S}_i$ can be filled independently of the remainder of L.

(ii) If $\alpha \in \mathrm{Aut}(L)$, then (a) $d_\infty \leqslant \lambda_i d_i$ for every $i \in I$ and (b) if d_i is even and λ_i is odd for some $i \in I$ then $d_\infty > 0$.

(iii) If α satisfies conditions (a)–(b) of (ii) above, then it is possible to fill the region $\bigcup_{i\in I} \mathcal{S}_i$.

Proof. Suppose L is a Latin square with $\alpha \in \mathrm{Aut}(L)$. For each $i \in I$, taking Λ as the set of divisors of d_i in Theorem 3.7 implies that $\mathcal{S}_i$ is a subsquare that admits an automorphism with the cycle structure $d_i^{\lambda_i} \cdot 1^{d_\infty}$, thus proving (i). Theorem 5.2, applied to each subsquare $\mathcal{S}_i$, now implies (ii).

The assumptions on α imply that any two distinct subsquares $\mathcal{S}_i$ and $\mathcal{S}_j$ intersect at $M_{\infty\infty}$ (which is empty if $d_\infty = 0$). If $d_\infty > 0$ then Theorem 3.7 with $\Lambda = \{1\}$ implies that $M_{\infty\infty}$ is a subsquare. Crucially, if $\mathcal{S}_i$ exists then we can replace its subsquare $M_{\infty\infty}$ by any other subsquare on the same symbols, without disrupting the automorphism that $\mathcal{S}_i$ is required to have. Hence, if the individual $\mathcal{S}_i$ exist, we may assume they share the same subsquare $M_{\infty\infty}$, which is the only place that they overlap. Thus $\bigcup_{i\in I} \mathcal{S}_i$ can be constructed if and only if all the individual $\mathcal{S}_i$ can be constructed, which happens if and only if the conditions of (ii) are satisfied, by Theorem 5.2. □

We next look at a useful way to construct a partial contour. In a block with g cell orbits, a *transversal* is a set of g cells that lie in different rows, different columns and different cell orbits. We will now give a simple but important condition for the existence of a transversal.

Lemma 6.4. *Let $S = \{(r_k, c_k)\}_{1\leqslant k\leqslant g}$ be a transversal of a $d_i \times d_j$ block M_{ij} with $i, j \in [m]$, where $g = \gcd(d_i, d_j)$. Then*

$$\sum_{k=1}^{g} c_k - \sum_{k=1}^{g} r_k \equiv \delta_g \pmod{g} \tag{6.1}$$

where

$$\delta_g = \sum_{k\in\mathbb{Z}_g} k \equiv \begin{cases} 0 \pmod{g} & \text{if } g \text{ is odd,} \\ \frac{1}{2}g \pmod{g} & \text{if } g \text{ is even.} \end{cases}$$

Proof. Label each cell of M_{ij} with its column index minus its row index, modulo g. The elements of S belong to different cell orbits of α if and only if their labels are distinct. Since there are g cell orbits, summing the labels yields (6.1), since every cell orbit is represented once in S. □

Lemma 6.4 is a standard argument on transversals; variants of it have been used, for example, in [15] and [53].

Let N be the smallest submatrix containing S in Lemma 6.4. It turns out that the necessary condition in Lemma 6.4 is also sufficient in several cases that will prove important to us later. These cases involve a situation where the rows and columns of N are contiguous within M_{ij}, except possibly for one gap, which either splits the rows and columns of N in half, or separates one column and one row from the remaining columns and rows of N. In the following result, e is the number of rows and columns in one of the two parts of N, h_1 is the vertical gap (between rows) and h_2 is the horizontal gap (between columns).

Lemma 6.5. *Suppose that N is a $g\times g$ submatrix of a $d_i\times d_j$ block M, where $g=\gcd(d_i,d_j)$. Suppose that for some integers r, c, e, h_1, h_2 the submatrix N is formed by the rows*

$$\{r-e+1,r-e+2,\dots,r\}\cup\{r+h_1+1,r+h_1+2,\dots,r+h_1+g-e\}$$

and columns

$$\{c-e+1,c-e+2,\dots,c\}\cup\{c+h_2+1,c+h_2+2,\dots,c+h_2+g-e\}$$

of M. Suppose further that $e=g-1$ or $g=2e$. Then for M to have a transversal inside N it is necessary and sufficient that

$$(h_1-h_2)e\equiv\delta_g \pmod g. \tag{6.2}$$

Proof. For the necessity we apply Lemma 6.4 and find that

$$\begin{aligned}\delta_g&=\sum_{i=1}^{e}\big((c-e+i)-(r-e+i)\big)+\sum_{i=1}^{g-e}\big((c+h_2+i)-(r+h_1+i)\big)\\&=g(c-r)+(g-e)(h_2-h_1)\\&\equiv(h_1-h_2)e \pmod g.\end{aligned}$$

To prove sufficiency, first suppose that $g=2e$. In this case $\delta_g=\frac12 g=e$ and $(h_1-h_2)e\equiv\delta_g \pmod g$ implies that h_1-h_2 is odd. Let T be the set of cells

$$\{(r-e+i,c+1-i):1\leqslant i\leqslant e\}\cup\{(r+h_1+i,c+h_2+e+1-i):1\leqslant i\leqslant e\}.$$

It is immediate that T has a representative from every row and column of N. Moreover, the labels on the cells in T (as defined in the proof of Lemma 6.4) are $\{c-r+1+e-2i:1\leqslant i\leqslant e\}\cup\{c-r+1+e+h_2-h_1-2i:1\leqslant i\leqslant e\}=\mathbb{Z}_g$ since h_2-h_1 is odd. Hence T is indeed a transversal.

Next suppose that $e=g-1$ and hence $h_2-h_1\equiv\delta_g \pmod g$. If g is even then we form T from the cells

$$\begin{aligned}\big\{(r+h_1+1,c+h_2+1)\big\}\cup\big\{(r-\tfrac12 g-i+2,c-g+i+1):1\leqslant i\leqslant\tfrac12 g\big\}\\\cup\big\{(r-i+1,c-\tfrac12 g+i+1):1\leqslant i\leqslant\tfrac12 g-1\big\}.\end{aligned}$$

The labels on these cells are

$$\{c-r+h_2-h_1\} \cup \{c-r-\tfrac{1}{2}g+2i-1 : 1 \leqslant i \leqslant \tfrac{1}{2}g\} \cup \big\{c-r-\tfrac{1}{2}g+2i : 1 \leqslant i \leqslant \tfrac{1}{2}g-1\big\}.$$

Since $h_2 - h_1 \equiv \delta_g \equiv \frac{1}{2}g \pmod{g}$, these labels cover every possibility modulo g. Similarly, it is easy to see that T covers every row and column of N.

It remains to show sufficiency when $e = g-1$ and g is odd. In this case we simply take T to consist of the cells

$$\big\{(r+h_1+1, c+h_2+1)\big\} \cup \big\{(r-i+1, c-g+i+1) : 1 \leqslant i \leqslant e\big\}.$$

The first of these has label $c-r+h_2-h_1 \equiv c-r \pmod{g}$, while the others have labels $\{c-r+2i : 1 \leqslant i \leqslant e\}$, which gives us a complete set. □

We remark that Lemma 6.5 can also be applied when the rows or columns are consecutive, by choosing $h_1 = 0$ or $h_2 = 0$, respectively.

7 Automorphisms with two nontrivial cycles

In this section we give necessary and sufficient conditions for membership in $\mathrm{Aut}(n)$ for those $\alpha \in S_n$ that consist of precisely two nontrivial cycles, of lengths d_1 and d_2.

Theorem 7.1 (Automorphisms with two nontrivial cycles)**.** *Suppose $\alpha \in S_n$ consists of a d_1-cycle, a d_2-cycle and d_∞ fixed points. If $d_1 = d_2$ then $\alpha \in \mathrm{Aut}(n)$ 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:*

(a) d_2 divides d_1,

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

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

Proof. The case $d_1 = d_2$ is resolved by Theorem 5.2, so assume $d_1 > d_2$. Suppose L is a Latin square with $\alpha \in \mathrm{Aut}(L)$. The block diagram of L must be as in Figure 1, as explained in Section 4.1. The necessity of conditions (b), (c) follows from Lemma 6.3. To see that (a) is necessary, observe that every symbol in M_{12} belongs to the d_1-cycle α_1. Then $d_1 = \mathrm{lcm}(d_1, d_1) = \mathrm{lcm}(d_1, d_2)$ by Lemma 3.6, so d_2 must divide d_1. (Note that we now have $n = d_1 + d_2 + d_\infty \leqslant d_1 + 2d_2 \leqslant 2d_1$, so $d_1 \geqslant \lceil \frac{1}{2}n \rceil$, as also demanded by Lemma 3.1.)

For the rest of the proof assume that conditions (a)–(c) hold. Our task is to find a Latin square L such that $\alpha \in \mathrm{Aut}(L)$. We construct such a square by means of a contour $\mathcal{C} = \mathcal{C}(i,j)$ that satisfies the conditions of Lemma 4.1 for the least possible d_∞. Examples with larger d_∞ can then be found using Lemma 6.1.

Case I: d_2 is odd. Here $d_\infty = 0$. First we specify the block M_{11}:

$$\mathcal{C}(i, t_2 - i - \mathcal{O}_{1,i}) = \begin{cases} t_1 & \text{if } 1 \leqslant i \leqslant d_1 - d_2, \\ t_2 & \text{if } d_1 - d_2 < i \leqslant d_1. \end{cases}$$

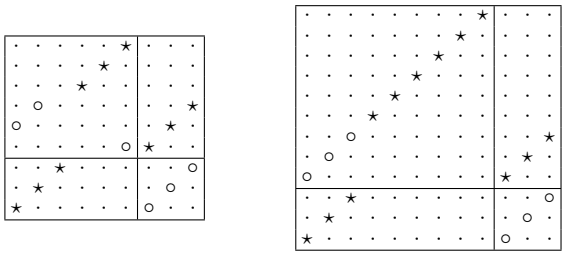


Figure 2: Contours for $d_1 = 6$, $d_2 = 3$, $d_\infty = 0$ and $d_1 = 9$, $d_2 = 3$, $d_\infty = 0$.

The block M_{22} can be completed by Lemma 6.3, and the blocks M_{12} and M_{21} can be completed by applying Lemma 6.5.

The contours for $d_1 = 6$, $d_2 = 3$, $d_\infty = 0$ and $d_1 = 9$, $d_2 = 3$, $d_\infty = 0$ are illustrated in Figure 2.

Case II: d_2 is even (and hence d_1 is also even). Here $d_\infty = 1$. We begin with M_{11}:

$$\mathcal{C}(i, t_2 - i - \mathcal{O}_{1,i}) = \begin{cases} t_1 & \text{if } 1 \leqslant i \leqslant \frac{1}{2}d_1 - d_2 \text{ or } \frac{1}{2}d_1 < i < d_1, \\ t_2 & \text{if } \frac{1}{2}d_1 - d_2 < i \leqslant \frac{1}{2}d_1, \\ n & \text{if } i = d_1. \end{cases}$$

The blocks M_{22}, $M_{2\infty}$, $M_{\infty 2}$ and $M_{\infty\infty}$ can be completed by Lemma 6.3. Once we complete $M_{12} \cup M_{21}$, we can complete L by Lemma 6.2. The block M_{21} can be completed using Lemma 6.5 with $e = g/2$.

Finally, we fill the block M_{12} with $\mathcal{C}(d_1, t_3 - 1) = t_1$, and if d_1/d_2 is even, we let

$$\begin{aligned} &\mathcal{C}(\tfrac{1}{2}d_1 - d_2 + i, t_3 - 1 - i) = t_1 && \text{for } 1 \leqslant i < \tfrac{1}{2}d_2 - 1, \\ &\mathcal{C}(\tfrac{1}{2}d_1 - \tfrac{1}{2}d_2 + i, t_2 + \tfrac{1}{2}d_2 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_2, \end{aligned}$$

while if d_1/d_2 is odd, we let

$$\begin{aligned} &\mathcal{C}(\tfrac{1}{2}d_1 - d_2 + i, t_2 + \tfrac{1}{2}d_2 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_2, \\ &\mathcal{C}(\tfrac{1}{2}d_1 - \tfrac{1}{2}d_2 + i, t_3 - 1 - i) = t_1 && \text{for } 1 \leqslant i < \tfrac{1}{2}d_2 - 1. \end{aligned}$$

These partial contours are illustrated in Figure 3 for $d_1 = 16$, $d_2 = 4$, $d_\infty = 1$, and $d_1 = 18$, $d_2 = 6$, $d_\infty = 1$. Focusing on the "missing" cell in the even pattern of the block M_{12} (shaded dark in Figure 3), it is not hard to see why the construction works. The shaded entry is in column $t_3 - 1$ when d_1/d_2 is even, and it is in column $t_3 - 1 - \frac{1}{2}d_2$ when d_1/d_2 is odd. □

8 Automorphisms with three nontrivial cycles

In this section we characterize automorphisms α of Latin squares with precisely three nontrivial cycles of lengths $d_1 \geqslant d_2 \geqslant d_3$.

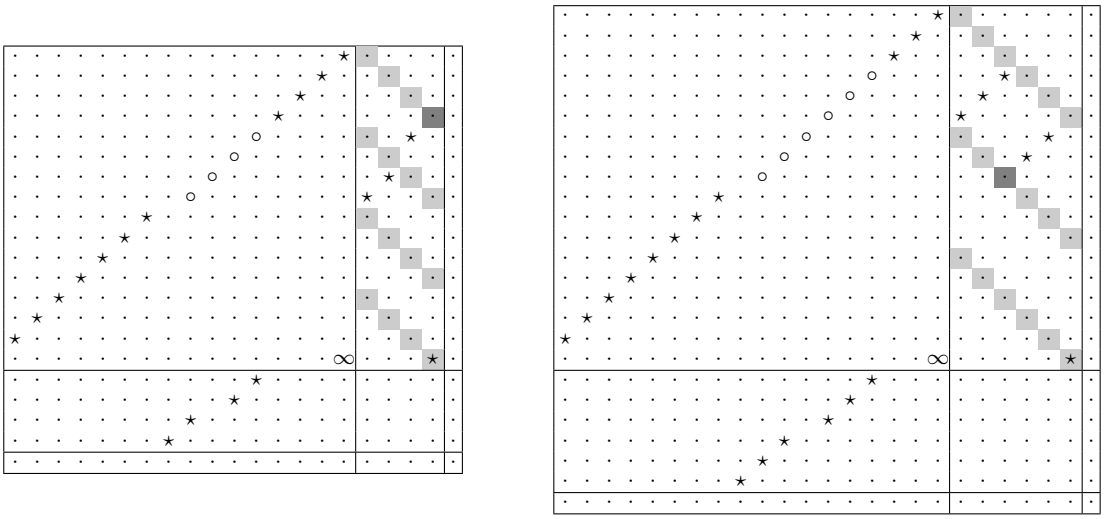


Figure 3: Partial contours for $d_1 = 16$, $d_2 = 4$, $d_\infty = 1$, and $d_1 = 18$, $d_2 = 6$, $d_\infty = 1$.

Theorem 8.1 (Automorphisms with three nontrivial cycles)**.** *Suppose that $\alpha \in S_n$ 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 $\alpha \in \mathrm{Aut}(n)$ if and only if one of the following cases holds:*

1. *$d_1 = d_2 = d_3$ and (a) $d_\infty \leqslant 3d_1$ and (b) if d_1 is even then $d_\infty \geqslant 1$,*
2. *$d_1 > d_2 = d_3$ 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 $d_\infty > 0$,*
3. *$d_1 = d_2 > d_3$ and (a) d_3 divides d_1, (b) $d_\infty \leqslant d_3$, and (c) if d_3 is even then $d_\infty > 0$,*
4. *$d_1 > d_2 > d_3$ and (a) $d_1 = \mathrm{lcm}(d_2, d_3)$, (b) $d_3 \geqslant d_\infty$, and (c) if d_1 is even then $d_\infty > 0$,*
5. *$d_1 > d_2 > d_3$ 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 $d_\infty > 0$.*

We will prove each case of Theorem 8.1 in a sequence of propositions in the remainder of this section. The case $d_1 = d_2 = d_3$ is covered by Theorem 5.2, so it remains to discuss the cases when $d_1 > d_2$ and/or $d_2 > d_3$.

8.1 The case $d_1 > d_2 = d_3$

Lemma 8.2. *For any d_1, d_2 such that $d_1 = 2d_2$, every isotopism with cycle structure (d_1, d_2^2, d_1) belongs to $\mathrm{Atp}(d_1)$.*

Proof. We specify a contour for a Latin square L of order d_1 that admits the autotopism

$$((1 \cdots d_1), (1 \cdots d_2)(d_2 + 1 \cdots d_1), (1 \cdots d_1))$$

by assigning $L(2i - 1, i) = L(2i, d_2 + i) = t_1$ for $1 \leqslant i \leqslant d_2$, as illustrated in Figure 4 when $d_1 = 6$. □

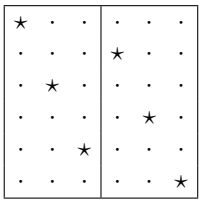


Figure 4: An example of the construction in the proof of Lemma 8.2.

Proposition 8.3 (Automorphisms with three nontrivial cycles of lengths $d_1 > d_2 = d_3$)**.** *Suppose that $\alpha \in S_n$ has precisely three nontrivial cycles of lengths $d_1 > d_2 = d_3$. Let d_∞ be the number of fixed points of α. Then $\alpha \in \mathrm{Aut}(n)$ if and only if all of the following conditions hold:*

(a) $d_1 \geqslant 2d_2 + d_\infty$,

(b) d_2 *divides* d_1,

(c) $d_\infty \leqslant 2d_2$,

(d) if d_2 *is even and* d_1/d_2 *is odd then* $d_\infty > 0$.

Proof. Let L be a Latin square such that $\alpha \in \mathrm{Aut}(L)$. By Lemma 6.3, $K = \bigcup_{i,j\in\{2,3,\infty\}} M_{ij}$ is a subsquare of L. Since $M_{i\infty} \cup M_{\infty i}$ can be filled later by Lemma 6.2, it suffices to consider only the blocks M_{11}, M_{12}, M_{13}, M_{21} and M_{31}. Figure 5 gives the part of a block diagram of L that concerns these blocks, with all entries being consequences of the fact that K is a subsquare of L. (Inside K, the block diagram of L is not uniquely determined by α, since $d_2 = d_3$.)

	α_1	α_2	α_3	α_∞
α_1	$\alpha_1 : d_1 - 2d_2 - d_\infty$ $\alpha_2 : d_1$ $\alpha_3 : d_1$ $\alpha_\infty : d_1$	$\alpha_1 : d_2$	$\alpha_1 : d_2$	$\alpha_1 : d_\infty$
α_2	$\alpha_1 : d_2$			
α_3	$\alpha_1 : d_2$			
α_∞	$\alpha_1 : d_\infty$			

Figure 5: Part of the block diagram of L with $d_1 > d_2 = d_3$.

By Theorem 5.2, the subsquare K can be filled provided (c) holds. From the M_{11} block of L we deduce (a) and (b). To prove that (d) is necessary, suppose that d_2 is even, d_1/d_2 is odd and $d_\infty = 0$. Let k be the largest odd divisor of d_1. Then α^k consists of an odd number of cycles of the even length d_1/k, contradicting Theorem 5.2.

For the sufficiency, assume that conditions (a)–(d) are satisfied, and let us construct a partial contour for $L \setminus K$.

Case I: $d_\infty > 0$ or d_1 is odd. Then we set

$$\begin{aligned} \mathcal{C}(i, t_2 - i - \mathcal{O}_{1,i}) &= t_2 && \text{for } \tfrac{1}{2}d_1 - d_2 + 1 \leqslant i \leqslant \tfrac{1}{2}d_1, \\ \mathcal{C}(i, t_2 - i - \mathcal{O}_{1,i}) &= t_3 && \text{for } \tfrac{1}{2}d_1 + 1 \leqslant i \leqslant \tfrac{1}{2}d_1 + d_3, \end{aligned}$$

and fill the remaining cells in $D = \{(i, t_2 - i - \mathcal{O}_{1,i});\ 1 \leqslant i \leqslant d_1\}$ with the symbol t_1 and fixed points, making sure that a fixed point appears in the last row when d_1 is even, so that the column d_1 does not contain two symbols t_1.

Note that there are at least $2d_2$ consecutive rows and columns in D not occupied by the leading symbol t_1. We can therefore fill $M_{12} \cup M_{13}$ with the pattern of Lemma 8.2, and $M_{21} \cup M_{31}$ with the transposed pattern of Lemma 8.2. A partial contour for $L \setminus K$ in the case $d_1 = 6$, $d_2 = d_3 = 2$, $d_\infty = 1$ can be found in Figure 6.

Case II: $d_\infty = 0$ and d_1 is even. If d_2 is odd then it divides $d_1/2$. If d_2 is even then d_1/d_2 is even by (d), so d_2 divides $d_1/2$ again. We can modify the partial contour from Case I as follows:

In M_{11}, we swap the symbols of the partial contour in rows d_1 and $d_1/2+d_3$ (the bottom-most occurrence of t_3), to prevent column d_1 from containing two copies of symbol t_1. Since there are still $2d_2$ consecutive columns in D not occupied by t_1, we can fill $M_{21} \cup M_{31}$ as above. We also leave M_{12} intact, but in M_{13} we move the bottom-most symbol t_1 in the partial contour down to row d_1, i.e., by $d_1/2 - d_3$ rows. Because $d_1/2 - d_3$ is a multiple of d_3, Lemma 4.1 is satisfied after these changes.

A partial contour for $L \setminus K$ in the case $d_1 = 12$, $d_2 = d_3 = 3$, $d_\infty = 0$ can be found in Figure 6, with the changes introduced in Case II highlighted. □

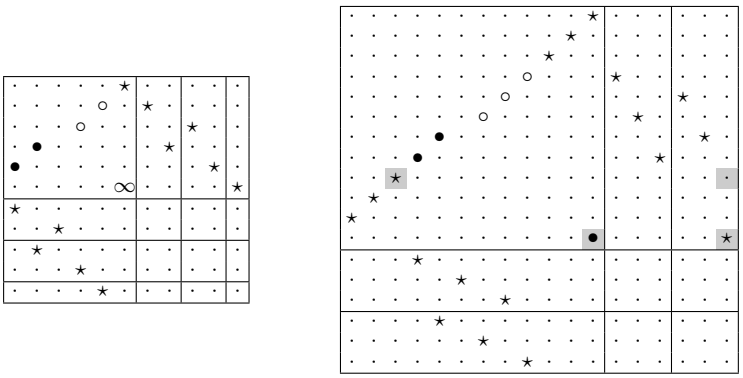


Figure 6: Partial contours for $d_1 = 6$, $d_2 = d_3 = 2$, $d_\infty = 1$, and $d_1 = 12$, $d_2 = d_3 = 3$, $d_\infty = 0$.

8.2 The case $d_1 = d_2 > d_3$

Proposition 8.4 (Automorphisms with three nontrivial cycles of lengths $d_1 = d_2 > d_3$)**.** *Suppose that $\alpha \in S_n$ has precisely three nontrivial cycles of lengths $d_1 = d_2 > d_3$. Let d_∞ be the number of fixed points of α. Then $\alpha \in \mathrm{Aut}(n)$ if and only if all of the following conditions hold:*

(a) d_3 *divides* d_1,

(b) $d_\infty \leqslant d_3$,

(c) if d_3 *is even then* $d_\infty > 0$.

Proof. Let L be a Latin square such that $\alpha \in \mathrm{Aut}(L)$. Lemma 6.3 implies that $K = \bigcup_{i,j\in\{3,\infty\}} M_{ij}$ is a subsquare of L and that conditions (b) and (c) must hold. Theorem 3.7 implies that $\alpha^{d_1} = \mathrm{id}$, otherwise L contains a subsquare of order $2d_1 + d_\infty > \frac{1}{2}n$, contradicting Lemma 3.1. Hence d_3 must divide d_1, which is condition (a).

For the sufficiency, assume that conditions (a)–(c) hold. Again, we need only find a partial contour for $L \setminus K$.

Case I: d_3 is odd. Theorem 7.1 implies that $\beta \in \mathrm{Aut}(n)$, where β has the cycle structure $(2d_1)\cdot d_3 \cdot 1^{d_\infty}$. Since $\beta^2 \in \mathrm{Aut}(n)$ has the same cycle structure as α, we have $\alpha \in \mathrm{Aut}(n)$ by Lemma 2.1.

Case II: d_3 is even. We will construct a partial contour satisfying the conditions of Lemma 4.1 for the case when $d_\infty = 1$. Examples with larger d_∞ can then be found using Lemma 6.1.

We first define the partial contour for $M_{11} \cup M_{12} \cup M_{21} \cup M_{22}$.

$$
\begin{aligned}
&\mathcal{C}(\tfrac{1}{2}d_1 + 1, \tfrac{1}{2}d_1) = n, && \\
&\mathcal{C}(\tfrac{1}{2}d_1 + 1 + i, \tfrac{1}{2}d_1 - i) = t_2 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1 - 1, \\
&\mathcal{C}(\tfrac{1}{2}d_1 + i, \tfrac{1}{2}d_1 - i + 2) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1, \\
&\mathcal{C}(i, 2d_1 - i) = t_2 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1, \\
&\mathcal{C}(i, t_3 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1 - d_3, \\
&\mathcal{C}(\tfrac{1}{2}d_1 - d_3 + i, t_3 - \tfrac{1}{2}d_1 + d_3 - i) = t_3 && \text{for } 1 \leqslant i \leqslant d_3, \\
&\mathcal{C}(t_2, 1) = t_1, && \\
&\mathcal{C}(d_1 + i, t_2 - i) = t_2 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1 - d_3, \\
&\mathcal{C}(\tfrac{3}{2}d_1 - d_3 + i, \tfrac{1}{2}d_1 + d_3 - i + 1) = t_3 && \text{for } 1 \leqslant i \leqslant d_3, \\
&\mathcal{C}(t_2 + i, t_2 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1 - 1, \\
&\mathcal{C}(\tfrac{3}{2}d_1 + 1, \tfrac{3}{2}d_1) = n, && \\
&\mathcal{C}(\tfrac{3}{2}d_1 + i, \tfrac{3}{2}d_1 - i) = t_2 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1 - 1, \\
&\mathcal{C}(\tfrac{3}{2}d_1 + 1 + i, \tfrac{3}{2}d_1 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_1 - 1, \\
&\mathcal{C}(2d_1, 2d_1) = t_2. &&
\end{aligned}
$$

We can now fill M_{31} using Lemma 6.5, with $e = \frac{1}{2}g$ and symbol t_2, and also M_{32} with symbol t_1. In blocks $M_{13} \cup M_{23}$ we use similar cells (transposed), but we use both leading

symbols t_2, t_3 in both blocks as follows:

$$\begin{aligned}
&\mathcal{C}(\tfrac{1}{2}d_1 - d_3 + i, n - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_3,\\
&\mathcal{C}(\tfrac{1}{2}d_1 - \tfrac{1}{2}d_3 + i + 1, n - \tfrac{1}{2}d_3 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_3 - 1,\\
&\mathcal{C}(\tfrac{1}{2}d_1 + 1, t_3) = t_2,\\
&\mathcal{C}(\tfrac{3}{2}d_1 - d_3 + i, n - i) = t_2 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_3,\\
&\mathcal{C}(\tfrac{3}{2}d_1 - \tfrac{1}{2}d_3 + i + 1, n - \tfrac{1}{2}d_3 - i) = t_2 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_3 - 1,\\
&\mathcal{C}(\tfrac{3}{2}d_1 + 1, t_3) = t_1.
\end{aligned}$$

The blocks $M_{1\infty} \cup M_{2\infty} \cup M_{\infty 1} \cup M_{\infty 2}$ can be filled using Lemma 6.2. The construction (with the partial contour of $L \setminus K$) is illustrated in Figure 7 for $d_1 = d_2 = 12$, $d_3 = 4$ and $d_\infty = 1$. □

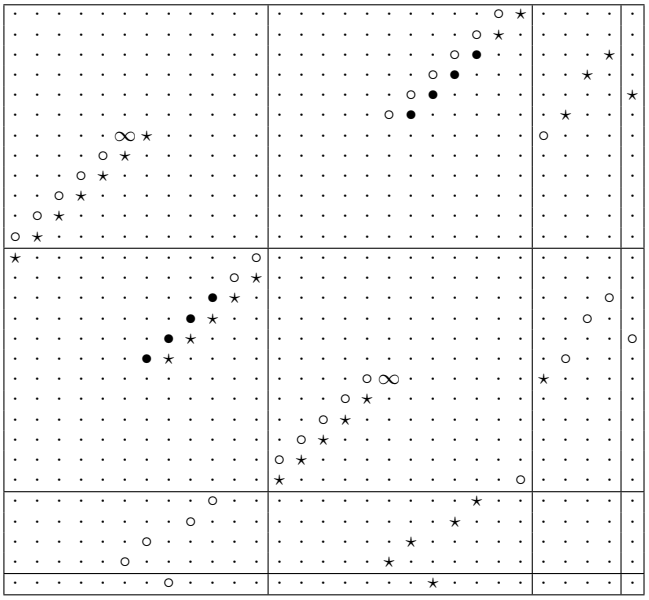


Figure 7: A partial contour for $d_1 = d_2 = 12$, $d_3 = 4$ and $d_\infty = 1$.

8.3 The case $d_1 > d_2 > d_3$

The case of three distinct cycle lengths splits into two, depending on whether or not d_3 divides d_2.

Proposition 8.5. *Suppose that $\alpha \in S_n$ has precisely three nontrivial cycles of lengths $d_1 > d_2 > d_3$ where d_3 does not divide d_2. Let d_∞ be the number of fixed points of α. Then $\alpha \in \mathrm{Aut}(n)$ if and only if (a) $d_1 = \mathrm{lcm}(d_2, d_3)$, (b) $d_3 \geqslant d_\infty$, and (c) if d_1 is even then $d_\infty > 0$.*

Proof. Let L be a Latin square such that $\alpha \in \mathrm{Aut}(L)$. For $i \in \{1, 2, 3\}$, blocks $M_{i\infty}$ and $M_{\infty i}$ can be constructed using Lemma 6.2. Also $M_{22} \cup M_{2\infty} \cup M_{\infty 2} \cup M_{33} \cup M_{3\infty} \cup M_{\infty 3} \cup M_{\infty\infty}$ can

be constructed using Lemma 6.3, assuming (b). Lemma 3.6 implies that only symbols from α_1 can appear in M_{23} and M_{32}, since d_3 does not divide d_2. Combining this information, and the constraints from the definition of a Latin square shows that the block diagram of L must be as in Figure 8.

	α_1	α_2	α_3	α_∞
α_1	$\alpha_1 : d_1 - d_2 - d_3 + 2g - d_\infty$ $\alpha_2 : d_1 - d_3$ $\alpha_3 : d_1 - d_2$ $\alpha_\infty : d_1$	$\alpha_1 : d_2 - g$ $\alpha_3 : d_2$	$\alpha_1 : d_3 - g$ $\alpha_2 : d_3$	$\alpha_1 : d_\infty$
α_2	$\alpha_1 : d_2 - g$ $\alpha_3 : d_2$	$\alpha_2 : d_2 - d_\infty$ $\alpha_\infty : d_2$	$\alpha_1 : g$	$\alpha_2 : d_\infty$
α_3	$\alpha_1 : d_3 - g$ $\alpha_2 : d_3$	$\alpha_1 : g$	$\alpha_3 : d_3 - d_\infty$ $\alpha_\infty : d_3$	$\alpha_3 : d_\infty$
α_∞	$\alpha_1 : d_\infty$	$\alpha_2 : d_\infty$	$\alpha_3 : d_\infty$	$\alpha_\infty : d_\infty$

Figure 8: Block diagram of L with $d_1 > d_2 > d_3$ the only nontrivial cycle lengths, d_3 does not divide d_2, and $g = d_2 d_3/d_1 = \gcd(d_2, d_3)$.

Applying Lemma 3.6 to M_{23} implies $\operatorname{lcm}(d_1, d_2, d_3) = \operatorname{lcm}(d_2, d_3)$ and so d_1 divides $\operatorname{lcm}(d_2, d_3)$. Applying Lemma 3.6 to M_{11} implies $d_1 = \operatorname{lcm}(d_1, d_1) = \operatorname{lcm}(d_1, d_2)$, and similarly $d_1 = \operatorname{lcm}(d_1, d_3)$. Hence d_2 and d_3 both divide d_1. Therefore $d_1 = \operatorname{lcm}(d_2, d_3)$, which is condition (a), and $g = \gcd(d_2, d_3) = d_2 d_3/d_1$. Given (a), we see that d_1 is even precisely when at least one of d_2, d_3 is even. Lemma 6.3(ii) then shows the necessity of conditions (b) and (c).

To prove sufficiency, we will give constructions of contours for the case when $d_\infty = 1$ and d_1 is even, and also when $d_\infty = 0$ and d_1 is odd. Examples with larger d_∞ can then be found using Lemma 6.1.

By Figure 8, each symbol from α_2 occurs $d_1 - d_3$ times in the block M_{11}. Note that $(d_1 - d_3)/(\operatorname{lcm}(d_1, d_2)/d_2) = (d_1 - d_3)/(d_1/d_2) = d_2 - g$. We therefore need to place $d_2 - g$ leading entries t_2 into M_{11}. Similarly, we need to place $d_3 - g$ leading entries t_3 into M_{11}.

It will be of importance in some contours to place these entries t_2 and t_3 into at most $d_1/2$ consecutive rows and columns of M_{11}. We claim that this can be done, because $\frac{1}{2}d_1 \geqslant (d_2 - g) + (d_3 - g)$. Indeed, if $d_1 = abg$, $d_2 = ag$ and $d_3 = bg$, the inequality is equivalent to $\frac{1}{2}ab = \frac{1}{2}(a-2)(b-2) + a + b - 2 \geqslant a + b - 2$, which holds since $a > b \geqslant 2$.

It is convenient to consider four cases. The cases (i)–(iii) will be handled with the same contour (up to the usual parity offsets) but they will require separate explanations. The case (iv) will require a slightly different contour. The cases are:

(i) d_1, d_2, d_3 and g are all odd, $d_\infty = 0$,

(ii) d_1 is even, precisely one of d_2 and d_3 is even, g is odd and $d_\infty = 1$,

(iii) d_1, $d_2 = ag$, $d_3 = bg$ and g are all even, $d_\infty = 1$ and $a - b$ is odd,

(iv) d_1, $d_2 = ag$, $d_3 = bg$ and g are all even, $d_\infty = 1$ and $a - b$ is even.

Cases (i)–(iii): To fill M_{11}, for $1 \leqslant i \leqslant d_1$, let

$$\mathcal{C}(i, t_2 - i - \mathcal{O}_{1,i}) = \begin{cases} t_2 & \text{for } 1 \leqslant i \leqslant d_2 - g, \\ t_3 & \text{for } d_2 - g < i \leqslant d_2 + d_3 - 2g, \\ n & \text{for } i = d_1 \text{ if } d_1 \text{ is even}, \\ t_1 & \text{otherwise.} \end{cases}$$

In addition to $\mathcal{O}_{1,i}$, define also offsets $\mathcal{O}_{j,i}$ for $j \in \{2, 3\}$ by

$$\mathcal{O}_{j,i} = \begin{cases} 1 & \text{if } d_j \text{ is even and } g < i \leqslant g + \frac{1}{2}d_j, \\ 0 & \text{otherwise.} \end{cases}$$

To fill $M_{12} \cup M_{21}$, for $1 \leqslant i \leqslant d_2$, let

$$\mathcal{C}(d_2 + 1 - i, d_1 + i - \mathcal{O}_{2,i}) = \mathcal{C}(t_3 - i + \mathcal{O}_{2,i}, d_1 - d_2 + i) = \begin{cases} t_3 & \text{if } g < i \leqslant 2g, \\ t_1 & \text{otherwise.} \end{cases}$$

To fill $M_{13} \cup M_{31}$, for $1 \leqslant i \leqslant d_3$, let

$$\mathcal{C}(d_2 - 2g + i, t_4 - i + \mathcal{O}_{3,i}) = \mathcal{C}(t_3 - 1 + i - \mathcal{O}_{3,i}, d_1 - d_2 + 2g + 1 - i) = \begin{cases} t_2 & \text{if } g < i \leqslant 2g, \\ t_1 & \text{otherwise.} \end{cases}$$

This partial contour is illustrated in Figure 9 with $d_1 = 15$, $d_2 = 5$, $d_3 = 3$ for case (i), and in Figure 10 with $d_1 = 24$, $d_2 = 8$, $d_3 = 6$ for case (iii).

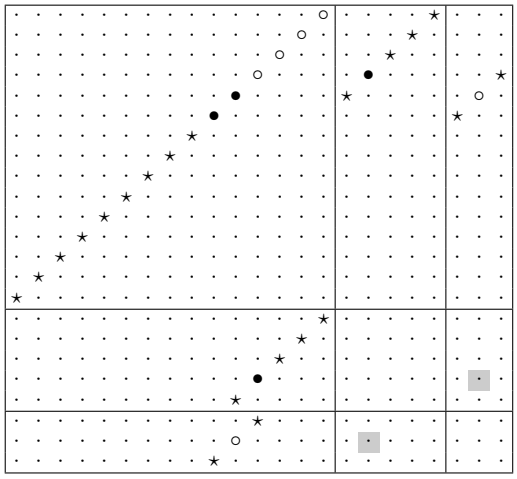


Figure 9: A partial contour for $d_1 = 15$, $d_2 = 5$, $d_3 = 3$, $d_\infty = 0$.

We claim that blocks M_{23} and M_{32} can now be completed by Lemma 6.5. Let N_{23} be the $g \times g$ submatrix of M_{23} formed by the rows of M_{21} not containing the leading symbol t_1, and by the columns of M_{13} not containing the leading symbol t_1. Define similarly the $g \times g$ submatrix N_{32} of M_{32}. These two submatrices are shaded gray in Figures 9 and 10.

In case (i), N_{23} and N_{32} consist of g consecutive rows and columns. We can represent this situation with parameters $e = g - 1$, $h_1 = 0$, $h_2 = 0$, as explained after Lemma 6.5. Since g is odd, Lemma 6.4 implies that $\delta_g \equiv 0 \pmod{g}$, and (6.2) becomes $(h_1 - h_2)(g-1) \equiv 0 \pmod{g}$, which is obviously satisfied.

In case (ii), let us first assume that d_2 is odd and d_3 is even. The submatrix N_{23} can be represented with parameters $e = g - 1$, $h_1 = 0$ (because d_2 is odd and there are no offsets) and $h_2 = d_3/2 - g$. Since g is odd, we again need $(h_1 - h_2)(g-1) \equiv 0 \pmod{g}$, which becomes $d_3/2 \equiv 0 \pmod{g}$, or $bg/2 \equiv 0 \pmod{g}$, which is equivalent to b being even. This is true, since g is odd and $d_3 = bg$ is even. Similarly for the submatrix N_{32}. The case d_2 even, d_3 odd is analogous.

In case (iii), the submatrix N_{23} can be represented with parameters $e = g - 1$, $h_1 = d_2/2 - g$, $h_2 = d_3/2 - g$. Since g is even, equation (6.2) becomes $(h_1 - h_2)e \equiv g/2 \pmod{g}$ by Lemma 6.4, i.e., $(d_2/2 - d_3/2) \equiv g/2 \pmod{g}$. This holds precisely when $a - b$ is odd, which is one of the assumptions of case (iii). Similarly for N_{32}.

In all cases (i)–(iii), the remaining blocks can be filled in using Lemmas 6.2 and 6.3.

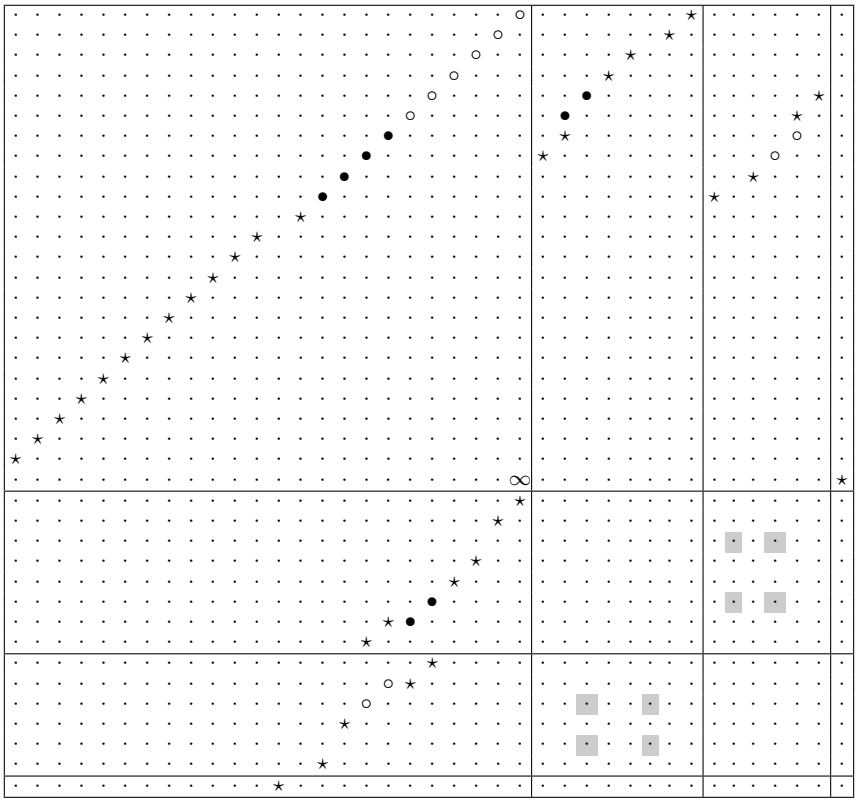


Figure 10: A partial contour for $d_1 = 24$, $d_2 = 8$, $d_3 = 6$, $d_\infty = 1$.

Case (iv). Since $a - b$ is even and $\gcd(a, b) = 1$, both a and b are odd. In particular, $d_1/d_3 = a$ is odd, and $d_1/2$ is an odd multiple of $d_3/2$.

The construction (illustrated for $d_1 = 30$, $d_2 = 10$, $d_3 = 6$ and $d_\infty = 1$ in Figure 11), is similar to the one above, but with several modifications, which we describe in words. First, we move the leading symbols (but not the selected cells) in M_{11} so that the break in the

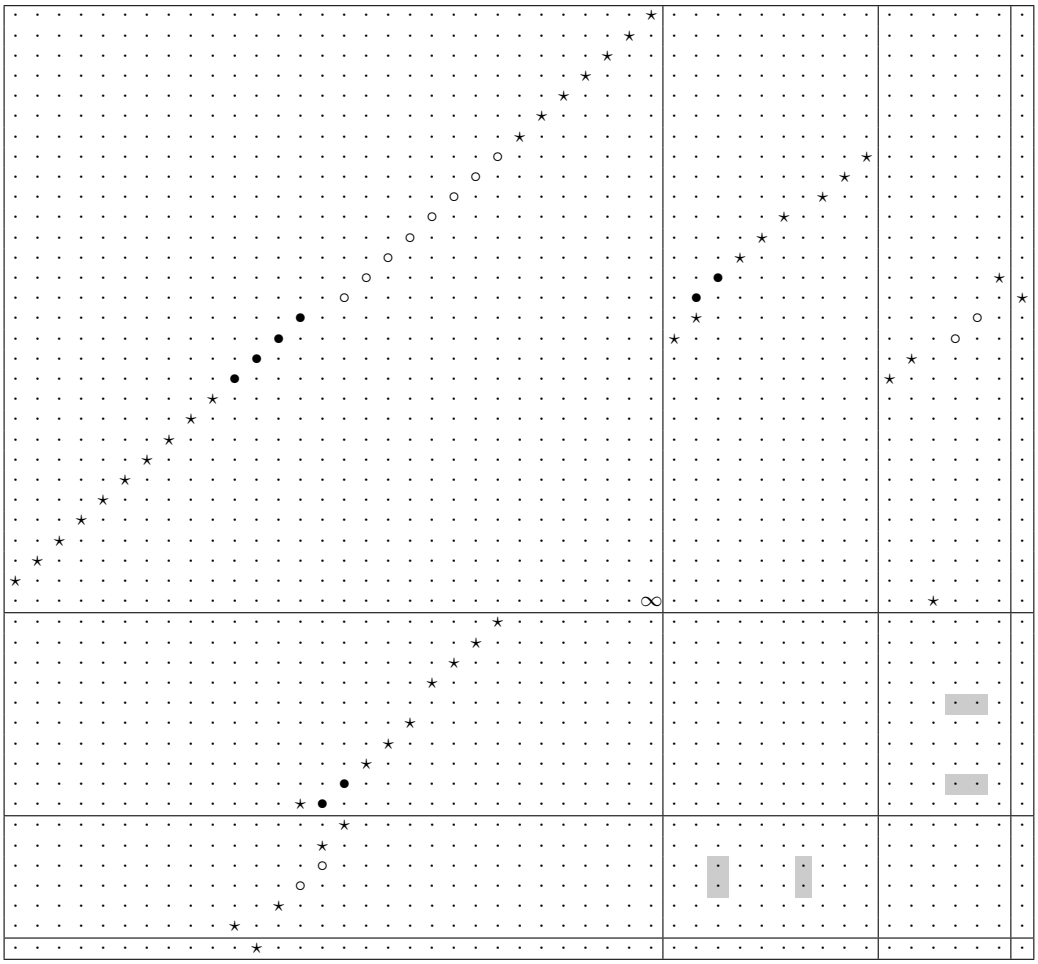


Figure 11: A partial contour for $d_1 = 30$, $d_2 = 10$, $d_3 = 6$, $d_\infty = 1$.

diagonal occurs precisely between the leading symbols t_2 and t_3. We fill M_{12} as above, with the appropriate vertical shift (which we will not mention any more). We fill M_{21} as above, except that we shift the pattern down and left by one—this is possible since we have an extra column to work with, the break between symbols t_2 and t_3 in M_{11}. The block M_{31} is filled with the pattern from M_{13} above, making sure that the leading symbols t_2 in M_{11} and M_{13} occupy consecutive columns. Finally, the block M_{13} is filled as above, except that the entry for $i = g$ is first moved down and to the left by $d_3/2$ (landing in row $d_1/2 + d_3/2$), and then further down to row d_1—since, as explained above, $d_1/2$ is an odd multiple of $d_3/2$, the last vertical move is a multiple of d_3 and will therefore not produce a clash with Lemma 4.1.

Define the submatrices N_{23} and N_{32} as above. Then N_{23} can be represented by the parameters $e = g - 1$, $h_1 = d_2/2 - g$, $h_2 = 0$. Equation (6.2) becomes $d_2/2 \equiv g/2 \pmod{g}$, which holds because a is odd. Similarly for N_{32}. The remaining blocks can be filled in using Lemmas 6.2 and 6.3. □

Finally, we treat the case of three distinct cycles when d_3 divides d_2.

Proposition 8.6. *Suppose that $\alpha \in S_n$ has precisely three nontrivial cycles of lengths $d_1 > d_2 > d_3$ where d_3 divides d_2. Let d_∞ be the number of fixed points of α. Then $\alpha \in \mathrm{Aut}(n)$ if and only if (a) d_2 divides d_1, (b) $d_3 \geqslant d_\infty$, and (c) if d_3 is even then $d_\infty > 0$.*

Proof. We claim that the block diagram of L must be as in Figure 12. The blocks $M_{i\infty}$ and $M_{\infty i}$, for $1 \leqslant i \leqslant 3$, are forced by Lemma 6.2. Let $K = \bigcup_{i,j>1} M_{ij}$. Theorem 3.7, with Λ as the set of divisors of d_2, implies K is a subsquare that obeys Theorem 7.1. In particular, its block diagram mirrors Figure 1. It is then easy to complete the rest of the diagram in Figure 12.

	α_1	α_2	α_3	α_∞
α_1	$\alpha_1 : d_1 - d_2 - d_3 - d_\infty$ $\alpha_2 : d_1$ $\alpha_3 : d_1$ $\alpha_\infty : d_1$	$\alpha_1 : d_2$	$\alpha_1 : d_3$	$\alpha_1 : d_\infty$
α_2	$\alpha_1 : d_2$	$\alpha_2 : d_2 - d_3 - d_\infty$ $\alpha_3 : d_2$ $\alpha_\infty : d_2$	$\alpha_2 : d_3$	$\alpha_2 : d_\infty$
α_3	$\alpha_1 : d_3$	$\alpha_2 : d_3$	$\alpha_3 : d_3 - d_\infty$ $\alpha_\infty : d_3$	$\alpha_3 : d_\infty$
α_∞	$\alpha_1 : d_\infty$	$\alpha_2 : d_\infty$	$\alpha_3 : d_\infty$	$\alpha_\infty : d_\infty$

Figure 12: Block diagram of L with $d_1 > d_2 > d_3$ the only nontrivial cycle lengths, where d_3 divides d_2.

A consequence of α_1 appearing in M_{21} in the block diagram of L, is that d_2 divides d_1, establishing (a). Since K is a subsquare, (b) and (c) follow from Theorem 7.1.

Conversely, if (a)–(c) hold then the subsquare K can be constructed by Theorem 7.1. It thus suffices to provide a partial contour for $L \setminus K$. As usual, employing Lemma 6.1, we may assume that $d_\infty = 1$ if d_3 is even and $d_\infty = 0$ if d_3 is odd.

We define D and the partial contour for the block M_{11} exactly as we did in Proposition 8.3.

Case I: d_3 is even (and $d_\infty = 1$). Then d_1, d_2, d_3 are all even. There are $d_2 + d_3 + 1$ consecutive columns in D that do not contain t_1. Utilizing these columns, we place an even pattern filled with symbols t_1 into M_{21} (occupying $d_2 + 1$ columns), and "wrap around it" an even pattern filled with symbols t_1 in M_{31}. Specifically, we define

$$\begin{aligned}
&\mathcal{C}(d_1 + i, \tfrac{1}{2}d_1 + d_2 - \tfrac{1}{2}d_3 + 1 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_2,\\
&\mathcal{C}(d_1 + i, \tfrac{1}{2}d_1 + d_2 - \tfrac{1}{2}d_3 - i) = t_1 && \text{for } \tfrac{1}{2}d_2 < i \leqslant d_2,\\
&\mathcal{C}(d_1 + d_2 + i, \tfrac{1}{2}d_1 + d_2 + 1 - i) = t_1 && \text{for } 1 \leqslant i \leqslant \tfrac{1}{2}d_3,\\
&\mathcal{C}(d_1 + d_2 + i, \tfrac{1}{2}d_1 - i) = t_1 && \text{for } \tfrac{1}{2}d_3 < i \leqslant d_3.
\end{aligned} \tag{8.1}$$

See Figure 13 for examples. This wrap-around construction works here because the gap in the even pattern in M_{31} has size $d_2 + 1 \equiv 1 \pmod{d_3}$.

Since there are only $d_2 + d_3$ consecutive rows without symbols t_1 in D, we will use a modified wrap-around construction in $M_{12} \cup M_{13}$. Namely, we transpose the partial contour in (8.1) and slide it vertically so that only the top symbol t_1 in M_{13} collides with M_{11}. If

d_3 divides $d_2/2$, we move this colliding symbol down to row d_1, i.e., by $d_2 + d_1/2$ rows, a multiple of d_3. If d_3 does not divide $d_2/2$, we have $d_2 = (2k+1)d_3$ for some k, and we move the colliding symbol down to the row corresponding to the gap in the even pattern in M_{12}, i.e., by $d_2/2 + d_3/2 = (k+1)d_3$ rows, again a multiple of d_3. Figure 13 illustrates both possibilities, with the moved colliding symbol highlighted.

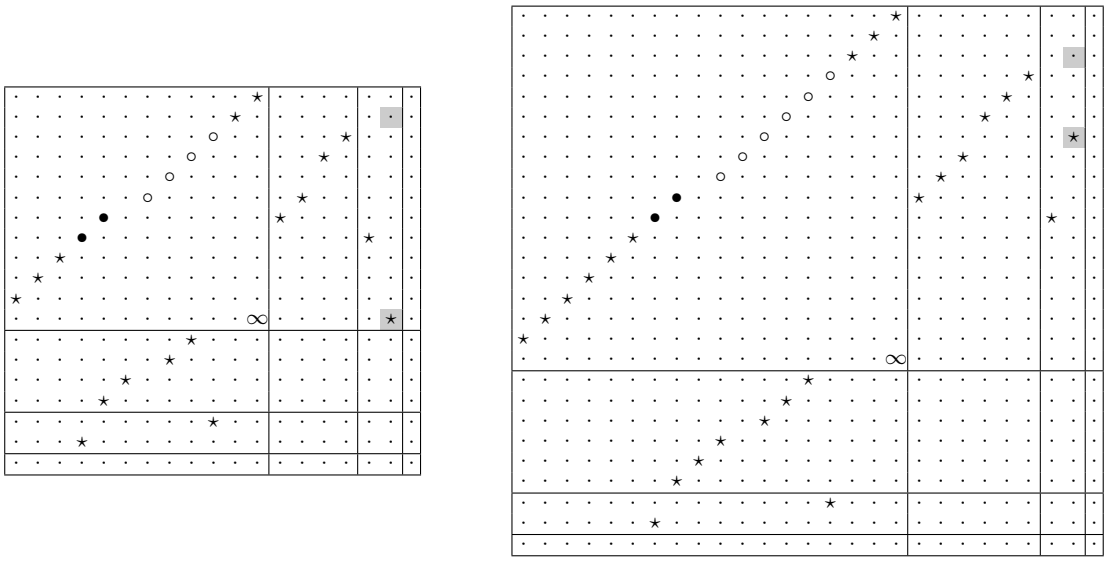


Figure 13: Partial contours for $d_1 = 12$, $d_2 = 4$, $d_3 = 2$, $d_\infty = 1$, and $d_1 = 18$, $d_2 = 6$, $d_3 = 2$, $d_\infty = 1$.

Case II: d_3 is odd (and $d_\infty = 0$). If d_1 is odd, it is straightforward to align odd patterns in $M_{21} \cup M_{31}$ and $M_{12} \cup M_{13}$ with, respectively, the columns and rows of D that do not contain t_1. We can therefore assume that d_1 is even.

For now, assume d_2 is even; an example of a partial contour in this case is given in Figure 14. Then d_3 divides $d_2/2$. We place an even pattern into the $d_2 + 1$ right-most available columns of M_{21}, and we position an odd pattern immediately to the left of it in M_{31}. Since there are now only $d_2 + d_3$ columns without t_1 in D, the left-most symbol in the partial contour of M_{31} collides with M_{11}, and we move it to the column corresponding to the break in the even pattern of M_{21}, i.e., by $d_3 + d_2/2$ columns, a multiple of d_3. Now we place an even pattern into the $d_2 + 1$ top-most available rows of M_{12}, and we position an odd pattern into M_{13} so that the top symbol t_1 in M_{13} collides with the bottom symbol t_1 in M_{12}. This colliding element can be moved into the row corresponding to the gap in the even pattern in M_{12}, i.e., by $d_2/2$ rows, a multiple of d_3. However, the bottom symbol t_1 in M_{13} still collides with M_{11}, and we move it to row d_1, i.e., by $d_1/2 - d_3$ rows, a multiple of d_3.

Finally, suppose that d_2 is odd. Since we can place odd patterns into M_{12}, M_{13}, M_{21}, M_{31}, the blocks $M_{21} \cup M_{31}$ can be filled easily, with $d_2 + d_3$ columns of D at our disposal. Place the odd pattern in M_{12} as high as possible, and the odd pattern in M_{13} immediately below it, so that only the bottom symbol t_1 in M_{13} collides with M_{11}. This colliding element can again be moved to row d_1, i.e., by $d_1/2 - d_3$ rows, a multiple of d_3. □

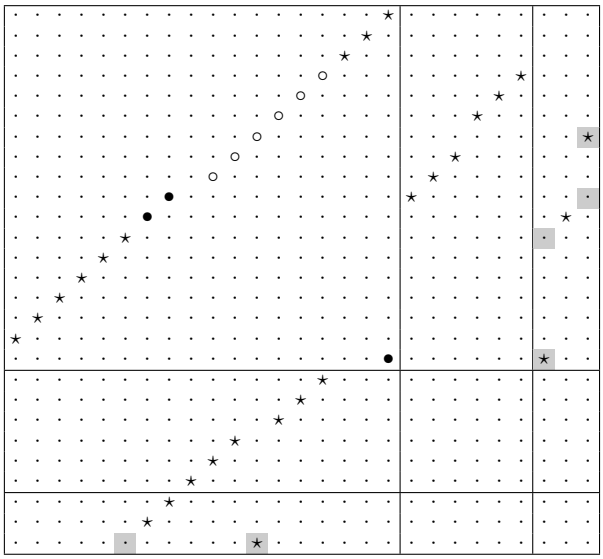


Figure 14: Partial contour for $d_1 = 18$, $d_2 = 6$, $d_3 = 3$, $d_\infty = 0$.

9 Autotopisms of small Latin squares

Falcón [17] identified $\mathrm{Atp}(n)$ for $n \leqslant 11$. The elements of $\mathrm{Atp}(n)$ for $n \leqslant 17$ are given in Appendix A. A representative Latin square that admits each claimed autotopism is given at [51], along with the `GAP` code [21] used in this project.

In [17], Falcón listed six isotopisms θ, that are not equivalent in the sense of Lemma 2.1, for which he proved computationally that $\theta \notin \mathrm{Atp}(n)$ but no theoretical reason was known. Five of these cases are resolved theoretically by Corollary 5.3. The remaining case has cycle structure $(4{\cdot}2, 4{\cdot}2, 4{\cdot}1^2)$. It is simple to check by hand that such an autotopism is not possible, although for reasons that seem peculiar to this example. Applying Theorem 3.7 we see that there is also no autotopism in $\mathrm{Atp}(14)$ with cycle structure $(8{\cdot}4{\cdot}2, 8{\cdot}4{\cdot}2, 8{\cdot}4{\cdot}1^2)$. We also observe that the example after Lemma 3.8 shows that there is no automorphism in $\mathrm{Aut}(17)$ with cycle structure $6{\cdot}3{\cdot}2^4$.

With the exception of the special cases just discussed, every isotopism $\theta \in \mathcal{I}_n$ for $n \leqslant 17$ either belongs to $\mathrm{Atp}(n)$ or can be shown to have $\theta \notin \mathrm{Atp}(n)$ using Lemma 3.6, Theorem 3.7 or Corollary 5.3.

10 Concluding remarks

We conclude this paper with some future research ideas. While it is known that the probability that a random Latin square admits a nontrivial autotopism is asymptotically zero [37], we propose the following conjecture.

Conjecture 10.1. *For $n > 0$ let $\mathbb{P}(n)$ be the probability that a randomly chosen $\alpha \in S_n$ is a component of some isotopism $(\alpha, \beta, \gamma) \in \mathrm{Atp}(n)$. Then $\lim_{n\to\infty} \mathbb{P}(n) = 0$.*

Motivated by the results of Falcón [17], we have verified computationally that the following question has an affirmative answer for all primes $p \leqslant 23$.

Problem 10.2. *Let $\theta = (\alpha,\ \beta,\ \gamma) \in \mathrm{Atp}(p)$ for some prime p. Must it be true that either θ is equivalent to $(\delta,\ \delta,\ \mathrm{id})$ where δ is a p-cycle, or that α, β and γ all have the same cycle structure?*

Horoševskiĭ proved [23, Theorem 2] that if G is a group of order $n > 1$ and φ is an automorphism of G then the order of φ cannot exceed $n-1$. Motivated by [23] and by our computational results, we ask:

Problem 10.3. *Suppose θ is an autotopism of a Latin square L of order n. Is the order of θ at most n?*

Acknowledgements

The authors are grateful to Chris Mears, who provided some assistance in finding Latin squares with a specified autotopism (see [32]), and to Michael Kinyon, who helped with the review of the loop-theoretical literature concerned with autotopisms. The authors are also grateful to the referees for their diligence and their useful feedback.

References

[1] R. H. Bruck, A Survey of Binary Systems, Springer, Berlin, 1971.

[2] R. H. Bruck and L. J. Paige, Loops whose inner mappings are automorphisms, *Ann. of Math.* (2) **63** (1956), 308–323.

[3] J. Browning, D. S. Stones and I. M. Wanless, Bounds on the number of autotopisms and subsquares of a Latin square. Submitted.

[4] J. Browning, P. Vojtěchovský and I. M. Wanless, Overlapping Latin subsquares and full products, *Comment. Math. Univ. Carolin.* **51** (2010), 175–184.

[5] D. Bryant, M. Buchanan and I. M. Wanless, The spectrum for quasigroups with cyclic automorphisms and additional symmetries, *Discrete Math.*, **304** (2009), 821–833.

[6] P. J. Cameron, *Permutation Groups*, Cambridge University Press, 1999.

[7] N. J. Cavenagh and D. S. Stones, Near-automorphisms of Latin squares. *J. Combin. Des.*, **19** (2011), 365-377.

[8] C. J. Colbourn and A. Rosa, *Triple systems*, Clarendon, Oxford, 1999.

[9] P. Csörgő, A. Drápal and M. Kinyon, *Buchsteiner loops*, Internat. J. Algebra Comput. **19** (2009), 1049–1088.

[10] S. Doro, Simple Moufang loops, *Math. Proc. Cambridge Philos. Soc.* **83** (1978), 377–392.

[11] A. Drápal and P. Jedlička, On loop identities that can be obtained by a nuclear identification, *European J. Combin*, **31** (2010), 1907–1923.

[12] A. A. Drisko, Loops with transitive automorphisms, *J. Algebra* **184** (1996), 213–229.

[13] A. A. Drisko, Loops of order $p^n + 1$ with transitive automorphism groups, *Adv. Math.*, 128 (1997), 36–39.

[14] A. A. Drisko, Proof of the Alon-Tarsi conjecture for $n = 2^r p$, *Electron. J. Combin.* **5** (1998) #R28, 5 pp.

[15] J. Egan and I. M. Wanless, Latin squares with no small odd k-plexes, *J. Combin. Designs* **16** (2008), 477–492.

[16] 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.

[17] R. M. Falcón, Cycle structures of autotopisms of the Latin squares of order up to 11, *Ars Combin.*, to appear.

[18] 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.

[19] R. M. F. Ganfornina, *Decomposition of principal autotopisms into triples of a Latin square*, in Book of abstracts of the Tenth Meeting on Computer Algebra and Applications, Seville, Spain, 7-9 Sep 2006, 95–98. (Author also known as R. M. Falcón.)

[20] R. M. F. Ganfornina, *Latin squares associated to principal autotopisms of long cycles. Application in cryptography*, in Proceedings of Transgressive Computing, Granada, Spain, 24–26 April 2006, 213–230. `http://www.orcca.on.ca/conferences/tc2006/TC2006-Proceedings.pdf`

[21] *GAP – Groups, algorithms, programming – A system for computational discrete algebra*. `http://www.gap-system.org/`.

[22] E. G. Goodaire and D. A. Robinson, A class of loops which are isomorphic to all loop isotopes, *Canad. J. Math.* **34** (1982), 662–672.

[23] M. V. Horoševskiĭ, Automorphisms of finite groups, *Math. Sb. (N.S.)* **93** (**135**) (1974). 576–587.

[24] A. Hulpke, P. Kaski and P. R. J. Östergård, The number of Latin squares of order 11, *Math. Comp.*, 80 (2011) 1197–1219.

[25] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, The structure of commutative automorphic loops, *Trans. Amer. Math. Soc.* **363** (2011), 365–384.

[26] P. Jedlička, M. K. Kinyon and P. Vojtěchovský, Constructions of commutative automorphic loops, *Comm. Algebra* **38** (2010), 3243–3267.

[27] B. Kerby and J. D. H. Smith, Quasigroup automorphisms and symmetric group characters, *Comment. Math. Univ. Carol.*, **51** (2010), 279–286.

[28] B. L. Kerby and J. D. H. Smith, Quasigroup automorphisms and the Norton-Stein complex, *Proc. Amer. Math. Soc.* **138** (2010), 3079–3088.

[29] M. K. Kinyon and K. Kunen, The structure of extra loops, *Quasigroups Related Systems* **12** (2004), 39–60.

[30] 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.

[31] C. Laywine and G. L. Mullen, Latin cubes and hypercubes of prime order, *Fibonacci Quart.* **23** (1985), 139–145.

[32] C. Mears, *Automatic Symmetry Detection and Dynamic Symmetry Breaking for Constraint Programming*, PhD thesis, Monash University, 2009. `http://www.csse.monash.edu.au/~cmears/files/thesis.pdf`.

[33] R. Moufang, Zur Struktur von Alternativkörpern, *Math. Ann.* **110** (1935), 416–430.

[34] B. M. Maenhaut, I. M. Wanless and B. S. Webb, Subsquare-free Latin squares of odd order, *European J. Combin.*, **28** (2007) 322–336.

[35] B. D. McKay, *nauty – Graph isomorphic software*, `http://cs.anu.edu.au/~bdm/nauty/`.

[36] B. D. McKay, A. Meynert and W. Myrvold, Small Latin squares, quasigroups and loops, *J. Combin. Des.*, **15** (2007), 98–119.

[37] B. D. McKay and I. M. Wanless, On the number of Latin squares, *Ann. Comb.*, **9** (2005), 335–344.

[38] H. Minc, *Permanents*, Addison-Wesley, 1978.

[39] G. P. Nagy and P. Vojtěchovský, *LOOPS – Computing with quasigroups and loops in GAP*. `http://www.math.du.edu/loops/`.

[40] G. P. Nagy and P. Vojtěchovský, Computing with small quasigroups and loops, *Quasigroups Related Systems*, **15** (2007), 77–94.

[41] A. A. Sade, Autotopies des quasigroupes et des systèmes associatifs, *Arch. Math. (Brno)*, **4** (1968), 1–23.

[42] D. S. Stones, The parity of the number of quasigroups. *Discrete Math.*, **310** (2010), 3033–3039.

[43] D. S. Stones, *On the Number of Latin Rectangles*, PhD thesis, Monash University, 2010. `http://arrow.monash.edu.au/hdl/1959.1/167114`.

[44] D. S. Stones, The many formulae for the number of Latin rectangles, *Electron. J. Combin.*, **17** (2010) A1.

[45] D. S. Stones and I. M. Wanless, Compound orthomorphisms of the cyclic group, *Finite Fields Appl.*, **16** (2010), 277–289.

[46] D. S. Stones and I. M. Wanless, Divisors of the number of Latin rectangles, *J. Combin. Th. Ser. A*, **117** (2010), 204–215.

[47] D. S. Stones and I. M. Wanless, A congruence connecting Latin rectangles and partial orthomorphisms, *Ann. Comb.*, to appear.

[48] D. S. Stones and I. M. Wanless, How not to prove the Alon-Tarsi Conjecture, Nagoya Math. J., to appear.

[49] I. M. Wanless, Diagonally cyclic Latin squares, *European J. Combin.*, **25** (2004), 393–413.

[50] I. M. Wanless, Atomic Latin squares based on cyclotomic orthomorphisms, *Electron. J. Combin.*, **12** (2005), R22.

[51] I. M. Wanless, author's homepage, `http://users.monash.edu.au/~iwanless/data/autotopisms`.

[52] I. M. Wanless and E. C. Ihrig, Symmetries that Latin Squares Inherit from 1-Factorizations, *J. Combin. Designs*, **13** (2005), 157–172.

[53] I. M. Wanless and B. S. Webb, The existence of Latin squares without orthogonal mates, *Des. Codes Cryptogr.*, **40** (2006), 131–135.

A Autotopism cycle structures for orders up to 17

Appealing to Lemma 2.1, we only list cycle structures (a, b, c) of autotopisms (α, β, γ). For a given order n, the first column gives the cycle structure of α. In a given row, the second column gives all possible cycle structures of β and γ, separated by commas. If β and γ have the same cycle structure, we only list the cycle structure of β, else we give the cycle structures of β and γ as an ordered pair in parentheses.

$n = 1$ α	β and γ
1	1

$n = 2$ α	β and γ
1^2	$1^2, 2$

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

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

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

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

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

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

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

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

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

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

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

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

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

$n = 16$ α	β and γ
1^{16}	$1^{16}, 2^8, 4^4, 8^2, 16$
$2{\cdot}1^{14}$	$2^8, 4^4, 8^2, 16$
$2^2{\cdot}1^{12}$	$2^8, 4^4, 8^2, 16$
$2^3{\cdot}1^{10}$	$2^8, 4^4, 8^2, 16$
$2^4{\cdot}1^8$	$2^4{\cdot}1^8, 2^8, 4^4, 8^2, 16$
$2^5{\cdot}1^6$	$2^5{\cdot}1^6, 2^8, 4^4, 8^2, 16$
$2^6{\cdot}1^4$	$2^6{\cdot}1^4, 2^8, 4^4, 8^2, 16$
$2^7{\cdot}1^2$	$2^7{\cdot}1^2, 2^8, 4^4, 8^2, 16$
2^8	$2^8, 4^4, 8^2, 16$
$3^3{\cdot}1^7$	$3^3{\cdot}1^7$
$3^4{\cdot}1^4$	$3^4{\cdot}1^4, 6^2{\cdot}2^2, 12{\cdot}4$
$3^4{\cdot}2{\cdot}1^2$	$6^2{\cdot}2^2, 12{\cdot}4$
$3^4{\cdot}2^2$	$6^2{\cdot}2^2, 12{\cdot}4$
$3^5{\cdot}1$	$3^5{\cdot}1$
$4{\cdot}1^{12}$	$4^4, 8^2, 16$
$4{\cdot}2{\cdot}1^{10}$	$4^4, 8^2, 16$
$4{\cdot}2^2{\cdot}1^8$	$4^4, 8^2, 16$
$4{\cdot}2^3{\cdot}1^6$	$4^4, 8^2, 16$
$4{\cdot}2^4{\cdot}1^4$	$4^4, 8^2, 16$
$4{\cdot}2^5{\cdot}1^2$	$4^4, 8^2, 16$
$4{\cdot}2^6$	$4^4, 8^2, 16$
$4^2{\cdot}1^8$	$4^2{\cdot}1^8, 4^2{\cdot}2^4, 4^4, 8^2, 16$
$4^2{\cdot}2{\cdot}1^6$	$4^2{\cdot}2^4, 4^4, 8^2, 16$
$4^2{\cdot}2^2{\cdot}1^4$	$4^2{\cdot}2^2{\cdot}1^4, 4^2{\cdot}2^4, 4^4, 8^2, 16$
$4^2{\cdot}2^3{\cdot}1^2$	$4^2{\cdot}2^3{\cdot}1^2, 4^2{\cdot}2^4, 4^4, 8^2, 16$
$4^2{\cdot}2^4$	$4^2{\cdot}2^4, 4^4, 8^2, 16$
$4^3{\cdot}1^4$	$4^3{\cdot}1^4, 4^3{\cdot}2^2, 4^4, 8^2, 16$
$4^3{\cdot}2{\cdot}1^2$	$4^3{\cdot}2{\cdot}1^2, 4^3{\cdot}2^2, 4^4, 8^2, 16$
$4^3{\cdot}2^2$	$4^3{\cdot}2^2, 4^4, 8^2, 16$
4^4	$4^4, 8^2, 16$
$5^2{\cdot}1^6$	$5^2{\cdot}1^6, 10{\cdot}2^3$
$5^2{\cdot}2{\cdot}1^4$	$10{\cdot}2^3$
$5^2{\cdot}2^2{\cdot}1^2$	$10{\cdot}2^3$
$5^3{\cdot}1$	$5^3{\cdot}1$
$6{\cdot}3{\cdot}2^2{\cdot}1^3$	$6{\cdot}3{\cdot}2^2{\cdot}1^3$
$6{\cdot}3{\cdot}2^3{\cdot}1$	$6{\cdot}3{\cdot}2^3{\cdot}1$
$6{\cdot}3^2{\cdot}1^4$	$6^2{\cdot}2^2, 12{\cdot}4$
$6{\cdot}3^2{\cdot}2{\cdot}1^2$	$6{\cdot}3^2{\cdot}2{\cdot}1^2, 6^2{\cdot}2^2, 12{\cdot}4$
$6{\cdot}3^2{\cdot}2^2$	$6{\cdot}3^2{\cdot}2^2, 6^2{\cdot}2^2, 12{\cdot}4$
$6^2{\cdot}1^4$	$6^2{\cdot}1^4, 6^2{\cdot}2^2, 12{\cdot}4$
$6^2{\cdot}2{\cdot}1^2$	$6^2{\cdot}2{\cdot}1^2, 6^2{\cdot}2^2, 12{\cdot}4$
$6^2{\cdot}2^2$	$6^2{\cdot}2^2, 12{\cdot}4$
$6^2{\cdot}3{\cdot}1$	$6^2{\cdot}3{\cdot}1$
$7^2{\cdot}1^2$	$7^2{\cdot}1^2, 14{\cdot}2$
$8{\cdot}1^8$	$8{\cdot}1^8, 8{\cdot}2^4, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}2{\cdot}1^6$	$8{\cdot}2^4, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}2^2{\cdot}1^4$	$8{\cdot}2^2{\cdot}1^4, 8{\cdot}2^4, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}2^3{\cdot}1^2$	$8{\cdot}2^3{\cdot}1^2, 8{\cdot}2^4, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}2^4$	$8{\cdot}2^4, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}4{\cdot}1^4$	$8{\cdot}4{\cdot}1^4, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}4{\cdot}2{\cdot}1^2$	$8{\cdot}4{\cdot}2{\cdot}1^2, 8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}4{\cdot}2^2$	$8{\cdot}4{\cdot}2^2, 8{\cdot}4^2, 8^2, 16$
$8{\cdot}4^2$	$8{\cdot}4^2, 8^2, 16$
8^2	$8^2, 16$
$9{\cdot}1^7$	$9{\cdot}1^7$
$9{\cdot}3^2{\cdot}1$	$9{\cdot}3^2{\cdot}1$
$10{\cdot}1^6$	$10{\cdot}1^6, 10{\cdot}2^3$
$10{\cdot}2{\cdot}1^4$	$10{\cdot}2^3$
$10{\cdot}2^2{\cdot}1^2$	$10{\cdot}2^2{\cdot}1^2, 10{\cdot}2^3$
$10{\cdot}5{\cdot}1$	$10{\cdot}5{\cdot}1$
$11{\cdot}1^5$	$11{\cdot}1^5$
$12{\cdot}1^4$	$12{\cdot}1^4, 12{\cdot}2^2, 12{\cdot}4$
$12{\cdot}2{\cdot}1^2$	$12{\cdot}2{\cdot}1^2, 12{\cdot}2^2, 12{\cdot}4$
$12{\cdot}2^2$	$12{\cdot}2^2, 12{\cdot}4$
$12{\cdot}3{\cdot}1$	$12{\cdot}3{\cdot}1$
$13{\cdot}1^3$	$13{\cdot}1^3$
$14{\cdot}1^2$	$14{\cdot}1^2, 14{\cdot}2$
$15{\cdot}1$	$15{\cdot}1$

$n = 17$ α	β and γ
1^{17}	$1^{17}, 17$
$2^5{\cdot}1^7$	$2^5{\cdot}1^7$
$2^6{\cdot}1^5$	$2^6{\cdot}1^5$
$2^7{\cdot}1^3$	$2^7{\cdot}1^3$
$2^8{\cdot}1$	$2^8{\cdot}1$
$3^3{\cdot}1^8$	$3^3{\cdot}1^8$
$3^4{\cdot}1^5$	$3^4{\cdot}1^5$
$3^5{\cdot}1^2$	$3^5{\cdot}1^2$
$4^3{\cdot}1^5$	$4^3{\cdot}1^5$
$4^3{\cdot}2^2{\cdot}1$	$4^3{\cdot}2^2{\cdot}1$
$4^4{\cdot}1$	$4^4{\cdot}1$
$5^2{\cdot}1^7$	$5^2{\cdot}1^7$
$5^3{\cdot}1^2$	$5^3{\cdot}1^2$
$6{\cdot}3{\cdot}2^3{\cdot}1^2$	$6{\cdot}3{\cdot}2^3{\cdot}1^2$
$6{\cdot}3^2{\cdot}2^2{\cdot}1$	$6{\cdot}3^2{\cdot}2^2{\cdot}1$
$6^2{\cdot}1^5$	$6^2{\cdot}1^5$
$6^2{\cdot}2^2{\cdot}1$	$6^2{\cdot}2^2{\cdot}1$
$6^2{\cdot}3{\cdot}1^2$	$6^2{\cdot}3{\cdot}1^2$
$7^2{\cdot}1^3$	$7^2{\cdot}1^3$
$8^2{\cdot}1$	$8^2{\cdot}1$
$9{\cdot}1^8$	$9{\cdot}1^8$
$9{\cdot}3^2{\cdot}1^2$	$9{\cdot}3^2{\cdot}1^2$
$10{\cdot}1^7$	$10{\cdot}1^7$
$10{\cdot}2^2{\cdot}1^3$	$10{\cdot}2^2{\cdot}1^3$
$10{\cdot}2^3{\cdot}1$	$10{\cdot}2^3{\cdot}1$
$10{\cdot}5{\cdot}1^2$	$10{\cdot}5{\cdot}1^2$
$11{\cdot}1^6$	$11{\cdot}1^6$
$12{\cdot}1^5$	$12{\cdot}1^5$
$12{\cdot}2^2{\cdot}1$	$12{\cdot}2^2{\cdot}1$
$12{\cdot}3{\cdot}1^2$	$12{\cdot}3{\cdot}1^2$
$12{\cdot}4{\cdot}1$	$12{\cdot}4{\cdot}1$
$13{\cdot}1^4$	$13{\cdot}1^4$
$14{\cdot}1^3$	$14{\cdot}1^3$
$14{\cdot}2{\cdot}1$	$14{\cdot}2{\cdot}1$
$15{\cdot}1^2$	$15{\cdot}1^2$
$16{\cdot}1$	$16{\cdot}1$
17	17