Small Latin Squares, Quasigroups and Loops

Brendan D. McKay*
Department of Computer Science
Australian National University
Canberra, ACT 0200, Australia
bdm@cs.anu.edu.au

Alison Meynert† and Wendy Myrvold
Department of Computer Science
University of Victoria
Victoria, B.C., Canada V8W 3P6
wendym@cs.uvic.ca

Abstract

We present the numbers of isotopy classes and main classes of Latin squares, and the numbers of isomorphism classes of quasigroups and loops, up to order 10. The best previous results were for Latin squares of order 8 (Kolesova, Lam and Thiel, 1990), quasigroups of order 6 (Bower, 2000) and loops of order 7 (Brant and Mullen, 1985). The loops of order 8 have been independently found by "QSCGZ" and Guérin (unpublished, 2001).

We also report on the most extensive search so far for a triple of mutually orthogonal Latin squares (MOLS) of order 10. Our computations show that any such triple must have only squares with trivial symmetry groups.

1 Introduction

A *Latin square of order* n is a $n \times n$ array $L = (\ell_{ij})$ such that each row and each column contains a permutation of $I_n = \{1, 2, \ldots, n\}$. A *quasigroup* G is a set together with a binary operation $\circ$ such that the equations $g \circ x = h$ and $y \circ g = h$ have unique solutions for each $g, h \in G$. A quasigroup G is a *loop* if it contains an element e such that $g \circ e = e \circ g = g$ for all $g \in G$. This paper is concerned with the numbers of Latin squares, quasigroups and loops for small n.

Some alternative representations of a Latin square can be useful. The *orthogonal array* representation of L is the set of n^2 ordered *triplets* $\{(i, j, \ell_{ij}) \mid 1 \le i, j \le n\}$. By the definition of L, each ordered pair of numbers from I_n appears exactly once in the first

*Supported by the Australian Research Council

†Current address: European Bioinformatics Institute, Wellcome Trust Genome Campus, Hinxton, Cambridge, CB10 1SD, UK; ameynert@ebi.ac.uk

two positions of the triplets, exactly once in the second and third positions, and exactly once in the first and third positions.

Another representation is obtained by interpreting L as the multiplication table of a quasigroup G. The elements of G are $\{g_1, g_2, \ldots, g_n\}$ and the binary operation is defined by $g_i \circ g_j = g_{\ell_{ij}}$. Clearly G is a loop if there is a number i such that row i and column i of L each contain the identity permutation.

Various equivalence relations are defined on the set of Latin squares. We will define these in terms of the orthogonal array representation. Define $I_n^3 = I_n \times I_n \times I_n$ and $S_n^3 = S_n \times S_n \times S_n$, where S_n is the symmetric group on I_n. The action of S_n^3 on I_n^3 is given by $(i,j,k)^{(r,c,s)} = (i^r, j^c, k^s)$ for $(i,j,k) \in I_n^3$ and $(r,c,s) \in S_n^3$. We also define the group T of order 3! that acts by consistently permuting the entries of the triplets. Recalling that the three positions in a triplet correspond to the rows, columns and symbols of L, we will write elements of T as permutations of the three tokens $\{R, C, S\}$. For example, (RC) is the matrix transpose operation, while (RCS) has the action $(i,j,k)^{(RCS)} = (k,i,j)$ for each triplet (i,j,k). The group $\langle S_n^3, T\rangle$ has order $6(n!)^3$ and is a representation of the wreath product $S_n \wr S_3$. Its elements can be specified by 4-tuples (r,c,s,τ), for $r,c,s \in S_n$ and $\tau \in T$. The element (r,c,s,τ) acts on I_n^3, and thus on the triplets comprising a Latin square, as $(i,j,k)^{(r,c,s,\tau)} = (i^r, j^c, k^s)^\tau$. The images of L under T are called its *conjugates*.

Let $\mathcal{L}_n$ be the set of all Latin squares of order n. In terms of the orthogonal array representation, the group $\langle S_n^3, T\rangle$ acts on $\mathcal{L}_n$ as $L^\sigma = \{(i,j,k)^\sigma \mid (i,j,k) \in L\}$ for $L \in \mathcal{L}_n, \sigma \in \langle S_n^3, T\rangle$. The orbits of this action are the *main classes* of $\mathcal{L}_n$, and two squares in the same main class are said to be *paratopic*. The stabiliser $\mathrm{Par}(L) = \{\sigma \in \langle S_n^3, T\rangle\} \mid L^\sigma = L\}$ is called the *autoparatopy group* of L, and its elements are the *autoparatopisms* of L.

If we restrict ourselves to the subgroup $S_n^3 \leq \langle S_n^3, T\rangle$, its orbits are called *isotopy classes* of $\mathcal{L}_n$, the stabiliser $\mathrm{Is}(L) = \{\sigma \in S_n^3 \mid L^\sigma = L\}$ is the *autotopy group* of L, and its elements are *autotopisms* of L. More generally, $\sigma \in S_n^3$ is an *isotopism* from L to L' if $L' = L^\sigma$.

A notion of equivalence intermediate between isotopy and paratopy is also of some interest. A *type* of Latin square is an equivalence class under the subgroup $\langle S_n^3, T'\rangle \leq \langle S_n^3, T\rangle$, where $T' = \langle (RC)\rangle$. In other words, the isotopisms are augmented by the matrix transpose operation. Types of Latin square correspond to isomorphism classes of 1-factorizations of complete bipartite graphs, with the transpose operation corresponding to interchange of the two colour classes.

The terminology (but not the notation) we have introduced above mostly follows the practice of Sade, who developed much of the basic theory of Latin squares in a long series

of papers. Much alternative terminology appears in the literature as well. For example, the autotopy group is sometimes called the *isotopy group*, and the autoparatopisms are also called *main class isotopisms*. Isotopy classes have been called *transformation sets*. The conjugates of a Latin square can be called its *adjugates* or its *parastrophes*. Main classes are sometimes called *paratopy classes* or *species*. Our use of the word *type* follows Schönhardt [50]; there does not seem to be a modern name for this concept.

The quasigroup view of a Latin square invites us to also consider isomorphisms and automorphisms as usually defined for algebraic structures. These are the isotopisms and autotopisms that lie in the diagonal subgroup $\Delta_n = \{(r, c, s) \in S_n^3 \mid r = c = s\}$. The *automorphism group* of L is $\mathrm{Aut}(L) = \mathrm{Is}(L) \cap \Delta_n$.

It is obvious that $\mathrm{Par}(L^\sigma) = \mathrm{Par}(L)^\sigma$, $\mathrm{Is}(L^\sigma) = \mathrm{Is}(L)^\sigma$ for any $L \in \mathcal{L}_n, \sigma \in \langle S_n^3, T\rangle$, and $\mathrm{Aut}(L^\sigma) = \mathrm{Aut}(L)^\sigma$ for any $L \in \mathcal{L}_n, \sigma \in \Delta_n$, where $\langle S_n^3, T\rangle$ acts on itself by conjugation. Equally clear is that each main class is a union of isotopy classes which, in turn, are unions of isomorphism classes.

A Latin square is called *reduced* (also sometimes called *normalized* or *in standard form*) if the first row and the first column contain the identity permutation. Since the total number of squares is $n!\,(n-1)!$ times the number of reduced squares, it will suffice to consider the latter.

History.

The counting of Latin squares has a long history, unfortunately beset by many published errors. The number of reduced squares up to order 5 was known to Euler [21] and Cayley [16]. McMahon [30] used a different method to find the same numbers, but obtained the wrong value for order 5. The number of reduced squares of order 6 was found by Frolov [24] and later by Tarry [53] (and later still, but incorrectly, by Jacob [26]). Frolov also gave an incorrect count of reduced squares of order 7. Tarry also found that there were 17 types of squares of order 6, agreeing with an apparent enumeration by Clausen nearly 60 years earlier (see [39]). Schönhardt [50] found the correct numbers of main classes, isotopy classes and reduced squares up to order 6. Fisher and Yates [23], apparently unaware of [50], confirmed Tarry's values and also correctly gave the numbers of isotopy classes of order up to 6. Norton [39] found 146 main classes and 562 isotopy classes of order 7. Norton acknowledged his method to be incomplete and, indeed, Sade [46] and Saxena [49] each found more reduced squares than Norton did. Sade [47] traced this to one main class that Norton had missed. This addition gave the correct number, 147, of main classes. Though Sade does not say so explicitly, he gives enough information

to imply that his new main class contains 2 isotopy classes. This corrects Norton's incomplete count of isotopy classes to 564, as was noted by Preece [43]. However, Brown [10] announced the incorrect value 563 and this was widely accepted and is still sometimes quoted in error [17, 20].

Brown also gave the wrong number of isotopy classes of order 8, while Arlazarov et al. [3] gave the wrong number of main classes. The correct number of reduced squares of order 8 was found by Wells [55], and the numbers of isotopy and main classes by Kolesova, Lam and Thiel [28].

The number of reduced squares was obtained for order 9 by Bammel and Rothstein [4], for order 10 by McKay and Rogoyski [34], and for order 11 by McKay and Wanless [35]. In each case the same numbers have been computed independently at least twice, so they are likely to be correct. No counts of isotopy or main classes for orders greater than 8 have appeared before the present paper. In view of the sorry history of the subject, we attempted to do as much of our computation in duplicate as possible.

Several explicit formulas for the number of reduced squares are in the literature ([51, 35], for example) but they are not very useful for computation. Nevertheless, Saxena [49] managed to count the reduced squares of order 7 by means of a formula of MacMahon.

The number of isomorphism classes of loops up to order 6 was found by Schönhardt [50] in 1930, but this was not noticed by Albert [2] or Sade [48] who obtained weaker results much later. Dénes and Keedwell [20] present counts of isomorphism types of "quasigroups" up to order 6, but in fact their numbers count loops. (Their error was due to the incorrect belief that each quasigroup is isomorphic to a reduced square.) The loops up to order 7 were counted by Brant and Mullen [8]. In 2001, "QSCGZ" (who declines to reveal his or her real name) announced the number of loops of order 8 in an electronic forum [44] and the same value was found independently by Guérin [25]. The quasigroups of order 6 were counted by Bower [7].

Mutually orthogonal Latin squares.

Two Latin squares $L = (\ell_{ij})$ and $L' = (\ell'_{ij})$ are *orthogonal* if the ordered pairs (ℓ_{ij}, ℓ'_{ij}) are distinct. Such a pair of Latin squares is also called a *Graeco-Latin square*. A set of two or more Latin squares, each two of them orthogonal, is commonly known as a "set of MOLS". See Colbourn and Dinitz [18] for a recent expository article.

Interest in MOLS dates at least from Euler, who conjectured [21] that there are no orthogonal pairs of order $n = 4k + 2$ for any k. This conjecture was disproved for some values of $k \geq 5$ by Bose and Shrikhande [5], for order 10 by Parker [40], then for all $k \geq 2$

by all three authors [6]. The question of whether sets of more than 2 MOLS exist for order 10 became a *cause célèbre*, partly because it was the smallest order for which the maximum size of a set of MOLS was unknown, and partly because of its relevance to the existence of a projective plane of order 10. The 1988 proof by Lam, Thiel and Swiercz [29] that no such plane exists, together with a theorem of Shrikhande [52], implies that there is no set of 7 MOLS of order 10.

Meanwhile, no set of 3 MOLS of order 10 has yet been found, despite a considerable amount of effort by many people. See [1, 9, 11, 12, 13, 14, 15, 36, 37, 41, 42, 54] for some representative partial results. In this paper we will add our own contribution to this quest; namely, we will describe computations that show that none of the 8,500,842,802 main classes of Latin squares with non-trivial autoparatopy groups lie in a set of 3 MOLS (where the other two squares may have trivial groups). We believe this to be by far the largest systematic search so far undertaken for 3 MOLS of order 10.

2 Enumeration techniques

As raw data for our computations for each n, we will use the total number R_n of reduced Latin squares of order n, together with a file $\mathcal{M}_n$ containing one square from each main class of square with non-trivial autoparatopy group.

The known values of R_n are given in Table 1. As noted before, the total number of squares, reduced or not, is $L_n = n!\,(n-1)!\,R_n$.

n	reduced squares
1	1
2	1
3	1
4	4
5	56
6	9408
7	16942080
8	535281401856
9	377597570964258816
10	7580721483160132811489280
11	5363937773277371298119673540771840

Table 1: Reduced Latin squares of order n

The generation of the squares with non-trivial autoparatopy groups will be described

in the next section. The advantage in using $\mathcal{M}_n$ is that it contains considerably fewer squares than the total number of main classes. This is especially true for $n = 10$, for which the exhaustive listing of all main classes is out of the question with current technology.

We begin by noting a few elementary properties of the groups associated with a Latin square. For $\rho \in S_n$, let $\mathrm{Fix}(\rho)$ be the set of points fixed by ρ.

Theorem 1. *Let L be a Latin square of order n and let $(r, c, s) \in \mathrm{Is}(L)$ be a non-trivial autotopism. Then one of the following is true.*
(i) r, c, s have the same cycle structure with at least one and at most $\lfloor n/2 \rfloor$ fixed points.
(ii) One of r, c, s has at least one fixed point, and the other two have the same cycle structure without fixed points.
(iii) None of r, c, s has fixed points.

Proof. Let $(r, c, s) \in \mathrm{Is}(L)$ be a non-trivial autotopism and let F be the set of triplets $(i, j, k) \in \mathrm{Fix}(r) \times \mathrm{Fix}(c) \times \mathrm{Fix}(s)$ in the orthogonal array representation of L. Since no two triplets overlap in more than one entry, the presence of two fixed points in a triplet implies that the third is also fixed. Therefore we have that

$$|F| = |\mathrm{Fix}(r)|\,|\mathrm{Fix}(c)| = |\mathrm{Fix}(r)|\,|\mathrm{Fix}(s)| = |\mathrm{Fix}(c)|\,|\mathrm{Fix}(s)|. \tag{1}$$

To satisfy (1), either $|\mathrm{Fix}(r)| = |\mathrm{Fix}(c)| = |\mathrm{Fix}(s)|$ or at least two of these values are 0. Also note that for any two permutations γ and δ without the same cycle structure, there is an integer t such that γ^t and δ^t have different numbers of fixed points. (Let t be the smallest number for which γ and δ have different numbers of cycles of length t.) We can easily see that (r, c, s) and all its powers satisfy (1) only if one of cases (i)–(iii) hold, apart from the final constraint in part (i). To prove that constraint, note that if $\mathrm{Fix}(r), \mathrm{Fix}(c), \mathrm{Fix}(s)$ are non-empty they induce a proper Latin subsquare of L, which is well known to have order at most half the order of L. □

For any Latin square L, define $\mathrm{Ty}(L) = 3, 2, 1, 1$ when $|\mathrm{Par}(L)|/|\mathrm{Is}(L)| = 1, 2, 3, 6$, respectively.

Theorem 2. *Let L be a Latin square of order n. Then*
(i) the number of isomorphism classes in the isotopy class of L is $(n!)^2|\mathrm{Aut}(L)|/|\mathrm{Is}(L)|$;
(ii) the number of types in the main class of L is $\mathrm{Ty}(L)$;
(iii) the number of isotopy classes in the main class of L is $6|\mathrm{Is}(L)|/|\mathrm{Par}(L)|$.

Proof. These are standard properties of group actions. Note that $\mathrm{Ty}(L)$ is the number of orbits of $\mathrm{Par}(L)$ on $\{R, C, S\}$. □

Theorem 3.
(i) The number of isotopy classes of Latin squares of order n is

$$\frac{R_n}{n\,n!} + \sum_{L \in \mathcal{M}_n} \frac{6(|\mathrm{Is}(L)| - 1)}{|\mathrm{Par}(L)|}.$$

(ii) The number of types of Latin square of order n is

$$\frac{R_n}{2n\,n!} + \sum_{L \in \mathcal{M}_n} \frac{\mathrm{Ty}(L)|\mathrm{Par}(L)| - 3}{|\mathrm{Par}(L)|}.$$

(iii) The number of main classes of Latin squares of order n is

$$\frac{R_n}{6n\,n!} + \sum_{L \in \mathcal{M}_n} \frac{|\mathrm{Par}(L)| - 1}{|\mathrm{Par}(L)|}.$$

Proof. The number of squares in the same main class as a square L is $6(n!)^3/|\mathrm{Par}(L)|$. This means that the number of squares whose main class is not represented in $\mathcal{M}_n$ is $L_n - 6(n!)^3 \sum_{L \in \mathcal{M}_n} 1/|\mathrm{Par}(L)|$, and (because they all have trivial autoparatopy groups) they are all in main classes of size $6(n!)^3$. This gives (iii). Claim (i) is just the same, on application of Theorem 2(iii). Claim (ii) follows from (iii) and Theorem 2(ii). □

The results of these computations appear in Table 2.

n	main classes	types	isotopy classes
1	1	1	1
2	1	1	1
3	1	1	1
4	2	2	2
5	2	2	2
6	12	17	22
7	147	324	564
8	283657	842227	1676267
9	19270853541	57810418543	115618721533
10	34817397894749939	104452188344901572	208904371354363006

Table 2: Isotopy classes, types and main classes of Latin squares of order n

Define the *cycle structure* of a permutation γ to be the sequence $(n_1, n_2, \dots)$, where n_i is the number of cycles of length i in γ. If $\sigma = (r, c, s)$ is an autotopism of a Latin square, define $\psi(\sigma)$ as follows:
(i) If r, c and s have the same cycle structure $(n_1, n_2, \dots)$, then $\psi(\sigma) = \prod_i n_i!\, i^{n_i}$;
(ii) otherwise, $\psi(\sigma) = 0$.

An element $(r, c, s) \in S_n^3$ will be called *diagonal* if $r = c = s$.

Lemma 1. *For any $\sigma \in S_n^3$, let $D(\sigma)$ denote the number of elements $\rho \in S_n^3$ such that σ^ρ is diagonal. Then $D(\sigma) = n!\,\psi(\sigma)^2$.*

Proof. Say $\sigma = (r, c, s)$ and $\rho = (x, y, z)$. Clearly $D(\sigma) = 0$ unless r, c, s have the same cycle structure, say $(n_1, n_2, \dots)$. We can choose x arbitrarily, in $n!$ ways. Given x, we must choose y such that $c^y = r^x$. This can be done in $\psi(\sigma)$ ways: for each i the cycles of c with length i can be mapped onto those of r^x in $n_i!$ orders, with the points mapping to the least points of each cycle of r^x chosen in i^{n_i} ways. Similarly, z can be chosen in $\psi(\sigma)$ ways. This gives the lemma. □

Lemma 2. *Let L be a Latin square. Define a map $\phi : S_n^3 \times \mathrm{Is}(L) \to \mathcal{L}_n \times S_n^3$ by $\phi(\rho, \sigma) = (L^\rho, \sigma^\rho)$. Define an equivalence relation on $S_n^3 \times \mathrm{Is}(L)$ by $(\rho, \sigma) \sim (\rho', \sigma')$ if and only if $\phi(\rho, \sigma) = \phi(\rho', \sigma')$. Then all the equivalence classes have size $|\mathrm{Is}(L)|$.*

Proof. Consider fixed $\rho \in S_n^3$ and $\sigma \in \mathrm{Is}(L)$. For each $\gamma \in \mathrm{Is}(L)$, $\phi(\gamma\rho, \sigma^{\gamma^{-1}}) = (L^{\gamma\rho}, \sigma^{\gamma^{-1}\gamma\rho}) = (L^\rho, \sigma^\rho) = \phi(\rho, \sigma)$. Moreover, each $\gamma\rho$ is distinct. Therefore the equivalence classes have size at least $|\mathrm{Is}(L)|$.

Conversely, if $\phi(\rho, \sigma) = \phi(\rho', \sigma')$ define $\gamma = \rho'\rho^{-1}$. Since $L^\rho = L^{\rho'} = L^{\gamma\rho}$ we must have $L = L^\gamma$; i.e., $\gamma \in \mathrm{Is}(L)$. Furthermore, since $\sigma^\rho = (\sigma')^{\rho'} = (\sigma')^{\gamma\rho}$, we have $\sigma = (\sigma')^\gamma$ and so $\sigma' = \sigma^{\gamma^{-1}}$. This is the case of equivalence we already identified, so the equivalence classes have size exactly $|\mathrm{Is}(L)|$. □

Theorem 4. *The number of isomorphism classes of Latin squares (that is, the number of isomorphism classes of quasigroups) of order n is*

$$(n-1)!\, R_n + \sum_{L \in \mathcal{M}_n} \frac{6}{|\mathrm{Par}(L)|} \sum_{\sigma \in \mathrm{Is}'(L)} \psi(\sigma)^2,$$

where $\mathrm{Is}'(L)$ is the autotopy group of L with the identity removed.

Proof. Let H be the set of diagonal elements of S_n^3. We need to determine the number of orbits of the action of H on $\mathcal{L}_n$. According to the Frobenius-Burnside Lemma [38], this is

equal to the average number of Latin squares L fixed by elements of H. That is, $n!$ times the number of isomorphism classes equals the number of distinct pairs (M, σ) such that $M \in \mathcal{L}_n$ and $\sigma \in H \cap \mathrm{Is}(M)$.

We will find the number of such pairs (M, σ) with M in the isotopy class of some given square L. Since $\mathrm{Is}(L^\rho) = \mathrm{Is}(L)^\rho$, each (M, σ) is $\phi(\rho, \sigma)$ for some $\rho \in S_n^3$ and $\sigma \in \mathrm{Is}(L)$, where ϕ is defined in Lemma 2. By Lemma 1, exactly $D(\sigma)$ values of ρ are such that σ^ρ are diagonal, and by Lemma 2 each value of $\phi(\rho, \sigma)$ appears for exactly $|\mathrm{Is}(L)|$ values of (ρ, σ). Thus we have that the number of isomorphism classes is

$$\sum_L \frac{1}{|\mathrm{Is}(L)|} \sum_{\sigma \in \mathrm{Is}(L)} \psi(\sigma)^2,$$

where the outer sum is over one arbitrary representative of each isotopy class. Moreover, $\sum_{\sigma \in \mathrm{Is}(L)} \psi(\sigma)^2$ is equal for all L in the same main class, so the theorem follows. □

We can identify the number of isomorphism classes of loops as the number of isomorphism classes of reduced Latin squares, since a loop has exactly one identity and we can label it first.

Given a Latin square $L = (\ell_{ij})$, there are $n^2(n-1)!$ elements $\rho \in S_n^3$ such that L^ρ is reduced. These can be parameterised $\rho(i, j, s)$, where $i, j \in I_n$ and $\delta \in S_n$ such that δ fixes 1. Set $k = \ell_{ij}$. First, swap row i with row 1, column j with column 1, and symbol k with symbol 1. Then apply δ to rename the symbols other than 1. Finally, permute the rows and columns such that the first row and first column are in numerical order. To identify $\rho(i, j, \delta)$ explicitly, let $r_i \in S_n$ be the permutation appearing in row i (that is, $\ell_{it} = t^{r_i}$ for each t). Similarly, let c_j be the permutation appearing in column j. Then $\rho(i, j, \delta) = \big(c_j(1\,k)\delta, r_i(1\,k)\delta, (1\,k)\delta\big)$.

If $\sigma = (r, c, s)$ is an autotopism of a Latin square, define $\lambda(\sigma)$ as follows:
(i) If r, c and s have the same cycle structure $(n_1, n_2, \dots)$, then $\lambda(\sigma) = n_1$;
(ii) otherwise, $\lambda(\sigma) = 0$.

Lemma 3. *Consider a Latin square L and $\sigma \in \mathrm{Is}(L)$. Define $(n-1)!\,N(L, \sigma)$ to be the number of $\rho \in S_n^3$ such that L^ρ is reduced and σ^ρ is diagonal. Then $N(L, \sigma) = \lambda(\sigma)^2$.*

Proof. By the preceding discussion, $\rho = \big(c_j(1\,k)\delta, r_i(1\,k)\delta, (1\,k)\delta\big)$ for some $i, j \in I_n$ and $\delta \in S_n$ such that δ fixes 1. Since any $\gamma \in S_n^3$ is diagonal if and only if $\gamma^{((1\,k)\delta,(1\,k)\delta,(1\,k)\delta)}$ is diagonal, we have that $N(L, \sigma)$ is the number of pairs (i, j) for which $\big(r^{c_j}, c^{r_i}, s\big)$ is diagonal; that is, for which $r^{c_j} = c^{r_i} = s$.

Consider the equation $c^{r_i} = s$, or equivalently $cr_i = r_i s$. Say $L = (\ell_{ij})$. For any j, $j^{cr_i} = \ell_{ijc}$ and $j^{r_i s} = \ell_{ij}^s$. Consider the two triplets (i, j^c, ℓ_{ijc}) and (i^r, j^c, ℓ_{ij}^s) in the orthogonal array representation of L—the first by definition and the second since $(r, c, s) \in \mathrm{Is}(L)$. Since triplets cannot have exactly two entries in common, we have that $\ell_{ijc} = \ell_{ij}^s$ if and only if $i^r = i$. That is, $c^{r_i} = s$ exactly when $i \in \mathrm{Fix}(r)$. Similarly, $r^{c_j} = s$ exactly when $j \in \mathrm{Fix}(c)$. By Theorem 1, $N(L, \sigma) = \lambda(\sigma)^2$. □

Theorem 5. *The number of isomorphism classes of reduced Latin squares (that is, the number of isomorphism classes of loops) is*

$$\frac{R_n}{(n-1)!} + \sum_{L \in \mathcal{M}_n} \frac{6}{|\mathrm{Par}(L)|} \sum_{\sigma \in \mathrm{Is}'(L)} \lambda(\sigma)^2,$$

where $\mathrm{Is}'(L)$ *is the autotopy group of* L *with the identity removed.*

Proof. Let H be the group of diagonal elements of S_n^3 that fix $(1, 1, 1)$, and consider H acting on the set of reduced Latin squares. The orbits of this action are the isomorphism classes of loops. By the Frobenius-Burnside Lemma, we have that $|H|$ times the number of orbits is equal to the number of distinct pairs (M, σ') such that M is a reduced square and σ' is a diagonal autotopism of M. (Note that all diagonal autotopisms of a reduced square must fix $(1, 1, 1)$.)

We determine the number of such pairs (M, σ') for which M is isotopic to a given reduced Latin square L. These all have the form (L^ρ, σ^ρ) for some $\sigma \in \mathrm{Is}(L)$ and $\rho \in S_n^3$. For given σ there are $(n-1)!\, N(L, \sigma)$ such values of ρ, but some of the pairs (L^ρ, σ^ρ) are the same. In fact, $(L^\rho, \sigma^\rho) = (L^{\rho'}, \sigma^{\rho'})$ if and only if $\rho' = \gamma\rho$ for some $\gamma \in \mathrm{Is}(L)$, so each value of (L^ρ, σ^ρ) occurs exactly $|\mathrm{Is}(L)|$ times. Therefore the number of isomorphism classes of reduced squares is

$$\sum_L \frac{1}{|\mathrm{Is}(L)|} \sum_{\sigma \in \mathrm{Is}(L)} N(L, \sigma),$$

where the outer sum is over one arbitrary representative of each isotopy class.

Since $N(L^\tau, \sigma^\tau) = N(L, \sigma)$ for any $\sigma \in \mathrm{Is}(L)$ and $\tau \in \langle S_n^3, T \rangle$, by Lemma 3, the contributions of each isotopy class in the same main class are the same.

The theorem now follows. □

Application of Theorems 4 and 5 gives the results shown in Table 3.

n	loops	quasigroups
1	1	1
2	1	1
3	1	5
4	2	35
5	6	1411
6	109	1130531
7	23746	12198455835
8	106228849	2697818331680661
9	9365022303540	15224734061438247321497
10	20890436195945769617	2750892211809150446995735533513

Table 3: Isomorphism classes of loops and quasigroups of order n

3 Generating the Latin squares with symmetries

In this section we will describe the method by which we found all the Latin squares of order up to 10 having non-trivial autoparatopy groups. To begin, we identify a set of autoparatopisms such that each square with non-trivial autoparatopy group is in the same main class as a square with at least one of these autoparatopisms.

Lemma 4. *Suppose L is a Latin square with non-trivial autoparatopy group. Then some Latin square L' in the same main class as L has an autoparatopism σ with one of the following structures.*
(i) For some prime p, $\sigma = (r, c, s)$ where r, c and s have order p with the same number m of fixed points, where $1 \leq m \leq n/2$.
(ii) For some prime p dividing n, $\sigma = (r, c, s)$ where r and c have order p and no fixed points, and s has order 1 or p. Moreover, in the case that $p = 2$ and $n \equiv 2 \pmod 4$, s has at least two fixed points.
(iii) $\sigma = (1, 1, s, (RC))$, where s has order 1 or 2 and has at least one fixed point.
(iv) $\sigma = (RCS)$.

Proof. In the case where $\mathrm{Is}(L)$ is non-trivial, Theorem 1 implies that there is an autotopism of type (i) or (ii) for any prime p dividing $|\mathrm{Is}(L)|$. It remains to prove the last claim of part (ii). Suppose r, c, s all have order 2 without fixed points. Take any partitions $I_n = R_1 \cup R_2 = C_1 \cup C_2 = S_1 \cup S_2$ such that r swaps R_1 and R_2, c swaps C_1 and C_2, and s swaps S_1 and S_2. For $R, C, S \subseteq I_n$, let $m(R, C, S)$ be the number of times an element of S appears in the submatrix of L induced by rows R and columns C. Since each symbol appears exactly once in each row and once in each column, $m(R_1, C_1, S_1) =$

$n^2/4 - m(R_1, C_2, S_1) = m(R_2, C_2, S_1)$. On the other hand, the action of σ gives that $m(R_1, C_1, S_1) = m(R_2, C_2, S_2)$. Therefore $m(R_2, C_2, S_1) = m(R_2, C_2, S_2) = n^2/8$. This is a problem for $n \equiv 2 \pmod 4$, since $n^2/8$ is not then an integer.

We are left with the possibility that $\mathrm{Par}(L)$ is non-trivial but $\mathrm{Is}(L)$ is trivial. Since $|T| = 6$, $\mathrm{Par}(L)$ contains an element σ of order 2 or 3. If σ has order 2, we can assume by conjugating L that $\sigma = (r, c, s, (RC))$. In order that $\sigma^2 = (rc, cr, s^2, 1)$ is not a non-trivial autotopism (which we are assuming to not exist), we must have $rc = s^2 = 1$. Now $L' = L^{(1,c,1)}$ has the autoparatopism $(1, 1, s, (RC))$. The reason that s must have at least one fixed point is that symbols on the diagonal must be fixed by s. If σ has order 3, we can assume by conjugating L that $\sigma = (r, c, s, (RCS))$. Since the autotopism σ^3 must be trivial by assumption, it must be that $rcs = 1$. Now $L' = L^{(1,r^{-1},s)}$ has the autoparatopism $(1, 1, 1, (RCS))$. □

For $n \leq 9$, the number of main classes of Latin squares having one of the above symmetries is small enough that we can keep them all on disk for processing at leisure. For $n = 10$, the numbers are slightly too large, so we took a more complex approach. For each of the symmetries σ of order 2 defined in Lemma 4, let $\mathcal{L}(\sigma)$ be the set of Latin squares L of order 10 such that $\mathrm{Par}(L) = \langle\sigma\rangle$. It turns out that the great majority of squares of order 10 either have trivial autoparatopy groups or lie in one of the sets $\mathcal{L}(\sigma)$; that is, they have $|\mathrm{Par}(L)| \leq 2$. Our generation programs were designed so that the main classes of each set $\mathcal{L}(\sigma)$ are generated a predictable number of times (such as once, or once per isotopy class). This enabled our counting theorems to be applied to each $\mathcal{L}(\sigma)$ as the squares were generated. Only the much smaller number of Latin squares with larger autoparatopism groups needed to be stored, for sorting according to main class.

To compute the various groups associated with a Latin square L, we used the program `nauty` [32]. Since `nauty` deals only with vertex-coloured graphs, we needed to convert L to a graph whose automorphisms correspond to the symmetries of L.

Consider the orthogonal array representation of L. Define vertex-coloured graphs $G_1(L)$, $G_2(L)$ and $G_3(L)$ thus:

- The $n^2 + 3n$ vertices of $G_2 = G_2(L)$ are

$$V(G_2) = \{r_i \mid i \in I_n\} \cup \{c_i \mid i \in I_n\} \cup \{s_i \mid i \in I_n\} \cup \{e_{ij} \mid i, j \in I_n\},$$

  where there is a different colour for each of the four subsets. The $3n^2$ edges of G_2 are

$$E(G_2) = \{r_i e_{ij}, c_j e_{ij}, s_k e_{ij} \mid (i, j, k) \in L\}.$$

- The graph $G_1 = G_1(L)$ is formed from G_2 by appending three additional vertices $\{R, C, S\}$ and $3n$ additional edges $\{Rr_i, Cc_i, Ss_i \mid i \in I_n\}$. The vertex colours are different: one colour for $\{R, C, S\}$, one for $\{r_i, c_i, s_i \mid i \in I_n\}$, and a third colour for the rest.

- The graph $G_3 = G_3(L)$ is formed from G_2 by adding $3n$ additional edges $\{r_ic_i, r_is_i, c_is_i \mid i \in I_n\}$. The vertex colours are the same as for G_2.

Theorem 6. *Let* $\mathrm{Aut}(G)$ *denote the automorphism group of graph* G*. Then the following hold for each Latin square* L *and for each pair* L_1, L_2 *of Latin squares of the same order.*
(i) $\mathrm{Aut}(G_1)$ *is isomorphic to* $\mathrm{Par}(L)$*. This isomorphism maps* $(r, c, s) \in \mathrm{Is}(L)$ *onto the automorphism of* G_1 *which acts like* r, c, s *on* $\{r_i \mid i \in I_n\}$, $\{c_i \mid i \in I_n\}$, *and* $\{s_i \mid i \in I_n\}$, *respectively. The image of* $\tau \in T$ *is the automorphism that acts as* τ *on* $\{(R, C, S)\} \cup \{(r_i, c_i, s_i) \mid i \in I_n\}$*. Moreover,* L_1 *is paratopic to* L_2 *if and only if* $G_1(L_1)$ *is isomorphic to* $G_1(L_2)$*.*
(ii) $\mathrm{Aut}(G_2)$ *is isomorphic to* $\mathrm{Is}(L)$*. Precisely, for each* $(r, c, s) \in \mathrm{Is}(L)$*, there is an automorphism* γ *of* G_2 *such that* r, c, s *are the actions of* γ *on* $\{r_i \mid i \in I_n\}$, $\{c_i \mid i \in I_n\}$, *and* $\{s_i \mid i \in I_n\}$, *respectively. Moreover,* L_1 *is isotopic to* L_2 *if and only if* $G_2(L_1)$ *is isomorphic to* $G_2(L_2)$*.*
(iii) $\mathrm{Aut}(G_3)$ *is isomorphic to* $\mathrm{Aut}(L)$*. The correspondence is the same as in part (ii). Moreover,* L_1 *is isomorphic to* L_2 *if and only if* $G_3(L_1)$ *is isomorphic to* $G_3(L_2)$*.*

Proof. In each case it is easy to see that the combinatorial structure of the graph corresponds precisely to that of the square. The colouring of G_2 forces automorphisms of G_2 to correspond to autotopisms of L. For G_3, the extra edges force automorphisms of the graph to correspond to automorphisms of the square. Details are left to the reader. □

All of the required generation tasks, corresponding to the symmetries listed in Lemma 4, were performed using at least two independent programs. This provided a good check against both coding errors and machine errors. In most cases, one generator used the orderly approach of Read [45] and Faradžev [22], while the other used the canonical construction path method of McKay [33]. We will present a representative example of each approach.

Orderly generation.

To illustrate the orderly approach to generation, we consider generating squares with an autoparatopism $\sigma = (1, 1, s, (RC))$ as in Lemma 4(iii). Given such a square L, let

$L[k]$ be the subsquare formed by the first k rows and first k columns. Clearly $L[k]$ is also invariant under σ if we make the convention of ignoring the missing rows and columns.

For each k, define P_k to be the set of 3-tuples (r', c', s') where r' and c' are the same permutation of $\{1, 2, \ldots, k\}$, and s' is a permutation of $\{1, 2, \ldots, n\}$ such that $s^{s'} = s$. It is clear that, if $L[k]^\sigma = L[k]$ and $\rho \in P_k$, then $L[k]^{\rho\sigma} = L[k]^\rho$. Two subsquares $L[k]$ and $L'[k]$ of the same size can be compared by comparing their upper triangles in the order $(1,1), (2,2), (1,2), (3,3), (2,3), (1,3), \ldots, (k,k), (k{-}1,k), \ldots, (1,k)$. We will say that $L[k]$ is *minimal* if $L[k] \leq L[k]^\rho$ under this ordering for all $\rho \in P_k$.

The essential property used by orderly generation is that if $L = L[n]$ is minimal then each of the subsquares $L[k]$ is also minimal. Therefore, we can find the minimal subsquares $L[k]$ by taking the minimal subsquares $L[k{-}1]$, bordering them with an extra row and column related by s, then rejecting the extended subsquares if they are not minimal.

One improvement is to reject certain subsquares which cannot possibly be extended to complete squares.

Lemma 5. *Suppose the permutation s fixes m symbols. For symbol x, let $N(x)$ be its number of appearances in $L[k]$, $1 \leq k < n$. Then*
(i) $N(x) \geq 2k - n$ for all x;
(ii) $\sum_x N(x) \geq n - k + (2k - n)m$, where the sum is over the symbols fixed by s;
(iii) $N(x) \equiv n \pmod 2$ for at least $k + m - n$ of the symbols fixed by s.

Proof. Let Q be the order $n-k$ subsquare of $L[n]$ complementary to $L[k]$. If some symbol x appears $N(x)$ times in $L[k]$, then it appears $n - 2k + N(x)$ times in Q. This proves (i). In the case of symbols fixed by s, Q must contain at least $n - k$ occurences of them altogether since only such symbols may appear on the diagonal. This gives (ii). The number of symbols fixed by s that appear an odd number of times in Q is at most $n - k$, since such symbols must appear on the diagonal. The value of $N(x)$ for such symbols has the opposite parity to n, which gives (iii). □

Cruse [19] proved that conditions (i) and (iii) are sufficient for $L[k]$ to be extendible to $L[n]$ in the case $m = n$. (Condition (ii) always holds in that case.)

It is clear that the most onerous part of this method is the minimality test of the extended subsquares, since P_k can be quite large. In principle we can just compare $L[k]^\rho$ to $L[k]$ for all $\rho \in P_k$, but there are ways to do the test faster on average. For example, since $L[k{-}1]$ is known to be minimal, any ρ which fixes the new row and column and gives $L[k]^\rho < L[k]$ must also give $L[k{-}1]^\rho = L[k{-}1]$. All such permutations, typically

few, were earlier found during the verification of the minimality of $L[k-1]$. We can also employ some heuristics. For example, if some $L[k]$ is rejected because $L[k]^\rho < L[k]$, then the same ρ is also likely to reject other candidates $L'[k]$ appearing in the near future.

The resulting output of this method is the set of Latin squares L such that $L^\sigma = L$ and L is minimal under P_n. This is then a set of equivalence class representatives under the action of P_n.

For example, consider the case $n = 10$, $s = (5\,6)(7\,8)(9\,10)$. There are 1699361022 squares output altogether. That is too many squares to easily keep around, but fortunately all but a relative handful, 1512278 to be precise, have the property that σ is their only non-trivial autoparatopism. If $\langle\sigma\rangle$ is the full autoparatopy group, then equivalence classes under P_n are the same as equivalence classes under S_n^3 (i.e., isotopy classes). Therefore, the contributions of the great majority of the output squares to the counting lemmas of the previous section are determined just by the number of such squares. The 1512278 squares with larger autoparatopy groups can be sorted into main classes using Theorem 6. The generation speed for this example was about 1500 per second (1GHz Pentium III).

Generation by canonical construction path.

As an example of the canonical construction path approach, we consider Lemma 4(i) with $n = 10$, $p = 2$ and $m = 2$. We can assume that $\sigma = (r, c, s)$, where $r = c = s = (3\,4)(5\,6)(7\,8)(9\,10)$, so that 1 and 2 are the fixed points.

The square is constructed one *(row) block* at a time, where a row block consists of the rows corresponding to a cycle of r. Thus, there are 2 blocks of 1 row each and 4 blocks of 2 rows each. If L is a Latin square with $\sigma \in \mathrm{Is}(L)$, let $L(k)$ denote the rectangle consisting of the first k blocks of L. For our example, $L(6) = L$.

We next define a limited type of isotopism. If L' is another square with $\sigma \in \mathrm{Is}(L')$, then L is σ-*isotopic* to L' if there is an isotopism $\rho : L \mapsto L'$ such that $\sigma^\rho = \sigma$. Similarly, we can define the σ-isotopism of $L(k)$ and $L'(k)$ for any k (just ignore the cycles of r lying outside the first k row blocks). Clearly, σ-isotopism is an equivalence relation so we can speak of σ-isotopism classes. We will call σ-isotopisms from $L(k)$ to itself σ-*autotopisms*.

The basic idea of the method is to generate one representative of each σ-isotopism class of k-block rectangles by extending the $(k-1)$-block rectangles by a single row block. Clearly this is possible; the issue is of how to efficiently restrict the generation to σ-isotopism class representatives. The general technique given in [33] achieves this by application of two "rules". Consider a $(k-1)$-block rectangle U. The σ-autotopisms ρ of U define an action on the set of row blocks which legally extend U to k blocks. (The

extended array must still be a Latin rectangle with autotopism σ.)

The first rule is to only consider one block from each orbit of this action, which can be implemented by computing all σ-autotopisms of U. This computation can be performed by applying `nauty` to a graph similar to $G_2(U)$, defined before Theorem 6, with extra edges $r_i r_j$, $c_i c_j$, $s_i s_j$ for each 2-cycle $(i\,j)$ of r. The latter edges restrict autotopisms to those normalizing σ. (In the similar cases for primes $p > 2$, the orbits of σ are marked using cycles of directed edges.)

The second rule is slightly harder to explain. We require a function f such that, for each rectangle $L(k)$, $f(L(k))$ is an orbit of row blocks of $L(k)$ under the action of the σ-autotopisms of $L(k)$. The required properties are that $f(L(k))$ is an orbit of blocks of 2 rows if there are any, otherwise an orbit of blocks of 1 row, and that $f(L(k)^g) = f(L(k))^g$ for any $g \in S_n^3$ such that $\sigma^g = \sigma$. Such a function can be computed by applying `nauty` to the same graph mentioned above, to put the row blocks of $L(k)$ into a canonical order. Then $f(L(k))$ can be defined as the orbit that includes the first block of the required number of rows. Now we can specify rule two: if $L(k)$ is formed by adding row block B to a $(k-1)$-block rectangle, then $L(k)$ is rejected unless $B \in f(L(k))$.

According to the main theorem of [33], simultaneous application of the two rules implies that exactly one square from each σ-isotopism class is constructed without being rejected.

In practice, use of `nauty` can often be avoided by computing σ-isotopism invariants of the rows, columns and symbols of the encountered rectangles. For example, we could associate each row with the number of 2×2 Latin subsquares which involve that row. With a suitably accurate invariant, we can often tell that a rectangle has no σ-autotopisms other than $\langle\sigma\rangle$ (by far the most common situation), and often find that one row block is uniquely identified by the invariant (in which case we can take $f(L(k))$ to be such a row block with the least value of the invariant). Such devices reduce applications of `nauty` to only a small fraction of cases, and on average speed up the remaining cases (since `nauty` can use the invariant to good effect). This greatly improves the generation speed.

The great majority of the 4838805676 outputs (representatives of σ-isotopism classes of squares with autotopism σ) have no non-trivial autoparatopisms at all other than σ. Clearly such squares are not paratopic to any other of the generated squares other than their conjugates (which are also generated) so there is no need to store them. Rather, we only need to note their number in order to determine their contributions to the counting theorems of the previous section. The remaining output squares, those 3094060 with larger autoparatopy groups, can be sorted into main classes using Theorem 6. The generation

speed was about 21,000 per second (1GHz Pentium III).

r	c	s	τ	N_2	$N_{\geq 3}$
2^3	2^3	2^3	id	476178	11022
2^4	2^4	2^4	id	1871784	17038
3^2	3^2	3^2	id		17835
3^3	3^3	3^3	id		862
id	3^3	3^3	id		368
3^1	3^3	3^3	id		3481
3^2	3^3	3^3	id		4908
5^1	5^1	5^1	id		576
7^1	7^1	7^1	id		258
id	id	id	(RC)	3321	139
id	id	2^1	(RC)	259213	1453
id	id	2^2	(RC)	1407889	8120
id	id	2^3	(RC)	434448	3913
id	id	2^4	(RC)	1679	297
id	id	id	(RCS)		26620

Table 4: Cases of Lemma 4 for order 9

A summary of all the computations for $n = 9, 10$ appears in Tables 4 and 5. The first four columns give the autoparatopism $\sigma = (r, c, s, \tau)$ indicated by Lemma 4. The code "id" means the identity permutation, while "p^k" means a permutation with k cycles of length p and other points fixed. Column N_2 gives the number of outputs with autoparatopy group of order exactly 2, while column $N_{\geq 3}$ gives the number of outputs with larger autoparatopy group. In all cases, the outputs counted by N_2 are in distinct isotopy classes, but those counted by $N_{\geq 3}$ may represent each isotopy class more than once. Thus, an independent replication should expect to duplicate N_2 but not necessarily $N_{\geq 3}$. The relative difficulty of each case is approximately in proportion to the number of outputs. It can be seen that the cases with σ of order 2 are much harder than the others.

To identify the isotopy and main classes uniquely, the outputs with autoparatopy groups larger than 2 were merged together and sorted. In the Appendix, we list the numbers of Latin squares up to order 10 according to the orders of their isotopy and autoparatopy groups.

As an additional check, we generated all of the isotopy classes of Latin squares of order 9 and their groups, using an entirely independent program that uses the orderly method. The results were in agreement with our previous calculations.

r	c	s	τ	N_2	$N_{\geq 3}$
2^3	2^3	2^3	id	38219124	312684
2^4	2^4	2^4	id	4835711616	3094060
id	2^5	2^5	id	51756308	193903
2^1	2^5	2^5	id	515250136	485074
2^2	2^5	2^5	id	1626154210	1350340
2^3	2^5	2^5	id	1860267794	882772
2^4	2^5	2^5	id	647667082	652086
3^2	3^2	3^2	id		775017
3^3	3^3	3^3	id		1698030
5^1	5^1	5^1	id		6516
id	5^2	5^2	id		97
5^1	5^2	5^2	id		1610
5^2	5^2	5^2	id		906
7^1	7^1	7^1	id		2172
id	id	id	(RC)	35785023	93487
id	id	2^1	(RC)	714025565	807303
id	id	2^2	(RC)	2852815668	2076665
id	id	2^3	(RC)	1697848744	1512278
id	id	2^4	(RC)	32544714	142186
id	id	id	(RCS)		3908953

Table 5: Cases of Lemma 4 for order 10

4 The search for three MOLS of order 10

If L is a Latin square of order n, then a *transversal* of L is a set of n entries of L containing one entry from each row, one entry from each column, and one appearance of each symbol.

The relevance of transversals to the search for MOLS is clear when we notice that the positions of one symbol in a Latin square form a transversal in its orthogonal mate. Thus, an orthogonal mate to a square L corresponds to n disjoint transversals of L. This idea, which was first used on a computer by Parker [41], forms the basis for our method of searching for sets of three MOLS.

Theorem 7. *Let L be a Latin square of order n. For $k = 0, 1$ define G_k to be the graphs whose vertices are the transversals of L, and whose edges join transversals with exactly k entries in common. Then L has two orthogonal mates, also orthogonal to each other, if and only if G_0 has two disjoint cliques A, B of order n such that each $a \in A$ is joined by an edge of G_1 to each $b \in B$.*

Proof. It is easy to see by the definitions that a clique of order n in G_0 corresponds to a

Latin square orthogonal to L. Given two such orthogonal mates of L with no common transversals, the orthogonality of each to the other follows from the stated condition on G_1. □

Our computational method involved constructing G_0 and G_1 explicitly, then searching for cliques in G_0 by a highly tuned backtracking method. The efficiency hurdle is that G_0 and G_1 are often quite large (up to 5504 vertices), so that finding cliques is not an easy task. An essential key to efficiency is to note that G_0 is easily properly n-coloured (for example, according to which entry in the first row is used by each transversal) and that any n-clique must include exactly one vertex of each colour.

We also used the automorphism groups of the graphs to partly eliminate solutions equivalent under these groups. Let Γ be any subgroup of $\mathrm{Aut}(G_0) \cap \mathrm{Aut}(G_1)$. A suitable Γ would be the group induced by $\mathrm{Par}(L)$, but we used a heuristic that might find a larger or smaller group. Consider one of the colour classes W defined above, and let $v_1 < v_2 < \cdots < v_k$ be the least-numbered vertices in the non-empty intersections of W with each of the orbits of Γ. If C is an n-clique in G_0, let i be the least index such that C includes a vertex in the same Γ-orbit as v_i. Then C is equivalent under Γ to some n-clique that includes v_i but does not include any vertex in the same orbit as any of $v_1, \ldots, v_{i-1}$. Thus, we can examine all the cliques containing v_1, eliminate the entire orbit of v_1 from the graph, examine all the cliques containing v_2, and so forth. This technique greatly sped-up the most difficult cases, but the average improvement over all cases was rather modest due to most of the groups being small. An example where this technique produces a massive speedup is given in [31].

The resulting program managed to test 2–3 squares per second (1GHz Pentium III). We ran it for representatives of each of the 8,500,842,802 main classes with non-trivial autoparatopy groups, but none of them produced a set of 3 MOLS. Those few (less than 5 million) with autoparatopy group greater than 2 in size were run with two independent programs, but this would have been too expensive for those with autoparatopy groups of order 2. The total computation time was 172 years (equal to about 110 years of 1GHz Pentium III).

In a rather smaller computation, we took the squares with autoparatopy groups of order 3 or more, and "turned" one or two intercalates. That is, we replaced

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \quad \text{with} \quad \begin{pmatrix} b & a \\ a & b \end{pmatrix}.$$

About 600 million of the resulting squares have trivial autoparatopy groups, and we also

tested these for extension to a set of 3 MOLS without success.

Despite the scope of this search, it covers only a tiny fraction of Latin squares of order 10. To quantify the difficulty in completing the search by this approach, we tested ten million random Latin squares generated by the Jacobson-Matthews method [27] with pseudo-random starting points and found that 60.8% of them have an orthogonal mate and on average they have 1.023 orthogonal mates (counted without regard to permutations of the symbols of the mate). This suggests there are approximately 10^{15} essentially distinct pairs of orthogonal Latin squares of order 10. With current computational technology, it does not seem plausible to exhaustively search for 3 MOLS by any method that first finds all possible pairs.

Acknowledgment.

We wish to thank Ian Wanless for valuable advice.

References

[1] D. M. Acketa and S. Matić-Kekić, An attempt for construction of a triple of pairwise mutually orthogonal Latin squares on 10 elements, *Zb. Rad. Prirod.-Mat. Fak. Ser. Mat.*, **25** (1995) 141–153.

[2] A. A. Albert, Quasigroups. II., *Trans. Amer. Math. Soc.*, **55** (1944) 401–419.

[3] V. L Arlazarov, A. M. Baraev, Ya. Yu. Gol'fand, I. A. Faradžev. Construction with the aid of a computer of all Latin squares of order 8 (Russian), Algorithmic investigations in combinatoric (Moscow, Nauka, 1978), pp. 129–141, 187.

[4] S. E. Bammel and J. Rothstein, The number of 9×9 Latin squares, *Discrete Math.*, **11** (1975) 93–95.

[5] R. C. Bose and S. S. Shrikhande, On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t+2$, *Proc. Nat. Acad. Sci. U.S.A.*, **45** (1959) 734–737.

[6] R. C. Bose, S. S. Shrikhande and E. T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.*, **12** (1960) 189–203.

[7] C. G. Bower, Private communication (2000).

[8] L. J. Brant, and G. L. Mullen, A note on isomorphism classes of reduced Latin squares of order 7, *Utilitas Math.* **27** (1985) 261–263.

[9] A. E. Brouwer, Four MOLS of order 10 with a hole of order 2, *J. Statist. Plann. Inference*, **10** (1984) 203–205.

[10] J. W. Brown, Enumeration of Latin squares with application to order 8, *J. Combinatorial Theory*, **5** (1968) 177–184.

[11] J. W. Brown, An extension of Mann's theorem to a triple of mutually orthogonal Latin squares of order 10. *J. Combin. Theory Ser. A*, **12** (1972) 316–318.

[12] J. W. Brown and E. T. Parker, A try for three order-10 orthogonal Latin squares, *Congr. Numer.*, **36** (1982) 143–144.

[13] J. W. Brown and E. T. Parker, Some attempts to construct orthogonal Latin squares, *Congr. Numer.*, **43** (1984) 201–202.

[14] J. W. Brown and E. T. Parker, An attempt to construct three mols °10 with a common transversal, *Algebras Groups Geom.*, **2** (1985) 258–262.

[15] J. W. Brown and E. T. Parker, More on order 10 turn-squares, *Ars Combin.*, **35** (1993) 125–127.

[16] A. Cayley, On Latin squares, *Oxford Camb. Dublin Messenger of Math.*, **19** (1890) 85–239.

[17] C. J. Colbourn and J. H. Dinitz (eds.), The CRC Handbook of Combinatorial Designs. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996. 753 pp.

[18] C. J. Colbourn and J. H. Dinitz, Mutually orthogonal Latin squares: a brief survey of constructions, *J. Statist. Plann. Inference*, **95** (2001) 9–48.

[19] A. Cruse, On embedding incomplete symmetric latin squares, *J. Comb. Theory Ser. A*, **16** (1974) 18–22.

[20] J. Dénes and A. D. Keedwell, Latin Squares and their Applications. Academic Press, New York-London, 1974.

[21] L. Euler, Recherches sur une nouvelle espèce de quarrés magiques, *Verhandelingen / uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen*, **9** (1782) 85–239.

[22] I. A. Faradžev, Constructive enumeration of combinatorial objects. Problèmes combinatoires et théorie des graphes, Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976, (CNRS Paris, 1978) pp131–135.

[23] R. A. Fisher and F. Yates, The 6×6 Latin squares, *Proc. Cambridge Philos. Soc.*, **30** (1934) 492–507.

[24] M. Frolov, Sur les permutations carrées, *J. de Math. spéc.*, **IV** (1890) 8–11, 25–30.

[25] P. Guérin, Private communication (2001).

[26] S. M. Jacob, The enumeration of the Latin rectangle of depth three by means of a formula of reduction, with other theorems relating to non-clashing substitutions and Latin squares, *Proc. London Math. Soc.*, **31** (1930) 329–354.

[27] M. T. Jacobson and P. Matthews, Generating uniformly distributed random Latin squares, *J. Combin. Des.*, **4** (1996) 405–437.

[28] G. Kolesova, C. W. H. Lam and L. Thiel, On the number of 8×8 Latin squares, *J. Combin. Theory Ser. A*, **54** (1990) 143–148.

[29] C. W. H. Lam, L. Thiel and S. Swiercz, The nonexistence of finite projective planes of order 10, *Canad. J. Math.*, **41** (1989) 1117–1123.

[30] P. A. MacMahon, Combinatory Analysis. Cambridge, 1915.

[31] B. M. Maenhaut and I. M. Wanless, Atomic Latin squares of order eleven, *J. Combin. Des.*, **12** (2004) 12–34.

[32] B. D. McKay, `nauty` graph isomorphic software, available at `http://cs.anu.edu.au/~bdm/nauty`.

[33] B. D. McKay, Isomorph-free exhaustive generation, *J. Algorithms*, **26** (1998) 306–324; also errata at `http://cs.anu.edu.au/~bdm/publications`.

[34] B. D. McKay and E. Rogoyski, Latin squares of order ten, *Electron. J. Combin.*, **2** (1995) #N3 (4 pp).

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

[36] W. Myrvold, Negative results for orthogonal triples of Latin squares of order 10, *J. Combin. Math. Combin. Comput.*, **29** (1999) 95–105.

[37] A. V. Nazarok, One more attempt to construct POLS$(10, 3)$ (Russian), Asymptotic methods in problems in the theory of random evolutions, Akad. Nauk Ukrain. SSR Inst. Mat., Kiev (1991) pp89–93.

[38] P. M. Neumann, A lemma that is not Burnside's, *Math. Sci.*, **4** (1979) 133–141.

[39] H. W. Norton, The 7×7 squares, *Ann. Eugenics*, **9** (1939) 269–307.

[40] E. T. Parker, Orthogonal latin squares, *Proc. Nat. Acad. Sci. U.S.A.*, **45** (1959) 859–862.

[41] E. T. Parker, Computer investigation of orthogonal Latin squares of order ten, Proc. Sympos. Appl. Math., Vol. XV, (Amer. Math. Soc., 1963) pp. 73–81.

[42] E. T. Parker, Nonexistence of a triple of orthogonal Latin squares of order 10 with group of order 25—a search made short, *J. Combin. Theory Ser. A*, **19** (1975) 243–244.

[43] D. A. Preece, Classifying Youden rectangles, *J. Royal Stat. Soc. Series B (Meth.)*, **28** (1966) 118–130.

[44] QSCGZ (pseudonym), Anonymous electronic posting to "loopforum", Oct. 2001. `http://groups.yahoo.com/group/loopforum/`

[45] R. C. Read, Every one a winner, *Annals Discrete Math.*, **2** (1978) 107–120.

[46] A. Sade, *Enumération des carrés latins. Application au* $7^{\text{ème}}$ *ordre. Conjectures pour les ordres supérieurs*, privately published, Marseille, 1948, 8pp.

[47] A. Sade, An omission in Norton's list of 7×7 squares. *Ann. Math. Stat.*, **22** (1951) 306–307.

[48] A. Sade, Morphismes de quasigroupes. Tables, *Univ. Lisboa Revista Fac. Ci. A* **13** (1970/71) 149–172.

[49] P. N. Saxena, A simplified method of enumerating Latin squares by MacMahon's differential operators; II. The 7×7 Latin squares, *J. Indian Soc. Agric. Statistics*, **3** (1951) 24–79.

[50] E. Schönhardt, Über lateinische Quadrate und Unionen, *J. Reine Angew. Math.*, **163** (1930) 183–230.

[51] J. Y. Shao and W. D. Wei, A formula for the number of Latin squares, *Discrete Math.*, **110** (1992) 293–296.

[52] S. S. Shrikhande, A note on mutually orthogonal Latin squares, *Sankhyā Ser. A*, **23** (1961) 115–116.

[53] G. Tarry, Le problème des 36 officiers, *Ass. Franç. Paris*, (1900) 29, 170-203.

[54] I. M. Wanless, Answers to questions by Dénes on Latin power sets, *Europ. J. Combin.*, **22** (2001) 1009–1020.

[55] M. B. Wells, The number of Latin squares of order eight, *J. Combinatorial Theory*, **3** (1967) 98–99.

Appendix: Counts by group size

In this appendix, we give counts of Latin squares according to the sizes of their autotopy and autoparatopy groups. The count in each case is the number of main classes. To obtain the number of isotopy classes corresponding to each entry, multiply the number of main classes by $6|\mathrm{Is}(L)|/|\mathrm{Par}(L)|$.

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
4	4	1

Table 6: Main classes of order 2 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
108	18	1

Table 7: Main classes of order 3 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
192	32	1	576	96	1

Table 8: Main classes of order 4 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
72	12	1	600	100	1

Table 9: Main classes of order 5 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
8	4	1	144	24	1
16	8	1	240	120	1
24	4	2	432	72	1
24	12	1	648	108	1
48	8	1	1296	216	1
72	36	1			

Table 10: Main classes of order 6 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
1	1	44	12	6	1
2	1	43	15	5	1
2	2	14	16	8	2
3	1	4	18	3	1
4	2	11	24	4	3
6	1	14	72	12	1
6	3	2	144	24	1
8	4	1	1008	168	1
10	5	1	1764	294	1
12	2	1			

Table 11: Main classes of order 7 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
1	1	270611	24	4	19
2	1	6769	24	8	2
2	2	4350	24	12	6
3	1	176	24	24	1
3	3	37	32	16	34
4	2	879	36	6	2
4	4	210	48	8	3
5	5	1	48	24	5
6	1	109	64	32	11
6	2	8	72	12	1
6	3	26	84	42	1
6	6	15	96	16	4
8	4	191	96	48	2
8	8	36	126	42	1
9	3	1	128	64	4
10	5	2	192	32	3
10	10	1	192	96	2
12	2	14	256	128	4
12	4	1	288	48	1
12	6	14	384	64	2
12	12	6	384	192	2
16	8	58	576	96	2
16	16	11	1536	256	3
18	3	8	3072	512	2
18	6	1	9216	1536	1
20	10	2	64512	10752	1
21	7	1			

Table 12: Main classes of order 8 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
1	1	19268330382	18	18	6
2	1	2106550	20	10	3
2	2	391327	21	7	4
3	1	12513	24	4	15
3	3	3105	24	12	13
4	2	6538	30	5	4
4	4	352	32	16	1
5	5	12	36	6	11
6	1	1158	36	18	12
6	2	87	48	8	1
6	3	824	54	9	2
6	6	168	60	10	1
7	7	5	72	12	2
8	4	150	72	36	4
8	8	1	96	16	1
9	3	6	96	48	1
9	9	4	108	18	2
10	5	20	108	54	2
10	10	1	162	27	1
12	2	63	168	56	1
12	6	125	216	36	1
12	12	8	216	108	1
14	7	1	324	54	1
16	8	10	432	72	1
18	3	27	972	486	1
18	6	6	2916	486	1
18	9	4	23328	3888	1

Table 13: Main classes of order 9 counted by group size

$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes	$\lvert\mathrm{Par}(L)\rvert$	$\lvert\mathrm{Is}(L)\rvert$	main classes
1	1	34817389393907137	24	24	1
2	1	5333019714	28	14	2
2	2	3162869555	30	5	6
3	1	1937530	32	16	31
3	3	199502	36	6	27
4	2	2364376	36	18	4
4	4	389128	40	20	25
5	5	386	40	40	4
6	1	28790	42	14	1
6	2	1210	42	21	3
6	3	8021	48	8	36
6	6	3144	48	16	1
7	7	52	48	24	3
8	4	16438	54	9	8
8	8	1510	60	10	1
9	3	126	63	21	3
9	9	6	72	12	13
10	5	86	80	40	8
10	10	68	96	16	8
12	2	616	96	48	2
12	4	200	100	50	4
12	6	816	100	100	1
12	12	148	108	18	1
14	7	5	108	54	1
14	14	6	120	20	1
15	5	11	144	24	1
16	8	528	144	72	1
16	16	30	160	80	1
18	3	136	200	100	4
18	6	6	288	48	3
18	9	2	324	54	1
18	18	1	400	200	2
20	10	52	432	72	1
20	20	22	1200	400	1
21	7	4	2400	400	1
24	4	254	2592	432	1
24	8	7	3000	500	1
24	12	102	12000	2000	1

Table 14: Main classes of order 10 counted by group size