The cycle structure of two rows in a random latin square

Nicholas J. Cavenagh and Catherine Greenhill*

School of Mathematics and Statistics
The University of New South Wales
NSW 2052 Australia

nickc@maths.unsw.edu.au, csg@unsw.edu.au

Ian M. Wanless†

School of Mathematical Sciences
Monash University
VIC 3800 Australia

ian.wanless@sci.monash.edu.au

Abstract

Let L be chosen uniformly at random from among the latin squares of order $n \geq 4$ and let r, s be arbitrary distinct rows of L. We study the distribution of $\sigma_{r,s}$, the permutation of the symbols of L which maps r to s. We show that for any constant $c > 0$, the following events hold with probability $1 - o(1)$ as $n \to \infty$:

(i) $\sigma_{r,s}$ has more than $(\log n)^{1-c}$ cycles,

(ii) $\sigma_{r,s}$ has fewer than $9\sqrt{n}$ cycles,

(iii) L has fewer than $\frac{9}{2}n^{5/2}$ intercalates (latin subsquares of order 2).

We also show that the probability that $\sigma_{r,s}$ is an even permutation lies in an interval $[\frac{1}{4} - o(1), \frac{3}{4} + o(1)]$ and the probability that it has a single cycle lies in $[2n^{-2}, 2n^{-2/3}]$. Indeed, we show that almost all derangements have similar probability (within a factor of $n^{3/2}$) of occurring as $\sigma_{r,s}$ as they do if chosen uniformly at random from among all derangements of $\{1, 2, \ldots, n\}$. We conjecture that $\sigma_{r,s}$ shares the asymptotic distribution of a random derangement.

Finally, we give computational data on the cycle structure of latin squares of orders $n \leq 11$.

*Supported by the UNSW Faculty Research Grants Scheme

†Supported by ARC grant DP0662946

1 Introduction

Any ordered pair (r, s) of distinct rows of a latin square L defines a permutation $\sigma_{r,s}$ which maps a symbol in r to the symbol in s which lies in the same column. The latin property implies that $\sigma_{r,s}$ is a derangement (that is, it has no fixed points). The purpose of this paper is to study $\sigma_{r,s}$ when L and (r, s) are chosen uniformly at random. In particular, we are interested in whether $\sigma_{r,s}$ asymptotically has the same distribution as a derangement chosen uniformly at random.

By symmetry, it suffices to focus on the row permutation $\sigma_{1,2}$ formed by the first two rows of the random latin square. Note that the number of extensions of a $2 \times n$ latin rectangle to an $n \times n$ latin square depends only on the cycle structure of the row permutation given by the first two rows. Hence the probability of $\sigma_{1,2}$ being a particular derangement d depends only on the cycle structure of d.

Jacobson and Matthews [7] designed a Markov chain whose stationary distribution is uniform over Latin squares of order n. They were not able to say how quickly their chain converges to its stationary distribution. One handicap to testing the convergence empirically is that very little is known about the structure of random latin squares.

McKay and Wanless [11] obtained some results about the distribution of intercalates (latin subsquares of order 2). They showed that with probability $1 - o(1)$ a random latin square has at least $n^{3/2-\epsilon}$ intercalates (for any fixed $\epsilon > 0$) and that the probability of there being no intercalates is $O\big(\exp(-n^{2-\epsilon})\big)$. In a later paper [12] the same authors showed that with probability $1 - o(1)$ a random latin square possesses no symmetry except the identity.

Cameron [1] showed that almost all $n \times n$ latin squares have the property that their rows, viewed as permutations, generate either the full symmetric group S_n or the alternating group A_n on n letters. (Here the columns are labelled with the same set as the symbols, so that row r maps j to e if and only if symbol e occurs in column j of row r.) It was subsequently shown by Häggkvist and Janssen [5] that the second of these possibilities can be ignored. They showed that the proportion of all-even $n \times n$ latin squares is $o(c^n)$ for some constant $c < 1$, where a latin square is called *all-even* if every row is an even permutation.

The results outlined above are the only prior results on the structure of random latin squares of which the present authors are aware.

An algorithm for generating random latin rectangles is given by McKay and Wormald [13]. Structural results for random $k \times n$ latin rectangles (with k much smaller than n) are fairly easy to obtain by switchings (see, for example, [4] and [11]). Some of this information can then be used to deduce properties of random latin squares (this is how the results quoted above from [11] were obtained). Unfortunately, much accuracy is lost because of the uncertainty in the number of extensions of a latin rectangle to a latin square. In this paper we avoid this problem by doing the switchings within latin squares themselves. This requires the use of more complicated switchings. First, in Section 2, we cover the basic definitions and notation which are used throughout the paper. Our switchings are described in Section 3.

The number of cycles in a random permutation of n symbols has a distribution which is asymptotically normal with mean and variance asymptotic to $\log n$, see Kolchin [8].

The same is known to be true for the number of cycles in a random derangement of n symbols, by the results of Flajolet and Soria [3]. We expect that this also holds for the number of cycles in $\sigma_{1,2}$ for a random $n \times n$ latin square. We have proved that for any constant $c > 0$, with probability which tends to 1, a random $n \times n$ latin square has between $(\log n)^{1-c}$ and $9\sqrt{n}$ cycles in the row permutation $\sigma_{1,2}$. These and other results are described in Section 4. In Section 5 we give data on the cycle structure of latin squares for orders $n \leq 11$. Finally, in Section 6 we formally state a conjecture which predicts that the distribution of $\sigma_{1,2}$ tends toward that of a random derangement as $n \to \infty$, and briefly explore the implications of this conjecture for the character theory of quasigroups.

2 Definitions

In this section we define the terminology and notation which will be used throughout the paper.

A *latin square of order* n is a matrix of order n in which each one of n symbols appears exactly once in each row and exactly once in each column. In this paper we assume that the symbol set is $[n] = \{1, 2, \ldots, n\}$, so that it coincides with the set of indices of the rows and columns. Since it will usually be clear from context which latin square we are dealing with, we will frequently use the notation $i \circ j$ for the symbol in row i and column j of a latin square. It is often convenient to think of a latin square of order n as a set of n^2 triples of the form $(i, j, i \circ j)$, where i is a row and j is a column. In particular, thinking of a latin square as a set allows us to use set notation and terminology.

A *partial latin square* Q of order n is an $n \times n$ array of symbols from the set $[n]$, where each symbol occurs at most once in each row and at most once in each column, with empty cells allowed. If there are no empty cells then Q is a latin square. As for latin squares we may denote Q as a set of ordered triples (elements) of the form $(i, j, i \circ j)$, where symbol $i \circ j$ occurs in row i and column j. The definition of Q above does not require that $Q \subseteq L$ for some latin square L of the same order as Q, but all partial latin squares in this paper will have that property.

A $k \times \ell$ *latin rectangle* is a $k \times \ell$ matrix in which each of ℓ symbols occurs exactly once in each row and at most once in each column. A *latin subrectangle* is a submatrix which is a latin rectangle. If $k = \ell$ then the latin subrectangle is called a *latin subsquare*, and a 2×2 latin subsquare is called an *intercalate*.

If R is a $2 \times m$ latin subrectangle of some latin square and R is minimal in that it contains no $2 \times m'$ latin subrectangle for $2 \leq m' < m$, then we say that R is a *row cycle* of length m.

Another way to think of row cycles is in terms of the permutation which maps one row to another row. Suppose that r and s are two rows of a latin square. We define a permutation $\sigma_{r,s} : [n] \mapsto [n]$ by $\sigma_{r,s}(r \circ j) = s \circ j$ for each $j \in [n]$. The latin property ensures that $\sigma_{r,s}$ is a *derangement*, meaning that every cycle has length at least 2. Each row cycle on r and s corresponds to a cycle of the permutation $\sigma_{r,s}$ and vice versa. If c is a cycle of $\sigma_{r,s}$ then we find the corresponding row cycle by taking all occurrences in r and s of symbols which occur in c.

A *column cycle* is a set of elements which forms a row cycle when the square is transposed. Thus $\sigma_{r,s}$ may also be defined if r and s are columns. (The context will make it clear whether r and s are rows or columns.) Row cycles and column cycles will collectively be known as *cycles*.

For the remainder of the paper we will consider latin squares of order $n \geq 4$ exclusively and $m = m(n)$ will be some integer between 4 and n. We say that a partial latin square F of order n is *suitable* if

- every cell in the first m columns of F is empty,
- no cell in the final $n - m$ columns of F is empty,
- the first two rows of F contain the same symbols.

This final condition on F means that the first two rows of F consist of entire row cycles (rather than fragments of row cycles). To illustrate, the first partial latin square shown below is suitable (with $m = 4$) but the second is not.

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

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

Any permutation of $[n]$ can be written as a product of disjoint cycles in the standard way. The lengths of these cycles define a partition of n which we call the *cycle structure* of the permutation.

If L is a latin square containing F then we use $\rho(L) = \rho(L, m)$ to denote the partition of m derived from the row cycles in the first two rows of $L \setminus F$. This gives a partition of m which has no part of size 1. Let $P(m)$ be the set of all such partitions.

Fix a suitable partial latin square F of order n. For each $\lambda \in P(m)$, let $S(\lambda, F)$ be the set of latin squares L such that $F \subseteq L$ and $\rho(L) = \lambda$. In the next section we estimate the relative sizes of the sets $S(\lambda, F)$ using switchings.

Then we consider the set $\Omega(F) = \bigcup_{\lambda \in P(m)} S(\lambda, F)$ consisting of all latin squares which contain F. Using uniform measure on this set we form a probability space which, by slight abuse of notation, we also denote $\Omega(F)$. All probabilities will be calculated in $\Omega(F)$, and we use $\mathbb{P}_F(\cdot)$ to denote such probabilities. In the particular case when $m = n$ and F is empty, $\Omega = \Omega(F)$ accords with the most obvious notion of random latin squares. However, stating our results in terms of F makes it possible to find probabilities which are conditional on certain structures being present in the last $n - m$ columns of the square. This extra generality may prove useful in some applications.

For a partition $\lambda \in P(n)$ we use $\kappa(\lambda)$ to denote the number of parts in λ. Since none of our partitions have parts of size 1, we will write $\lambda = (2^{\lambda_2}, 3^{\lambda_3}, 4^{\lambda_4}, \ldots, n^{\lambda_n})$ to signify that λ has λ_i parts of size i, for $i = 2, 3, \ldots, n$. If $\lambda_i = 0$ then we may omit i^{λ_i} from the list, and if $\lambda_i = 1$ then we will write i instead of i^1.

Let $\mathcal{D}_n$ be the set of derangements of $[n]$, and let $\gamma(\lambda)$ denote the number of derangements with cycle structure λ. It is elementary that if $\lambda = (2^{\lambda_2}, 3^{\lambda_3}, 4^{\lambda_4}, \ldots, n^{\lambda_n}) \in P(n)$ then

$$\gamma(\lambda) = \frac{n!}{\prod_{i=2}^{n} \lambda_i!\, i^{\lambda_i}}. \tag{1}$$

We use $\mathbb{Q}_n$ to denote the uniform probability distribution on $\mathcal{D}_n$. Hence $\mathbb{Q}_n(\lambda) = \gamma(\lambda)/|\mathcal{D}_n|$ is the probability of a random member of $\mathcal{D}_n$ having cycle structure λ.

Define a metric on $P(n)$ as follows. Let Γ_n be the graph with vertex set $P(n)$ and with an edge between two partitions $\lambda, \mu \in P(n)$ if and only if λ can be formed by splitting one part of μ into two parts, or vice versa. We then define the distance $d(\lambda, \mu)$ between arbitrary partitions $\lambda, \mu \in P(n)$ to be the length of the shortest path in Γ_n between the vertices corresponding to λ and μ.

3 Switchings

Let $\mu, \lambda \in P(m)$ with $d(\mu, \lambda) = 1$. We will assume that μ is obtained from λ by splitting one part of size $\alpha + \beta$ into two parts of size α and β. In this section we describe how to switch between sets $S(\mu, F)$ and $S(\lambda, F)$ via *latin trades*. Our aim is to approximate the ratio $|S(\mu, F)|/|S(\lambda, F)|$.

A partial latin square Q of order n is said to be a *latin trade* if there exists a partial latin square Q' (also of order n) such that:

- Q and Q' occupy the same set of non-empty cells,
- if $(i, j, k) \in Q$ and $(i, j, k') \in Q'$, then $k \neq k'$ (that is, Q and Q' are *disjoint*),
- for each $i \in [n]$, the set of symbols in row i of Q is equal to the set of symbols in row i of Q' (row i is *balanced*), and
- for each $j \in [n]$, the set of symbols in column j of Q is equal to the set of symbols in column j of Q' (column j is *balanced*).

The partial latin square Q' is called a *disjoint mate* of Q. The choice of Q' may not be unique. We thus sometimes refer to the pair (Q, Q') as a *latin bitrade*. Note that if Q is a latin trade within a latin square L, then $(L \setminus Q) \cup Q'$ is also a latin square. Thus latin trades describe the "difference" between two latin squares of the same order. It is also useful to note that if (Q, Q') is a latin bitrade, then (Q', Q) is also a latin bitrade. In this sense latin trades are always "reversible"; an important property for the switching process below.

Lemma 3.1. *Any row cycle R is a latin trade, with a unique disjoint mate obtained by swapping the symbols in each column of R. Similarly any column cycle is also a latin trade, with a unique disjoint mate obtained by exchanging the symbols in each row.*

For an analysis of how latin squares of order $n \leq 8$ are connected by the trades in Lemma 3.1 see [15].

Given a column j of a latin square L, we define $\omega_L(j) = \omega(j) \neq j$ to be the column such that $1 \circ \omega(j) = 2 \circ j$:

	j	$\omega(j)$
1	e_1	e_2
2	e_2	e_3

We may define a similar function for any ordered pair of columns j and j'. Let $\delta_{j,j'}$ be the permutation of the rows of the latin square given by: $\delta_{j,j'}(i) = i'$, where $i \circ j' = i' \circ j$.

Next, let j, j' be two columns in a latin square L such that $j' \notin \{j, \omega(j), \omega^{-1}(j)\}$. We identify the pair $\{j, j'\}$ as either an A-pair or a B-pair as follows. Consider the column cycles of $\{j, j'\}$. If rows 1 and 2 belong to different cycles then $\{j, j'\}$ is an A-pair. Otherwise rows 1 and 2 belong to the same cycle and $\{j, j'\}$ is a B-pair.

For example, the left and right diagrams below illustrate an A-pair of columns and a B-pair of columns, respectively. A double line is used between rows 2 and 3 of the latin square for clarity.

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

A

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

B

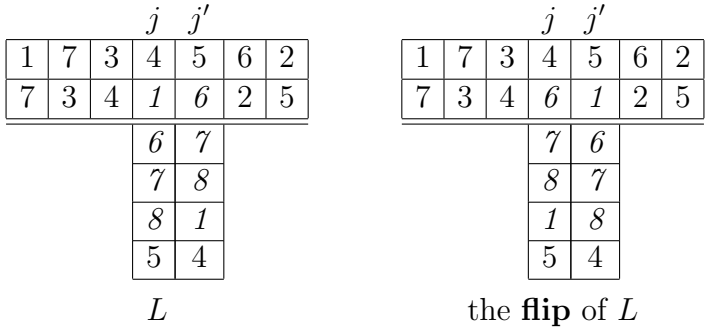
Definition 3.2. Let $L \in S(\mu, F)$ and let (j, j') be an A-pair of columns that belong to different row cycles in rows 1 and 2. Suppose furthermore that j and j' belong to row cycles of length α and β, respectively. Let Q be the column cycle within columns $\{j, j'\}$ that includes row 2 and let Q' be its unique disjoint mate. Let L' be the latin square defined by $L' = (L \setminus Q) \cup Q'$. We say that L' is the **flip** of L (with respect to columns j, j').

In the following lemma $(\omega')^\beta$ denotes the map formed by taking β iterations of ω'. Such notation will subsequently be used without further comment.

Lemma 3.3. *Let $L \in S(\mu, F)$ and let L' be the* **flip** *of L with respect to columns j, j' where $1 \leq j, j' \leq m$. Then $L' \in S(\lambda, F)$ and $(\omega')^\beta(j) = j'$, where $\omega' = \omega_{L'}$.*

Proof. The fact that $L' \in S(\lambda, F)$ follows from the definition of the flip operation. Let $i \circ' j$ denote the symbol in cell (i, j) of L'. Then $2 \circ j = 2 \circ' j'$ and $2 \circ' j = 2 \circ j'$, while every other symbol in rows 1 and 2 is the same in L as in L'. It follows that $\omega'(j) = \omega(j')$ and $\omega'(j') = \omega(j)$, with $\omega(c) = \omega'(c)$ for any other column c. Thus $(\omega')^\beta(j) = (\omega')^{\beta-1}(\omega(j')) = \omega^\beta(j') = j'$. Similarly, $(\omega')^\alpha(j') = j$. This implies that j and j' belong to a row cycle of length $\alpha + \beta$ in L'. □

The following example demonstrates Lemma 3.3 in action with $\alpha = 4$ and $\beta = 3$. The latin trade Q and its disjoint mate Q' are shown in italics.



Definition 3.4. Let $L \in S(\lambda, F)$ and let (j, j') be an A-pair of distinct columns that belong to the same cycle of length $\alpha + \beta$ in rows 1 and 2. Suppose furthermore that $\omega^\beta(j) = j'$. Let Q be the cycle of column pair $\{j, j'\}$ that includes row 2 and let Q' be its unique disjoint mate. Let $L' = (L \setminus Q) \cup Q'$. We say that L' is the **backflip** of L (with respect to columns j, j').

Lemma 3.5. *Let L' be the* **backflip** *of $L \in S(\lambda, F)$ with respect to columns j, j' with $1 \le j, j' \le m$. Then $L' \in S(\mu, F)$. Moreover, suppose we can apply the* **flip** *(respectively,* **backflip***) operation to a latin square L with respect to a pair of columns $\{j, j'\}$ to obtain a latin square L'. Then if we apply the* **backflip** *(respectively,* **flip***) operation to L' (again with respect to columns $\{j, j'\}$), we obtain our original latin square L.*

Proof. Observe that the **backflip** operation is the exact inverse of the **flip** operation. □

The above results describe how to join and split cycles within rows 1 and 2 across A-pairs of columns. The next lemmas describe ways to change columns between A-pairs and B-pairs, under certain conditions.

Definition 3.6. Let $L \in S(\mu, F)$. Let Q_1 and Q_2 be two distinct row cycles in the first m columns of rows 1 and 2. Suppose that column j belongs to cycle Q_1 and column j' belongs to cycle Q_2. Without loss of generality, suppose Q_1 contains a symbol that is smaller than every symbol in Q_2. Let Q_1' be its unique disjoint mate and let L' be the latin square given by $(L \setminus Q_1) \cup Q_1'$. We say that L' is the **switch** of L (with respect to columns j and j').

Lemma 3.7. *Let $L \in S(\mu, F)$ and let L' be the* **switch** *of L with respect to columns j and j', where $1 \le j, j' \le m$. Then $L' \in S(\mu, F)$ and $\{j, j'\}$ is an A-pair of columns in L if and only if it is a B-pair of columns in L', and vice versa.*

Proof. Replacing a row cycle in rows 1 and 2 with its disjoint mate does not change the lengths of any cycles in those rows. Thus L' still belongs to $S(\mu, F)$. However, $1 \circ j = 2 \circ' j$ and $1 \circ' j = 2 \circ j$ while $1 \circ j' = 1 \circ' j'$ and $2 \circ j' = 2 \circ' j'$. It follows that the pair $\{j, j'\}$ changes its status from an A-pair to a B-pair, or vice versa. □

The following diagram shows Lemma 3.7 in action. Note that Q_1 contains the smallest symbol (in this case, 1). Both Q_1 and Q_1' are shown in italics. The pair $\{j, j'\}$ is an A-pair in L and becomes a B-pair in the **switch** of L.

			j	j'		
1	*7*	*3*	*4*	5	6	2
7	*3*	*4*	*1*	6	2	5

6	7
7	8
8	1
5	4

L

			j	j'		
7	*3*	*4*	*1*	5	6	2
1	*7*	*3*	*4*	6	2	5

6	7
7	8
8	1
5	4

the **switch** of L

Corollary 3.8. *Suppose we can apply the* **switch** *operation to a latin square L with respect to a pair of columns $\{j, j'\}$ to obtain a latin square L'. Then if we apply the* **switch** *operation to L' (again with respect to columns $\{j, j'\}$), we obtain the latin square L.*

In Lemma 3.7 we showed that if we trade a cycle of rows 1 and 2, the B-pairs with exactly one column in this cycle become A-pairs; and vice-versa. Thus it is always possible to transform a B-pair into an A-pair when the columns of the pair belong to different row cycles. Now we describe an operation which can be performed when the columns of a B-pair belong to the same row cycle.

Definition 3.9. Let $L \in S(\lambda, F)$ and let (j, j') be a B-pair of distinct columns that belong to the same row cycle of length $\alpha + \beta$ in rows 1 and 2, where $\alpha, \beta \geq 2$. Suppose furthermore that $j' = \omega^\alpha(j)$. Let $(1, j, e_1), (1, j', e_2), (2, j, e_3), (2, j', e_4) \in L$. Note that e_1, e_2, e_3 and e_4 are pairwise distinct. Let $\delta = \delta_{j,j'}$ and let a and b be the smallest positive integers such that $\delta^a(1) = 2$ and $\delta^b(2) = 1$. We define a partial latin square $Q \subset L$ as follows. Firstly suppose that $\min(e_1, e_2, e_3, e_4) \in \{e_1, e_4\}$. Then let

$$Q = \big\{(2, j, e_3), (1, j', e_2)\big\} \cup \big\{(1, \omega^k(j), 1 \circ \omega^k(j)), (2, \omega^k(j), 2 \circ \omega^k(j)) \mid 1 \leq k < \alpha\big\}$$
$$\cup \big\{(\delta^k(1), j, \delta^k(1) \circ j), (\delta^k(1), j', \delta^k(1) \circ j') \mid 1 \leq k < a\big\}$$

and

$$Q' = \big\{(2, j, e_2), (1, j', e_3)\big\} \cup \big\{(1, \omega^k(j), 2 \circ \omega^k(j)), (2, \omega^k(j), 1 \circ \omega^k(j)) \mid 1 \leq k < \alpha\big\}$$
$$\cup \big\{(\delta^k(1), j, \delta^k(1) \circ j'), (\delta^k(1), j', \delta^k(1) \circ j) \mid 1 \leq k < a\big\}.$$

Otherwise $\min(e_1, e_2, e_3, e_4) \in \{e_2, e_3\}$. In this case we let

$$Q = \big\{(1, j, e_1), (2, j', e_4)\big\} \cup \big\{(1, \omega^k(j'), 1 \circ \omega^k(j')), (2, \omega^k(j'), 2 \circ \omega^k(j')) \mid 1 \leq k < \beta\big\}$$
$$\cup \big\{(\delta^k(2), j, \delta^k(2) \circ j), (\delta^k(2), j', \delta^k(2) \circ j') \mid 1 \leq k < b\big\}$$

and

$$Q' = \big\{(1, j, e_4), (2, j', e_1)\big\} \cup \big\{(1, \omega^k(j'), 2 \circ \omega^k(j')), (2, \omega^k(j'), 1 \circ \omega^k(j')) \mid 1 \leq k < \beta\big\}$$
$$\cup \big\{(\delta^k(2), j, \delta^k(2) \circ j'), (\delta^k(2), j', \delta^k(2) \circ j) \mid 1 \leq k < b\big\}.$$

Let $L' = (L \setminus Q) \cup Q'$. (In the above, $\circ$ is defined with respect to L rather than L'.) We say that L' is the **cross-switch** of L (with respect to columns j and j').

The following example shows the situation before and after a **cross-switch** operation. Here $\alpha = 3$ and $\beta = 4$. Note how the pair of columns $\{\omega^2(j), \omega(j')\}$ changes from an A-pair to a B-pair.

	j		$\omega^2(j)$	j'	$\omega(j')$	
1	2	*3*	*4*	*5*	6	7
2	*3*	*4*	*5*	6	7	1
	5		6	7	4	
	7		1	*3*	5	
	6		7	2	1	

L

	j		$\omega^2(j)$	j'	$\omega(j')$	
1	2	*4*	*5*	*3*	6	7
2	*5*	*3*	*4*	6	7	1
	7		6	5	4	
	3		1	*7*	5	
	6		7	2	1	

the **cross-switch** of L

Lemma 3.10. *Let $L \in S(\lambda, F)$ and let j, j', L', Q, Q' be as in the Definition* 3.9*, where $1 \leq j, j' \leq m$. Then (Q, Q') is a latin bitrade and $L' \in S(\lambda, F)$. Moreover, for any $1 \leq k < \alpha$ and $1 \leq k' < \beta$, the pair $\{\omega^k(j), \omega^{k'}(j')\}$ is an A-pair in L' if and only if it is a B-pair in L, and vice versa.*

Proof. We first show that (Q, Q') is a latin bitrade. We assume that $\min(e_1, e_2, e_3, e_4) \in \{e_1, e_4\}$; the other case is similar. It is easy to see that Q and Q' occupy the same set of non-empty cells and are disjoint.

Observe that $1 \circ \omega^\alpha(j) = 1 \circ j' = e_2$ and that for each k, $2 \circ \omega^k(j) = 1 \circ \omega^{k+1}(j)$ (by the definition of ω). In particular, $1 \circ \omega(j) = 2 \circ j = e_3$. It follows that row 1 contains the set of symbols

$$\{1 \circ \omega^k(j) \mid 1 \leq k \leq \alpha\}$$

in Q and Q'. Thus row 1 is balanced. Similarly, observing that $2 \circ \omega^0(j) = 2 \circ j = e_3$ and $2 \circ \omega^{\alpha-1}(j) = 1 \circ j' = e_2$, Q and Q' both contain the set of symbols

$$\{2 \circ \omega^k(j) \mid 0 \leq k < \alpha\}$$

in row 2. Every other row of Q contains two symbols, which are swapped in Q'.

Next we show that the columns of (Q, Q') are balanced. Consider column j. Observe that $\delta^a(1) \circ j = 2 \circ j = e_3$ and that for each k, $\delta^k(1) \circ j' = \delta^{k+1}(1) \circ j$ (by the definition of δ). In particular, $\delta(1) \circ j = 1 \circ j' = e_2$. It follows that column j contains the set of symbols

$$\{\delta^k(1) \circ j \mid 1 \leq k \leq a\}$$

in Q and Q'. Thus column j is balanced. Similarly column j' is balanced. The remaining columns of Q each contain two symbols, which are swapped in Q'.

Thus (Q, Q') is a latin bitrade. The fact that $L' \in S(\lambda, F)$ follows from the definition of the cross-switch operation. Next, if $1 \leq k < \alpha$ and $1 \leq k' < \beta$, then precisely one column from the pair $\{\omega^k(j), \omega^{k'}(j')\}$ has symbols swapped in rows 1 and 2 when the **cross-switch** operation is applied. The other column remains unchanged. Thus the pair $\{\omega^k(j), \omega^{k'}(j')\}$ changes from an A-pair to a B-pair, or vice-versa. □

Corollary 3.11. *Suppose we can apply the* **cross-switch** *operation to a latin square L with respect to a pair of columns $\{j, j'\}$ to obtain a latin square L'. Then if we apply the* **cross-switch** *operation to L' (again with respect to columns $\{j, j'\}$), we obtain the latin square L.*

In the following we need to distinguish carefully between the cases $\alpha \neq \beta$ and $\alpha = \beta$. In the former, using the notation from Section 2, μ has μ_α parts of size α, μ_β parts of size β and $\mu_{\alpha+\beta}$ parts of size $\alpha+\beta$, where $\mu_\alpha, \mu_\beta \geq 1$ and $\mu_{\alpha+\beta} \geq 0$. Thus λ has $\mu_\alpha - 1$ parts of size α, $\mu_\beta - 1$ parts of size β and $\mu_{\alpha+\beta} + 1$ parts of size $\alpha+\beta$. As $d(\mu, \lambda) = 1$, all other parts occur the same number of times in μ as in λ.

In the case that $\alpha = \beta$, μ has $\mu_\alpha \geq 2$ parts of size $\alpha (= \beta)$, and $\mu_{2\alpha} \geq 0$ parts of size 2α. Thus λ has $\mu_\alpha - 2$ parts of size α and $\mu_{2\alpha} + 1$ parts of size 2α. Again, all other parts occur the same number of times in μ as in λ.

We now use the latin trades defined in this section to obtain bounds for the ratio $|S(\lambda, F)|/|S(\mu, F)|$. To do this we define two bipartite multigraphs with edges between $S(\lambda, F)$ and $S(\mu, F)$. Each edge from $L \in S(\lambda, F)$ to $L' \in S(\mu, F)$ will correspond to some latin bitrade (Q, Q') such that $L' = (L \setminus Q) \cup Q'$. The first multigraph, $\mathcal{G}_S$, is defined with respect to $S(\lambda, F)$ (**Splitting**) and the second multigraph, $\mathcal{G}_J$, is defined with respect to $S(\mu, F)$ (**Joining**).

Splitting

Let $L \in S(\lambda, F)$. In each of the $\mu_{\alpha+\beta} + 1$ cycles of length $\alpha+\beta$ and for each of the $\alpha+\beta$ pairs of columns $\{j, j'\} \subset [m]$ such that $\omega^\alpha(j) = j'$ (or α such pairs if $\alpha = \beta$),

1. If $\{j, j'\}$ is an A-pair then **backflip** with respect to $\{j, j'\}$;
2. else if $\{j, j'\}$ is a B-pair and $\{\omega(j), \omega(j')\}$ is an A-pair then **backflip** with respect to $\{\omega(j), \omega(j')\}$;
3. otherwise $\{j, j'\}$ is a B-pair and $\{\omega(j), \omega(j')\}$ is a B-pair. In this case **cross-switch** with respect to $\{\omega(j), \omega(j')\}$. Now $\{j, j'\}$ has become an A-pair, and we **backflip** with respect to $\{j, j'\}$.
4. In each of 1 to 3 above we obtain a latin square $L' \in S(\mu, F)$, and we place an edge between L and L' in $\mathcal{G}_S$. Note that in each case we have backflipped with respect to a pair of columns which is an A-pair in L'.
5. Now **switch** L' with respect to $\{j, j'\}$ to obtain a latin square $L'' \in S(\mu, F)$. We also place an edge between L and L'' in $\mathcal{G}_S$.

Joining

Let $L \in S(\mu, F)$. For each of the $\mu_\alpha \mu_\beta$ pairs of cycles of length α and β (or $\mu_\alpha(\mu_\alpha - 1)/2$ pairs in the case $\alpha = \beta$) and for each of the $\alpha\beta$ pairs $\{j, j'\} \subset [m]$ of columns where column j belongs to the cycle of length α and column j' belongs to the cycle of length β,

1. If $\{j, j'\}$ is a B-pair, then **switch** with respect to $\{j, j'\}$. This ensures that $\{j, j'\}$ is an A-pair.
2. Next, **flip** with respect to $\{j, j'\}$ to create a latin square $L' \in S(\lambda, F)$. Place an edge between L and L' in $\mathcal{G}_J$.

3. If $\{\omega^{-1}(j), \omega^{-1}(j')\}$ is now a B-pair then add an extra edge between L and L' in $\mathcal{G}_J$; and

4. If $\{\omega(j), \omega(j')\}$ is now a B-pair, then **cross-switch** with respect to $\{\omega(j), \omega(j')\}$ to create a latin square $L'' \in S(\lambda, F)$. Place an edge between L and L'' in $\mathcal{G}_J$.

Lemma 3.12. *Let λ and μ be partitions such that $d(\lambda, \mu) = 1$, where μ may be obtained from λ by splitting one part of λ of size $\alpha+\beta$ to give two parts of μ of size α,β. If $\alpha \neq \beta$, then*

$$\frac{1}{2} \leq \frac{|S(\lambda, F)|}{|S(\mu, F)|} \frac{(\mu_{\alpha+\beta}+1)(\alpha+\beta)}{\mu_\alpha \mu_\beta \alpha\beta} \leq \frac{3}{2}.$$

Otherwise $\alpha = \beta$ and

$$\frac{1}{2} \leq \frac{|S(\lambda, F)|}{|S(\mu, F)|} \frac{2(\mu_{2\alpha}+1)}{\alpha\mu_\alpha(\mu_\alpha - 1)} \leq \frac{3}{2}.$$

Proof. From Lemma 3.5, Corollary 3.8 and Corollary 3.11, the bipartite multigraphs $\mathcal{G}_J$ and $\mathcal{G}_S$ are identical (that is, they have exactly the same multiset of edges). Write $\mathcal{G} = \mathcal{G}_J = \mathcal{G}_S$ and denote the number of edges in $\mathcal{G}$ (counting multiplicities) by Z. In $\mathcal{G}$, each vertex of $S(\lambda, F)$ has degree $2(\mu_{\alpha+\beta}+1)(\alpha+\beta)$ (or $2(\mu_{\alpha+\beta}+1)\alpha$ if $\alpha = \beta$), which implies that

$$Z = \begin{cases} 2(\mu_{\alpha+\beta}+1)(\alpha+\beta)\,|S(\lambda, F)| & \text{if } \alpha \neq \beta, \\ 2(\mu_{\alpha+\beta}+1)\alpha\,|S(\lambda, F)| & \text{if } \alpha = \beta. \end{cases} \tag{2}$$

Similarly, in $\mathcal{G}$ each vertex of $S(\mu, F)$ has some degree d such that $\mu_\alpha\mu_\beta\alpha\beta \leq d \leq 3\mu_\alpha\mu_\beta\alpha\beta$ (if $\alpha \neq \beta$), or $\mu_\alpha(\mu_\alpha-1)\alpha\beta/2 \leq d \leq 3\mu_\alpha(\mu_\alpha-1)\alpha\beta/2$ (if $\alpha = \beta$). This implies that

$$\begin{aligned} \mu_\alpha\mu_\beta\alpha\beta\,|S(\mu, F)| \leq Z \leq 3\mu_\alpha\mu_\beta\alpha\beta\,|S(\mu, F)| & \qquad \text{if } \alpha \neq \beta, \\ \mu_\alpha(\mu_\alpha-1)\alpha\beta/2\,|S(\mu, F)| \leq Z \leq 3\mu_\alpha(\mu_\alpha-1)\alpha\beta/2\,|S(\mu, F)| & \qquad \text{if } \alpha = \beta. \end{aligned}$$

The result follows by substituting (2) into the above inequalities. □

Theorem 3.13. *Let λ and μ be partitions such that $d(\lambda, \mu) = 1$, where μ may be obtained from λ by splitting one part of λ into two. Then,*

$$\frac{1}{2} \leq \frac{|S(\lambda, F)|}{|S(\mu, F)|} \Big/ \frac{\gamma(\lambda)}{\gamma(\mu)} \leq \frac{3}{2}.$$

Proof. Suppose that μ may be obtained from λ by splitting one part of λ of size $\alpha+\beta$ into two parts of size α and β. From equation (1) in the previous section, if $\alpha \neq \beta$ then

$$\frac{\gamma(\lambda)}{\gamma(\mu)} = \frac{\mu_\alpha\mu_\beta\alpha\beta}{(\mu_{\alpha+\beta}+1)(\alpha+\beta)}.$$

Similarly, if $\alpha = \beta$ then

$$\frac{\gamma(\lambda)}{\gamma(\mu)} = \frac{\mu_\alpha(\mu_\alpha-1)\alpha}{2(\mu_{2\alpha}+1)}.$$

The result then follows from Lemma 3.12. □

4 Properties of random latin squares

In this section we derive some properties of random latin squares. In Section 4.1 upper and lower bounds on various probabilities are calculated, and in Section 4.2 these are used to analyse the number of cycles in the row permutation formed by the first two rows of a random latin square.

4.1 Bounds on probabilities

To obtain bounds on the size of $S(\lambda, F)$, for $\lambda \in P(m)$, we will compare $S(\lambda, F)$ with $S((m), F)$, where (m) is the partition of m with one part.

Lemma 4.1. *Let $\lambda \in P(m)$. Then*

$$(2/3)^{\kappa(\lambda)-1} \leq \frac{|S(\lambda, F)|}{|S((m), F)|} \cdot \frac{(m-1)!}{\gamma(\lambda)} \leq 2^{\kappa(\lambda)-1}.$$

Proof. Let

$$(m) = p_0, p_1, \ldots, p_{\kappa(\lambda)-1} = \lambda$$

be a sequence of partitions, starting from (m) and ending at λ, such that for $1 \leq i \leq \kappa(\lambda) - 1$, the partition p_i is obtained from p_{i-1} by splitting one part of p_{i-1} into two. Then by Theorem 3.13 we have for $1 \leq i \leq \kappa(\lambda) - 1$,

$$\frac{\gamma(p_{i-1})}{2\gamma(p_i)} \leq \frac{|S(p_{i-1}, F)|}{|S(p_i, F)|} \leq \frac{3\gamma(p_{i-1})}{2\gamma(p_i)}.$$

Therefore

$$\begin{aligned}
\frac{|S((m), F)|}{|S(\lambda, F)|} &= \prod_{i=1}^{\kappa(\lambda)-1} \frac{|S(p_{i-1}, F)|}{|S(p_i, F)|} \\
&\geq (1/2)^{\kappa(\lambda)-1} \prod_{i=1}^{\kappa(\lambda)-1} \frac{\gamma(p_{i-1})}{\gamma(p_i)} \\
&= (1/2)^{\kappa(\lambda)-1} \frac{\gamma((m))}{\gamma(\lambda)} \\
&= (1/2)^{\kappa(\lambda)-1} \frac{(m-1)!}{\gamma(\lambda)}.
\end{aligned}$$

Inverting this gives the upper bound. The lower bound is proved similarly. □

While the above result will be used most often, we can also prove something more general.

Lemma 4.2. *Let $\lambda, \mu \in P(m)$. Then*

$$(1/2)^{d(\lambda,\mu)} \leq \frac{|S(\lambda, F)|}{|S(\mu, F)|} \cdot \frac{\gamma(\mu)}{\gamma(\lambda)} \leq 2^{d(\lambda,\mu)}.$$

Proof. The proof is very similar to the proof of Lemma 4.1. There is a path from λ to μ in the graph Γ_n of length $d(\lambda, \mu)$, say

$$\lambda = p_0,\ p_1,\ \ldots,\ p_{d(\lambda,\mu)} = \mu.$$

For $1 \le i \le d(\lambda, \mu)$, the partition p_i is obtained from p_{i-1} by splitting one part of p_{i-1} into two or by joining two parts of p_{i-1} into one. If there are r splitting steps then we find that

$$\frac{|S(\lambda, F)|}{|S(\mu, F)|} \cdot \frac{\gamma(\mu)}{\gamma(\lambda)} \le (3/2)^r\, 2^{d(\lambda,\mu)-r} \le 2^{d(\lambda,\mu)}$$

and

$$\frac{|S(\lambda, F)|}{|S(\mu, F)|} \cdot \frac{\gamma(\mu)}{\gamma(\lambda)} \ge (1/2)^r\, (2/3)^{d(\lambda,\mu)-r} \ge (1/2)^{d(\lambda,\mu)}.$$

Here we have used the inequalities of Theorem 3.13 directly for a splitting step, but these inequalities must be inverted for a joining step. □

In subsequent results, recall that $\mathbb{P}_F$ refers to probability in the uniform space $\Omega(F)$.

Theorem 4.3. *Let $\Omega(F) = E \cup O$, where E (respectively, O) is the set of all latin squares $L \in \Omega(F)$ such that $\sigma_{1,2}(L)$ is an even (respectively, odd) permutation. Then as $m \to \infty$*

$$\tfrac{1}{4} - o(1) \le \mathbb{P}_F(E) \le \tfrac{3}{4} + o(1).$$

In particular $\frac{1}{7} \le \mathbb{P}_F(E) \le \frac{6}{7}$ for $m \ge 4$. Since $\mathbb{P}_F(O) = 1 - \mathbb{P}_F(E)$, the same results hold for $\mathbb{P}_F(O)$.

Proof. We build a multigraph on the whole of $\Omega(F)$ by applying every possible splitting and joining process from Section 3. (Note that, as in the proof of Lemma 3.12, the multigraph obtained from all splitting operations is equal to the multigraph obtained from all joining operations.)

Consider the degree of some $L \in \Omega(F)$. There are between $\frac{1}{2}m$ and m pairs $\{j, j'\}$ of distinct columns such that $j' \in \{\omega(j), \omega^{-1}(j)\}$. Every other pair of columns results in between 1 and 3 edges by either splitting or joining. Hence the degree of L is somewhere between $\binom{m}{2} - m = \frac{1}{2}m(m-3)$ and $3\big(\binom{m}{2} - \frac{1}{2}m\big) = \frac{1}{2}m(3m-6)$.

Now regardless of whether we split or join, the parity of $\sigma_{1,2}(L)$ changes, which means that our multigraph is bipartite, with every edge joining a vertex in E to a vertex in O. It follows that

$$\frac{m-3}{3m-6}\,|E| \le |O| \le \frac{3m-6}{m-3}\,|E|.$$

This implies that

$$\frac{m-3}{4m-9} \le \frac{|E|}{|E|+|O|} \le \frac{3m-6}{4m-9},$$

from which the result follows. □

Let $\mathbb{P}_F(\lambda) = |S(\lambda, F)|/|\Omega(F)|$ be the probability that a randomly chosen element of $\Omega(F)$ gives rise to the partition λ. Also, by a slight abuse of notation, let $\kappa(\pi)$ denote the number of cycles in the cycle decomposition of the permutation π.

Lemma 4.4. *Let $m \geq 4$. The probability that the first two rows and first m columns of a random element of $\Omega(F)$ consist of a single m-cycle is bounded as follows:*

$$2m^{-2} \leq \mathbb{P}_F((m)) \leq 2m^{-2/3}.$$

Proof. Using Lemma 4.1, we have

$$\begin{aligned}
\mathbb{P}_F((m))^{-1} &= \sum_{\lambda \in P(m)} \frac{|S(\lambda, F)|}{|S((m), F)|} \\
&\leq \sum_{\lambda \in P(m)} \frac{\gamma(\lambda)}{(m-1)!}\, 2^{\kappa(\lambda)-1} \\
&= \frac{1}{2(m-1)!} \sum_{\pi \in \mathcal{D}_m} 2^{\kappa(\pi)}.
\end{aligned}$$

This sum can be evaluated using generating functions (for example by adapting [16, p.82]). If $h(m,k)$ denotes the number of derangements of m with k cycles then

$$\sum_{\pi \in \mathcal{D}_m} 2^{\kappa(\pi)} = \sum_k h(m,k)\, 2^k = m!\, [x^m]\, e^{-2x}\, (1-x)^{-2} \tag{3}$$

where $[x^m]f(x)$ denotes the coefficient of x^m in the Maclaurin series of $f(x)$. Now

$$\begin{aligned}
[x^m]e^{-2x}(1-x)^{-2} &= \sum_{i=0}^{m} \frac{(-2)^i}{i!} \binom{-2}{m-i} (-1)^{m-i} \\
&= \sum_{i=0}^{m} \frac{1}{i!}(-2)^i\, (m-i+1) \\
&\leq m.
\end{aligned}$$

To see this, write

$$\sum_{i=0}^{m} \frac{1}{i!}(-2)^i\, (m-i+1) = \sum_{i=0}^{m} (-1)^i t_i$$

where $t_i = 2^i(m-i+1)/i!$. Notice that $t_i > t_{i+1}$ for $1 \leq i < m$. So the whole sum is bounded above by $t_0 - t_1 + t_2 = m - 1$, which we bound above by m for simplicity. Therefore

$$\mathbb{P}_F((m))^{-1} \leq \frac{m!\, m}{2(m-1)!} = m^2/2$$

giving the stated lower bound.

For the upper bound we similarly find that

$$\mathbb{P}_F((m))^{-1} \geq \frac{3}{2(m-1)!} \sum_{\pi \in \mathcal{D}_m} (2/3)^{\kappa(\pi)}.$$

Replace 2 by 2/3 in (3) and calculate that

$$[x^m]e^{-2x/3}(1-x)^{-2/3} = \sum_{i=0}^{m} \frac{1}{i!}\,(-2/3)^i \binom{-2/3}{m-i} (-1)^{m-i}$$
$$= \sum_{i=0}^{m} (-1)^i t_i \tag{4}$$

where

$$t_i = \frac{2^i}{3^m} \cdot \frac{2 \cdot 5 \cdots (3(m-i)-1)}{i!\,(m-i)!}.$$

Since for $0 \le i < m$

$$\frac{t_{i+1}}{t_i} = \frac{2(m-i)}{(i+1)(3(m-i)-1)} < 1,$$

we can write

$$\sum_{i=0}^{m} (-1)^i t_i > t_0 - t_1 + t_2 - t_3 = g(m)\, t_0$$

where

$$g(m) = \frac{41m^3 - 174m^2 + 217m - 84}{3(3m-1)(3m-4)(3m-7)}.$$

Observing that

$$t_0 = (-1)^m \binom{-2/3}{m} = \frac{2 \cdot 5 \cdot 8 \cdots (3m-1)}{3 \cdot 6 \cdot 9 \cdots (3m)}$$

we introduce

$$u = \frac{1 \cdot 4 \cdot 7 \cdots (3m-2)}{2 \cdot 5 \cdot 8 \cdots (3m-1)} \quad \text{and} \quad v = \frac{3 \cdot 6 \cdot 9 \cdots (3m)}{4 \cdot 7 \cdot 10 \cdots (3m+1)}.$$

Then $t_0^2 > uv$ since

$$\Big(\frac{3k-1}{3k}\Big)^2 > \frac{3k-2}{3k-1}\,\frac{3k}{3k+1}$$

for all integers $k \ge 1$. Hence ${t_0}^3 > u t_0 v = 1/(3m+1)$ which implies that $t_0 > (3m+1)^{-1/3}$. This gives

$$\mathbb{P}_F((m))^{-1} \ge \frac{3m}{2} g(m)\, t_0 > \frac{3m}{2(3m+1)^{1/3}}\, g(8) \ge \tfrac{1}{2}\, m^{2/3}$$

whenever $m \ge 8$. Therefore $\mathbb{P}_F((m)) \le 2\, m^{-2/3}$ as required, provided that $m \ge 8$. For $4 \le m \le 7$ the same inequality can be verified by direct computation of (4). □

Corollary 4.5. *If $\lambda \in P(m)$ then*

$$3m^{-1}\,\frac{\gamma(\lambda)}{m!}\,\left(\frac{2}{3}\right)^{\kappa(\lambda)} \le \mathbb{P}_F(\lambda) \le m^{1/3}\,\frac{\gamma(\lambda)}{m!}\,2^{\kappa(\lambda)}.$$

Proof. For the lower bound, combine the lower bounds of Lemma 4.4 and Lemma 4.1 to give

$$\begin{aligned}\mathbb{P}_F(\lambda) &= \mathbb{P}_F((m))\,\frac{|S(\lambda,F)|}{|S((m),F)|} \\ &\geq 2m^{-2}\frac{\gamma(\lambda)}{(m-1)!}\,(2/3)^{\kappa(\lambda)-1} \\ &= 3m^{-1}\,\frac{\gamma(\lambda)}{m!}\,(2/3)^{\kappa(\lambda)}\end{aligned} \tag{5}$$

as claimed. The upper bound is proved similarly. □

An interesting aspect of Corollary 4.5 is that $\gamma(\lambda)/m!$ is the proportion of permutations of $[m]$ which have cycle type λ. This leads us to our next observation.

Corollary 4.6. *If $\lambda \in P(m)$ and $\kappa(\lambda) \leq \frac{6}{5}\log m$ then*

$$m^{-3/2} \leq \frac{\mathbb{P}_F(\lambda)}{\mathbb{Q}_m(\lambda)} \leq m^{3/2}.$$

Proof. By definition $\mathbb{Q}_m(\lambda) = \gamma(\lambda)/|\mathcal{D}_m| = (\gamma(\lambda)/m!)(m!/|\mathcal{D}_m|)$. Standard theory on derangements gives that for $m \geq 4$,

$$\frac{1}{3} = \frac{|\mathcal{D}_3|}{3!} < \frac{|\mathcal{D}_m|}{m!} < 1.$$

This allows us to rewrite Corollary 4.5 as

$$m^{-1}\left(\frac{2}{3}\right)^{\kappa(\lambda)} \leq \frac{\mathbb{P}_F(\lambda)}{\mathbb{Q}_m(\lambda)} \leq m^{1/3}\,2^{\kappa(\lambda)}.$$

The result now follows, since $\frac{6}{5}\log\frac{2}{3} - 1 > -\frac{3}{2}$ and $\frac{6}{5}\log 2 + \frac{1}{3} < \frac{3}{2}$. □

Since the number of cycles in a random derangement of $[m]$ is asymptotically normal with mean and variance asymptotic to $\log m$, as $m \to \infty$ (see [3]), it follows using Chebyshev's inequality that all but a vanishing proportion of derangements of $[m]$ satisfy the hypothesis $\kappa(\lambda) < \frac{6}{5}\log m$. Thus Corollary 4.6 shows that almost all derangements of $[m]$ have the same probability, to within a multiplicative factor of $m^{3/2}$, of occurring as a random derangement as they have of occurring as the permutation between rows 1 and 2 within the first m columns of a random element of $\Omega(F)$.

It is not obvious that the upper bound given in Corollary 4.5 is nontrivial. So we also prove the next result, which is weaker but more transparent.

Lemma 4.7. *Let $\lambda \in P(m)$. Then*

$$\mathbb{P}_F(\lambda) \leq 16\,m^{-2/3}\,\left(\frac{3}{4}\right)^{\kappa(\lambda)}.$$

Proof. Again we form a sequence of partitions, starting with (m) and ending up at λ:

$$(m) = p_0,\, p_1,\, \ldots, p_{\kappa(\lambda)-1} = \lambda.$$

However, this time we insist that p_{i+1} is formed from p_i in a particular way: we always split the *largest* part of p_i and we split it to produce the smallest part in λ which is not yet present in p_i (counting multiplicities). For example, to produce $\lambda = (2^2, 3, 4^2) \in P(15)$ we have the sequence

$$(m) = (15),\ (2, 13),\ (2^2, 11),\ (2^2, 3, 8),\ (2^2, 3, 4^2) = \lambda.$$

Let $\ell_i = |S(p_i, F)|/|S(p_{i+1}, F)|$. We will argue that $\ell_i \geq 4/3$ except in a few cases. Suppose that a part of size $\alpha + \beta$ in p_i is split to give parts of size α and β in p_{i+1}, where without loss of generality $\alpha \leq \beta$. By our choice of cuts, p_i has exactly one part of size $\alpha + \beta$. Also, if $i < \kappa(\lambda) - 2$ (that is, if the step from p_i to p_{i+1} is not the last step) then $\beta \geq 2\alpha$. Using the lower bounds from Lemma 3.12 it then follows that $\ell_i \geq 4/3$ unless one of the following holds:

- $i < \kappa(\lambda) - 2$, $\alpha = 2$ and p_i has no parts of size 2, in which case $\ell_i \geq 2/3$;
- $i < \kappa(\lambda) - 2$, $\alpha = 3$ and p_i has no parts of size 3, in which case $\ell_i \geq 1$;
- $i = \kappa(\lambda) - 2$ and $\alpha \leq 4$, in which case $\ell_i \geq 3/5$.

None of these three cases can arise more than once on the path from (m) to λ. Even if all three arise then they contribute at worst $2/5$ instead of $(4/3)^3$ to the product $\prod_i \ell_i$. It follows that

$$\frac{|S((m), F)|}{|S(\lambda, F)|} = \prod_{i=0}^{\kappa(\lambda)-2} \ell_i \geq \frac{2}{5} \left(\frac{4}{3}\right)^{\kappa(\lambda)-4} = \frac{81}{640} \left(\frac{4}{3}\right)^{\kappa(\lambda)}.$$

Therefore, using the upper bound from Lemma 4.4,

$$\mathbb{P}_F(\lambda) = \mathbb{P}_F((m)) \frac{|S(\lambda, F)|}{|S((m), F)|} \leq 2m^{-2/3} \times \frac{640}{81} \left(\frac{3}{4}\right)^{\kappa(\lambda)}$$

leading to the stated bound. □

Corollary 4.8. *Suppose that $m \geq 12$. The most likely partition for the cycle structure of the row cycles of the first two rows and first m columns of a randomly chosen element of $\Omega(F)$ is either (m) or $(2, m-2)$.*

Proof. With notation and arguments as in Lemma 4.7 we form the sequence

$$(m) = p_0,\, p_1, \ldots, p_{\kappa(\lambda)-1} = \lambda.$$

Firstly suppose that λ has no parts of size 2. Then we have $\ell_i > 1$ for all $i \geq 0$ except the case $i = 0$, $\alpha = 3$, $\beta \leq 6$ (which cannot happen, as it implies $m \leq 9$). The case when λ has parts of size 2 works similarly except that we compare to $p_1 = (2, m-2)$ rather

than to $p_0 = (m)$. A case analysis reveals that $\lambda_i > 1$ for $i \geq 1$ except for the case when p_i has no parts of size 3, but $\alpha = 3$ and $\beta \leq 6$ (which given that $m \geq 12$ implies that λ has at least two parts of size 2 and hence $\ell_1 \geq 8/5$). It is thus easy to see $\prod_{i \geq 1} \ell_i > 1$ whenever λ has a part of size 2.

Applying (5) completes the proof. □

The condition $m \geq 12$ in Corollary 4.8 is necessary, since we cannot with our current results rule out the partition $(2, 3, 6)$ being as likely as $(2, 9)$ and more likely than (11). However, in the particular case $m = n \leq 11$ we will see in Section 5 that the most likely partition is always (m), which is also the most common partition in $\mathcal{D}_n$.

4.2 Asymptotic results

Throughout this section we assume that $m = m(n) \to \infty$ as $n \to \infty$. We work with a sequence (F_n) of suitable partial latin squares and we are interested in the sequence of probability spaces given by $(\Omega(F_n))$. In the special case that $m = n \to \infty$ and $F_n = \emptyset$ for all n, we obtain asymptotic results about uniformly random $n \times n$ latin squares.

Order notation $O(\cdot)$, $o(\cdot)$ will be for $n \to \infty$ and uniform over all sequences $(m(n))$ and (F_n). Some further comments about $O(\cdot)$ are required. We will only write $f = O(g)$ when $g(m)$ has no zeroes at integer points $m \geq 4$. In this case, if $f(m) \leq cg(m)$ for all sufficiently large m (where c is a constant) then there exists a constant C such that $f(m) \leq Cg(m)$ for all $m \geq 4$. In turn this implies that $f = O(g)$ where f and g are considered as functions of n and where $m(n) \to \infty$, regardless of how slowly.

We first prove that a randomly chosen element of $\Omega(F_n)$ is unlikely to have many row cycles within the first two rows and the first m columns.

Theorem 4.9. *Let (F_n) be a sequence of suitable partial latin squares where $n \to \infty$. The probability that a random element of $\Omega(F_n)$ has at least k row cycles within the first two rows and the first m columns is*

$$o\left(\left(\frac{3}{4}\right)^k \exp(\pi\sqrt{2m/3})\right).$$

In particular, there is a constant c with $0 < c < 1$ such that the probability that a random element of $\Omega(F_n)$ has at least $9\sqrt{m}$ such cycles is $o(c^{\sqrt{m}})$.

Proof. Let λ be a partition in $P(m)$ with at least k parts. Then Lemma 4.7 implies that

$$\mathbb{P}_{F_n}(\lambda) \leq 16m^{-2/3}\left(\frac{3}{4}\right)^k.$$

Hardy and Ramanujan [6] proved that the number of partitions of m is asymptotically equal to

$$\frac{1}{4m\sqrt{3}} \exp(\pi\sqrt{2m/3})$$

as $m \to \infty$. This will do as an (asymptotic) upper bound on the number of partitions with no parts of size 1 and at least k parts. Multiplying these together, the probability

that a random element of $\Omega(F_n)$ has at least k row cycles (within the first two rows and first m columns) is

$$O(m^{-5/3}) \left(\frac{3}{4}\right)^k \exp(\pi\sqrt{2m/3}),$$

proving the first statement. If $k = 9\sqrt{m}$ then this probability is $o(\exp(c'\sqrt{m}))$, where

$$c' = \pi\sqrt{2/3} - 9\log(4/3) < 0.$$

Putting $c = \exp(c')$ gives $0 < c < 1$ and completes the proof. □

In particular this implies that with probability $1-o(1)$ as $n \to \infty$, a randomly chosen element of $\Omega(F_n)$ should have one or more cycles of length at least $\sqrt{m}/9$ in the first two rows and m columns.

Corollary 4.10. *The probability that the total number of row cycles among all the rows of a random $n \times n$ latin square is at least $\frac{9}{2}n^{5/2}$ is $o(1)$. Hence the probability that a random $n \times n$ latin square has at least $\frac{9}{2}n^{5/2}$ intercalates is $o(1)$.*

Proof. The probability that two given rows of a random latin square have at least $9\sqrt{n}$ cycles is $o(n^{-2})$, by Theorem 4.9 with $F_n = \emptyset$ and $m = n \to \infty$. Since there are fewer than $\frac{1}{2}n^2$ pairs of distinct rows in the latin square, this implies the first statement. The second statement holds since every intercalate is a row cycle. □

Having obtained an upper bound on the likely number of cycles, we now seek a lower bound.

Theorem 4.11. *Let (F_n) be a sequence of suitable partial latin squares and let c be a positive constant. Then with probability $1 - o(1)$ as $n \to \infty$, a randomly chosen element of $\Omega(F_n)$ has more than $(\log m)^{1-c}$ cycles in the first two rows and first m columns.*

Proof. Let $K = (\log m)^{1-c}$ and let P_K be the probability that a randomly chosen element of $\Omega(F_n)$ has no more than K cycles in the first two rows and m columns. By Corollary 4.5,

$$P_K = \sum_{\substack{\lambda \in P(m) \\ \kappa(\lambda) \le K}} \mathbb{P}_{F_n}(\lambda) \le m^{1/3}\, 2^K \sum_{\substack{\lambda \in P(m) \\ \kappa(\lambda) \le K}} \frac{\gamma(\lambda)}{m!} = m^{1/3}\, 2^K\, p,$$

where p is the probability that a random permutation of $[m]$ is a derangement with at most K cycles.

Kolchin [8, Theorem 4.2.4] proves that whenever $k = o(\log m)$, the probability that a random permutation of $[m]$ has exactly k cycles is

$$f(k) = \frac{k}{m \log m} \frac{(\log m)^k}{k!} (1 + o(1)).$$

It is easy to check that

$$\frac{f(k+1)}{f(k)} = (1 + o(1)) \frac{\log m}{k}$$

and hence $f(k) \leq f(K)$ for all $k \leq K$ when m is large enough. Therefore, as derangements are asymptotically a non-zero fraction of all permutations,

$$p = O(1)\,\frac{K^2}{m\log m}\,\frac{(\log m)^K}{K!} = O(m^{-1})(\log m)^{\frac{1}{2}(1-3c)+cK}e^K,$$

using Stirling's formula. We deduce that

$$P_K = O(m^{-2/3})(\log m)^{\frac{1}{2}(1-3c)+cK}(2e)^K = O(m^{-2/3})\exp\big(o(\log m)\big) = o(1),$$

which proves the theorem. □

5 Computational results

In this section we report computational results for latin squares of small order. The aim is to give exact values for the probability of each possible cycle structure for each order $n \leq 11$. With regard to the results of the previous section we only consider here the case when $m = n$ and $F = \emptyset$.

For $n \leq 3$ there is only one possible cycle structure, which therefore has probability 1. Data for each partition $\lambda \in P(n)$ for $4 \leq n \leq 9$ is given in Table 1, whilst Table 2 gives data for $n \in \{10, 11\}$.

Suppose R is a $2 \times n$ latin rectangle. We say that an $n \times n$ latin square whose first two rows are R is a completion of R. The number of completions depends on the cycle structure λ of the two rows of R, but not otherwise on R. Also the completions of R fall into equivalence classes of size $(n-2)!$, where squares are equivalent if they differ only in the order of the rows after the first two. We define $C(\lambda)$ to be $1/(n-2)!$ times the number of completions for any R with cycle structure λ.

In the column headed $\mathbb{P}_n(\lambda)$ we give the probability of the first two rows of a randomly chosen latin square of order n having cycle structure λ. For comparison, in the column headed $\mathbb{Q}_n(\lambda)$ we give the probability $\mathbb{Q}_n(\lambda) = \gamma(\lambda)/|\mathcal{D}_n|$ of a random member of $\mathcal{D}_n$ having cycle structure λ.

The value of $\mathbb{Q}_n(\lambda)$ is easily calculated from (1). We next explain how $C(\lambda)$ and $\mathbb{P}_n(\lambda)$ were calculated. Note that they are related by

$$\mathbb{P}_n(\lambda) = \frac{\gamma(\lambda)C(\lambda)}{\displaystyle\sum_{\mu\in P(n)}\gamma(\mu)C(\mu)}.$$

Let S_n be the full symmetric group on $[n]$. There is a natural action of $S_n \times S_n \times S_n$ on the latin squares of order n found by considering these squares as sets of triples. The orbits of this action are called *isotopism classes* and the stabiliser of a latin square is called its *autotopism group*. The number of isotopism classes of latin squares is known [10] for each order $n \leq 10$ (the number of latin squares of order 11 is known [12], but the number of isotopism classes is not).

The probabilities $\mathbb{P}_n(\lambda)$ reported in Table 1 were calculated by two entirely independent methods. The first method used a program written by Meynert for her work in

λ	$C(\lambda)$	$\mathbb{P}_n(\lambda)$	$\mathbb{Q}_n(\lambda)$
(2^2)	2	$\frac{1}{2}$	$\frac{1}{3}$
(4)	1	$\frac{1}{2}$	$\frac{2}{3}$
$(2,3)$	4	$\frac{5}{14} \approx 0.357$	$\frac{5}{11} \approx 0.455$
(5)	6	$\frac{9}{14} \approx 0.643$	$\frac{6}{11} \approx 0.545$
(2^3)	224	$\frac{7}{98} \approx 0.071$	$\frac{3}{53} \approx 0.057$
(3^2)	192	$\frac{16}{98} \approx 0.163$	$\frac{8}{53} \approx 0.151$
$(2,4)$	176	$\frac{33}{98} \approx 0.337$	$\frac{18}{53} \approx 0.340$
(6)	168	$\frac{42}{98} \approx 0.429$	$\frac{24}{53} \approx 0.453$
$(2^2,3)$	55296	$\frac{252}{2206} \approx 0.1142$	$\frac{35}{309} \approx 0.1133$
$(3,4)$	54528	$\frac{497}{2206} \approx 0.2253$	$\frac{70}{309} \approx 0.2265$
$(2,5)$	55040	$\frac{602}{2206} \approx 0.2729$	$\frac{84}{309} \approx 0.2718$
(7)	54720	$\frac{855}{2206} \approx 0.3876$	$\frac{120}{309} \approx 0.3883$
(2^4)	258392064	$\frac{78855}{10890328} \approx 0.0072$	$\frac{15}{2119} \approx 0.0071$
$(2,3^2)$	252518400	$\frac{822000}{10890328} \approx 0.0755$	$\frac{160}{2119} \approx 0.0755$
$(2^2,4)$	254582784	$\frac{932310}{10890328} \approx 0.0856$	$\frac{180}{2119} \approx 0.0849$
(4^2)	252850176	$\frac{925965}{10890328} \approx 0.0850$	$\frac{180}{2119} \approx 0.0849$
$(3,5)$	251894784	$\frac{1967928}{10890328} \approx 0.1807$	$\frac{384}{2119} \approx 0.1812$
$(2,6)$	252952576	$\frac{2470240}{10890328} \approx 0.2268$	$\frac{480}{2119} \approx 0.2265$
(8)	252110848	$\frac{3693030}{10890328} \approx 0.3391$	$\frac{720}{2119} \approx 0.3398$
$(2^3,3)$	22710505439232	$\frac{3032179605}{160046713496} \approx 0.0189$	$\frac{315}{16687} \approx 0.0189$
(3^3)	22618103611392	$\frac{2684304560}{160046713496} \approx 0.0168$	$\frac{280}{16687} \approx 0.0168$
$(2,3,4)$	22645209169920	$\frac{18140769675}{160046713496} \approx 0.1133$	$\frac{1890}{16687} \approx 0.1133$
$(2^2,5)$	22679270326272	$\frac{10900833363}{160046713496} \approx 0.0681$	$\frac{1134}{16687} \approx 0.0680$
$(4,5)$	22606854291456	$\frac{21732052923}{160046713496} \approx 0.1358$	$\frac{2268}{16687} \approx 0.1359$
$(3,6)$	22613272363008	$\frac{24153580710}{160046713496} \approx 0.1509$	$\frac{2520}{16687} \approx 0.1510$
$(2,7)$	22646925230080	$\frac{31100818950}{160046713496} \approx 0.1943$	$\frac{3240}{16687} \approx 0.1942$
(9)	22610937544704	$\frac{48302173710}{160046713496} \approx 0.3018$	$\frac{5040}{16687} \approx 0.3020$

Table 1: Data for $4 \leq n \leq 9$

λ	$C(\lambda)$	$\mathbb{P}_n(\lambda)$	$\mathbb{Q}_n(\lambda)$
(2^5)	51411315765364654080	$\frac{3575078749235}{5020513457165912} \approx 0.00071$	$\frac{105}{148329} \approx 0.00071$
$(2^2, 3^2)$	51215051179356585984	$\frac{94971486795080}{5020513457165912} \approx 0.01892$	$\frac{2800}{148329} \approx 0.01888$
$(2^3, 4)$	51275576338789957632	$\frac{71312791977630}{5020513457165912} \approx 0.01420$	$\frac{2100}{148329} \approx 0.01416$
$(3^2, 4)$	51076163026198462464	$\frac{189427874450360}{5020513457165912} \approx 0.03773$	$\frac{5600}{148329} \approx 0.03775$
$(2, 4^2)$	51140368085911863296	$\frac{213374243141045}{5020513457165912} \approx 0.04250$	$\frac{6300}{148329} \approx 0.04247$
$(2, 3, 5)$	51143865047155998720	$\frac{455229511680720}{5020513457165912} \approx 0.09067$	$\frac{13440}{148329} \approx 0.09061$
(5^2)	51074806889452666880	$\frac{272768896656928}{5020513457165912} \approx 0.05433$	$\frac{8064}{148329} \approx 0.05437$
$(2^2, 6)$	51207824325532975104	$\frac{284874256673440}{5020513457165912} \approx 0.05674$	$\frac{8400}{148329} \approx 0.05663$
$(4, 6)$	51072884275767410688	$\frac{568247143316860}{5020513457165912} \approx 0.11319$	$\frac{16800}{148329} \approx 0.11326$
$(3, 7)$	51074461189093195776	$\frac{649445358137680}{5020513457165912} \approx 0.12936$	$\frac{19200}{148329} \approx 0.12944$
$(2, 8)$	51140258707024117760	$\frac{853495147107050}{5020513457165912} \approx 0.17000$	$\frac{25200}{148329} \approx 0.16989$
(10)	51072829020284387328	$\frac{1363791668479884}{5020513457165912} \approx 0.27164$	$\frac{40320}{148329} \approx 0.27183$
$(2^4, 3)$	366510690331559851950971289 6	$\frac{131415776701318605804}{55506181523176647910224} \approx 0.00237$	$\frac{3465}{1468457} \approx 0.00236$
$(2, 3^3)$	365467012743292378642435276 8	$\frac{465925534255529661236}{55506181523176647910224} \approx 0.00839$	$\frac{12320}{1468457} \approx 0.00839$
$(2^2, 3, 4)$	365807362817544774801476812 8	$\frac{1573963105880708302914}{55506181523176647910224} \approx 0.02836$	$\frac{41580}{1468457} \approx 0.02832$
$(3, 4^2)$	365106861548519559356900966 4	$\frac{1570949051859006624882}{55506181523176647910224} \approx 0.02830$	$\frac{41580}{1468457} \approx 0.02832$
$(2^3, 5)$	366153683895991618737537024 0	$\frac{630181290060088514748}{55506181523176647910224} \approx 0.01135$	$\frac{16632}{1468457} \approx 0.01133$
$(3^2, 5)$	365111398053264139600527360 0	$\frac{1675699809199651405170}{55506181523176647910224} \approx 0.03019$	$\frac{44352}{1468457} \approx 0.03020$
$(2, 4, 5)$	365450302348500649170173952 0	$\frac{3773824267499312011524}{55506181523176647910224} \approx 0.06799$	$\frac{99792}{1468457} \approx 0.06796$
$(2, 3, 6)$	365456049590709614456025907 2	$\frac{4193204018247818993496}{55506181523176647910224} \approx 0.07554$	$\frac{110880}{1468457} \approx 0.07551$
$(5, 6)$	365098975649071060261797888 0	$\frac{5026928387578452522783}{55506181523176647910224} \approx 0.09057$	$\frac{133056}{1468457} \approx 0.09061$
$(2^2, 7)$	365802134869851941243558297 6	$\frac{2698183905490885837608}{55506181523176647910224} \approx 0.04861$	$\frac{71280}{1468457} \approx 0.04854$
$(4, 7)$	365100174540312560437035008 0	$\frac{5386012387199840468655}{55506181523176647910224} \approx 0.09703$	$\frac{142560}{1468457} \approx 0.09708$
$(3, 8)$	365105915843241973828603084 8	$\frac{6283779931052691933096}{55506181523176647910224} \approx 0.11321$	$\frac{166320}{1468457} \approx 0.11326$
$(2, 9)$	365450560938441850244772659 2	$\frac{8386282084065682431712}{55506181523176647910224} \approx 0.15109$	$\frac{221760}{1468457} \approx 0.15102$
(11)	365099702147526238621872947 2	$\frac{13709831974085660596596}{55506181523176647910224} \approx 0.24700$	$\frac{362880}{1468457} \approx 0.24712$

Table 2: Data for $n = 10, 11$

[10]. For a given order, Meynert's program produces one representative of each isotopism class of latin square, together with the order of its autotopism group. Suppose that we consider one representative L of an isotopism class I, for which the autotopism group has order a. It is a simple matter to find all the row cycles in L and therefore to count, for each λ, the number $\#(L,\lambda)$ of (unordered) pairs of rows of L with have cycle structure λ. By the orbit-stabiliser theorem there are $n!^3/a$ squares in I. Moreover, of these squares, the proportion which have cycle structure λ between rows 1 and 2 is exactly $\#(L,\lambda)/\binom{n}{2}$. From the output of Meynert's program then, it is straightforward to calculate the probabilities $\mathbb{P}_n(\lambda)$ given in Table 1. The computation for the 115618721533 isotopism classes of order 9 took more than one GHz year. To corroborate the values quoted we checked that the results of the program were consistent with the total number of latin squares as known from [10], [12].

The second method was more powerful and allowed us to gather data for all $n \leq 11$. Thus we were able to independently verify the accuracy of Table 1, as well as finding the data in Table 2. The method made use of data collected in the computation [12] to count the latin squares of orders up to 11. That computation involved counting the 1-factorizations of all k-regular bipartite graphs on 22 or fewer vertices. From this information the number of $k \times n$ latin rectangles was calculated for $1 \leq k \leq n \leq 11$. Each rectangle R has an associated bipartite graph $G(R)$ which records the information required to find the number of completions of R to a latin square. Crucially, the function $G(\cdot)$ is many to one. This allowed the computation, which dealt solely with the graphs, to be fast enough to work for $n = 11$, but at the cost of not being able to extract all data (e.g. the number of isotopism classes) from the results.

Happily for our current purposes, we can infer the number of completions for each $2 \times n$ latin rectangle from the data generated by the computation in [12]. This is essentially because for $(n-2) \times n$ latin rectangles R the cycle structure of the two 'missing' rows can be inferred from $G(R)$. However, the completions for $k \times n$ rectangles (for $k > 2$) cannot be so easily recovered, because of the information lost by mapping R to $G(R)$.

In Theorem 4.3 we examined the probabilities $\mathbb{P}_F(O)$, $\mathbb{P}_F(E)$ of $\sigma_{1,2}$ being an odd (resp. even) permutation. The tables just given allow us to calculate these probabilities exactly in the case $m = n \leq 11$. The results are shown in Table 3.

To test the hypothesis that the number of completions of a $2 \times n$ latin rectangle becomes less sensitive to the structure of the rectangle as n grows, we calculated the following statistic for each n. Take the numbers of completions as listed in Tables 1 and 2, and find the standard deviation divided by the mean. The values of this statistic (which is called the coefficient of variation) for $n = 4, 5, \ldots, 11$ are approximately 0.33333, 0.20000, 0.11288, 0.00537, 0.00833, 0.00154, 0.00195 and 0.00117. From this it may be hypothesised that the trend is toward zero, but that odd and even values of n behave slightly differently. However, there are too few data points for this to be totally convincing. Another way to measure the spread of these values for each n is simply to take the maximum number of completions divided by the minimum number. This gives the approximate values 2.0000, 1.5000, 1.3333, 1.0141, 1.0258, 1.0046, 1.0066, 1.0039 for $n = 4, 5, \ldots, 11$.

n	$\mathbb{P}_F(O)$	$\mathbb{P}_F(E)$
4	$\frac{1}{2}$	$\frac{1}{2}$
5	$\frac{5}{14} \approx 0.3571429$	$\frac{9}{14} \approx 0.6428571$
6	$\frac{1}{2}$	$\frac{1}{2}$
7	$\frac{1099}{2206} \approx 0.4981868$	$\frac{1107}{2206} \approx 0.5018132$
8	$\frac{1361835}{2722582} \approx 0.5001998$	$\frac{1360747}{2722582} \approx 0.4998002$
9	$\frac{20004658047}{40011678374} \approx 0.4999705$	$\frac{20007020327}{40011678374} \approx 0.5000295$
10	$\frac{627568158293671}{1255128364291478} \approx 0.5000032$	$\frac{627560205997807}{1255128364291478} \approx 0.4999968$
11	$\frac{385459343334624914377}{770919187821897887642} \approx 0.4999997$	$\frac{385459844487272973265}{770919187821897887642} \approx 0.5000003$

Table 3: Probability of $\sigma_{1,2}$ being an odd/even permutation

6 A conjecture

The data given in Tables 1, 2 shows very good agreement between $\mathbb{P}_n$ and $\mathbb{Q}_n$ and leads us to conjecture that the cycle structure of a random derangement and the first two rows of a random latin square have asymptotically the same distribution. The *total variation distance* between two probability distributions σ, τ on the same underlying set A is defined by

$$d_{\mathrm{TV}}(\sigma, \tau) = \tfrac{1}{2} \sum_{x \in A} |\sigma(x) - \tau(x)| = \max_{B \subseteq A} |\sigma(B) - \tau(B)|.$$

Conjecture 6.1. *$d_{\mathrm{TV}}(\mathbb{P}_n, \mathbb{Q}_n) = o(1)$ as $n \to \infty$.*

The values of $d_{\mathrm{TV}}(\mathbb{P}_n, \mathbb{Q}_n)$ for $n = 4, 5, \ldots, 11$ are approximately 0.17, 0.097, 0.027, 0.0020, 0.0012, 0.00047, 0.00040, 0.00029.

In looser language, Conjecture 6.1 suggests that for large n the number of completions of a $2 \times n$ latin rectangle R to an $n \times n$ latin square is fairly insensitive to the choice of R. This may even be true for $k \times n$ latin rectangles for any fixed k, although we have no evidence to test that hypothesis.

If Conjecture 6.1 turned out to be true it would provide very accurate information on the cycle structure of random latin squares and thus, for example, give strong results on the distribution of intercalates. Another consequence would be the following, which was communicated to us by P. J. Cameron.

Lemma 6.2. *Conjecture 6.1 implies that for almost all reduced $n \times n$ latin squares, the group of permutations generated by the rows is the symmetric group S_n. This in turn implies that almost all loops have trivial character theory.*

We now explain what is meant by this lemma and why it is true.

A latin square on the symbol set $[n]$ is said to be *reduced* if its first row and column are in the natural order $1, 2, \ldots, n$. The rows of a latin square, considered as permutations, generate a transitive group. Łuczak and Pyber [9] showed that, for a proportion $1 - o(1)$ of

elements $g \in S_n$, the only transitive subgroups of S_n containing g are S_n and (possibly) A_n. Since $|\mathcal{D}_n|/|S_n|$ approaches $1/e > 0$, the same assertion holds if g is a random derangement. Now if Conjecture 6.1 is true then the second row of a random reduced latin square L is essentially a random derangement, so it would follow that the rows of L generate either S_n or A_n with probability $1 - o(1)$. A result of Häggkvist and Janssen [5] (mentioned in the introduction) implies that the chance of generating A_n is exponentially small. So the rows of almost all reduced latin squares would generate S_n.

Reduced latin squares correspond to algebras called loops, and in general latin squares correspond to quasigroups (see [10], for example, for details). Smith [14] has extended the character theory of groups to quasigroups. Cameron [1] showed that almost every quasigroup Q has trivial character theory by showing that the rows of Q generate either S_n or A_n. If Conjecture 6.1 is true, then this result on quasigroups also holds for loops (in either case, [5] shows that the group in question is almost never A_n).

For good estimates of the asymptotic probability that random permutations generate A_n or S_n, see [2].

References

[1] P. J. Cameron, Almost all quasigroups have rank 2, *Discrete Math.* **106/107**, (1992) 111-115.

[2] J. D. Dixon, Asymptotics of Generating the Symmetric and Alternating Groups, *Electron. J. Combin.* **12**, (2005) R56.

[3] P. Flajolet and M. Soria, Gaussian limiting distributions for the number of components in combinatorial structures, *J. Combinatorial Theory, Ser. A* **53**, (1990) 165–182.

[4] C. D. Godsil and B. D. McKay, Asymptotic enumeration of Latin rectangles, *J. Combinatorial Theory, Ser. B* **48**, (1990) 19–44.

[5] R. Häggkvist and J. C. M. Janssen, All-even latin squares, *Discrete Mathematics* **157** (1996), 199–206.

[6] G. H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc. Ser. 2* **17** (1918), 75–115.

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

[8] V.F. Kolchin, *Random graphs*, Cambridge University Press, Cambridge, 1999.

[9] T. Łuczak and L. Pyber, On random generation of the symmetric group, *Combin. Probab. Comput.* **2** (1993), 505–512.

[10] B. D. McKay, A. Meynert and W. Myrvold, Small Latin squares, quasigroups and loops, *J. Combin. Des.*, to appear.

[11] B. D. McKay and I. M. Wanless, Most latin squares have many subsquares, *J. Comb. Th. Ser. A* **86**, (1999) 323–347.

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

[13] B. D. McKay and N. C. Wormald, Uniform generation of random Latin rectangles, *J. Combin. Math. Combin. Comput.* **9**, (1991) 179–186.

[14] J. D. H. Smith, *An introduction to quasigroups and their representations*, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[15] I. M. Wanless, Cycle switching in Latin squares, *Graphs Combin.* **20** (2004), 545–570.

[16] H. S. Wilf, *Generatingfunctionology* (2nd edn.), Academic Press, San Diego, 1994.