Intercalates and Discrepancy in Random Latin Squares

Matthew Kwan * Benny Sudakov†

Abstract

An *intercalate* in a Latin square is a 2×2 Latin subsquare. Let $\boldsymbol{N}$ be the number of intercalates in a uniformly random $n \times n$ Latin square. We prove that asymptotically almost surely $\boldsymbol{N} \geq (1-o(1))\,n^2/4$, and that $\mathbb{E}\boldsymbol{N} \leq (1+o(1))\,n^2/2$ (therefore asymptotically almost surely $\boldsymbol{N} \leq fn^2$ for any $f \to \infty$). This significantly improves the previous best lower and upper bounds. We also give an upper tail bound for the number of intercalates in two fixed rows of a random Latin square. In addition, we discuss a problem of Linial and Luria on low-discrepancy Latin squares.

1 Introduction

A $n \times n$ *Latin square* is an $n \times n$ array of the numbers between 1 and n (we call these *symbols*), such that each row and column contains each symbol exactly once. Latin squares are a fundamental type of combinatorial design, and have many essentially equivalent formulations. In their various guises, Latin squares play an important role in many contexts, ranging from group theory, to projective geometry, to experimental design, to the theory of error-correcting codes. An introduction to the vast subject of Latin squares can be found in [11].

Since Erdős and Rényi's seminal paper on random graphs [5] and Erdős' popularization of the probabilistic method, there has been great interest in random combinatorial structures of all kinds, and of course it is natural to consider random Latin squares. In fact random Latin squares are of more than theoretical interest, due to the importance of randomization in experimental design (see for example [20]).

The simplest and most natural notion of a random Latin square is the uniform probability distribution over the set $\mathcal{L}$ of $n \times n$ Latin squares. Random Latin squares are very difficult to study: they lack independence or any kind of recursive structure, which rules out many of the techniques used to study binomial random graphs and random permutations, and there is little freedom to make local changes, which limits the use of "switching" techniques often used in the study of random regular graphs (see for example [14]). It is not even known how to efficiently generate a uniformly random $\boldsymbol{L} \in \mathcal{L}$. Jacobson and Matthews [9] and Pittenger [19] designed Markov chains on $\mathcal{L}$ which converge to the uniform distribution, but it is not known if these Markov chains converge rapidly.

Some of the earlier work on random Latin squares concerned algebraic properties (see for example [2, 7]). In this paper we are more interested in structural questions. An *intercalate* in a Latin square L is a 2×2 Latin subsquare. That is, it is a pair of rows i, j and a pair of columns x, y such that

*Department of Mathematics, ETH, 8092 Zürich. Email: matthew.kwan@math.ethz.ch.

†Department of Mathematics, ETH, 8092 Zürich. Email: benjamin.sudakov@math.ethz.ch. Research supported in part by SNSF grant 200021-149111.

$L_{i,x} = L_{j,y}$ and $L_{i,y} = L_{j,x}$. An important statistic of a Latin square L is the number $N(L)$ of intercalates that it contains. Clearly this number is at most n^3, because each of the n^2 entries in a Latin square can be involved in at most n intercalates. In a series of papers due to Kotzig, Lindner, McLeish, Rosa and Turgeon [12, 18, 13], it was proved that for all orders except 2×2 and 4×4 there exist Latin squares with no intercalates, and Heinrich and Wallis [8] proved that for all n there exist $n \times n$ Latin squares with $\Omega(n^3)$ intercalates.

In [17] McKay and Wanless conjectured the following.

Conjecture 1. *Let $\boldsymbol{N} = N(\boldsymbol{L})$ be the number of intercalates in a uniformly random Latin square $\boldsymbol{L} \in \mathcal{L}$. For any $\varepsilon > 0$, a.a.s.*[1]

$$(1-\varepsilon)\frac{n^2}{4} \le \boldsymbol{N} \le (1+\varepsilon)\frac{n^2}{4}.$$

They were able to prove the substantially weaker lower bound that a.a.s. $\boldsymbol{N} \ge n^{3/2-\varepsilon}$ for any $\varepsilon > 0$. Before our paper, the best upper bound was due to Cavenagh, Greenhill and Wanless [3], who proved that a.a.s. $\boldsymbol{N} \le (9/2)n^{5/2}$. The techniques used for these upper and lower bounds are very different, and we incorporate both to prove the following improved bounds. In particular we are able to prove the lower bound in Conjecture 1.

Theorem 1. *Let $\boldsymbol{N} = N(\boldsymbol{L})$ be the number of intercalates in a uniformly random Latin square $\boldsymbol{L} \in \mathcal{L}$. First,*

$$(1-o(1))\frac{n^2}{4} \le \mathbb{E}\boldsymbol{N} \le (1+o(1))\frac{n^2}{2}.$$

Second, for any fixed $\varepsilon > 0$ and any function $f \to \infty$, a.a.s.

$$(1-\varepsilon)\frac{n^2}{4} \le \boldsymbol{N} \le fn^2.$$

Theorem 1 is an immediate corollary of two theorems that may be of independent interest, which we discuss in Section 2.

A different property that likely holds a.a.s. for random Latin squares is that they have "low discrepancy" or are "quasirandom" in a certain sense. This is related to a conjecture by Linial and Luria [16]. To state their conjecture, note that $\mathcal{L}$ can more symmetrically be interpreted as the set of all $n \times n \times n$ zero-one arrays with a single "1" in each axis-aligned line. To be specific, an $n \times n$ Latin square L corresponds to the $n \times n \times n$ array $A = A(L)$ where $A_{i,x,q} = 1$ if $L_{i,x} = q$. A *box* is a set of the form $T = I \times X \times Q$, where $I, X, Q \subseteq [n]$. For a box T, define its *volume* $\operatorname{vol} T = |I||X||Q|$. Let $N_T(L)$ be the number of ones in $A(L)$ in the positions in the box T. Linial and Luria's conjecture is as follows.

Conjecture 2. *There exist arbitrarily large Latin squares L with the following property. For any box $T = I \times X \times Q$,*

$$\left| N_T(L) - \frac{\operatorname{vol} T}{n} \right| = O\left(\sqrt{\operatorname{vol} T}\right).$$

That is, Linial and Luria conjecture that there are Latin squares (zero-one arrays) such that in any box, the density of ones is very close to the density $1/n$ of ones in the entire $n \times n \times n$ array.

[1] By "asymptotically almost surely", or "a.a.s.", we mean that the probability of an event is $1 - o(1)$. Here and for the rest of the paper, asymptotics are as $n \to \infty$.

It is natural to expect that in fact the statement of Conjecture 2 holds a.a.s. for a uniformly random Latin square $\boldsymbol{L} \in \mathcal{L}$. Linial and Luria proved the weaker result that a.a.s. every "empty" box T with $N_T(\boldsymbol{L}) = 0$ has $\operatorname{vol} T \le n^2 \log^2 n$. We are able to give a simple argument showing that random Latin squares a.a.s. have quite low discrepancy, especially when considering boxes of volume $\Omega\big(n^2 \log^2 n\big)$. This encompasses Linial and Luria's aforementioned result.

Theorem 2. *For a uniformly random $\boldsymbol{L} \in \mathcal{L}$, we a.a.s. have the following. For any box $T = I \times X \times Q$,*

$$\left| N_T(\boldsymbol{L}) - \frac{\operatorname{vol} T}{n} \right| = O\Big(\sqrt{\operatorname{vol} T} \log n + n \log^2 n\Big).$$

The proof of Theorem 2 is in Section 6.

2 Outline of the proof of Theorem 1

The first new ingredient for the proof of Theorem 1 is the following upper bound, both in expectation and with high probability, for the number of intercalates in two rows of a random Latin square.

Theorem 3. *Let $\boldsymbol{N_2} = N_2(\boldsymbol{L})$ be the number of intercalates in the first two rows of a uniformly random Latin square $\boldsymbol{L} \in \mathcal{L}$. We have*

$$\mathbb{E}\boldsymbol{N_2} \le 1 + o(1)$$

and

$$\Pr(\boldsymbol{N_2} \ge t) = e^{-\Omega(t \log t)}.$$

Note that $\mathbb{E}\boldsymbol{N} = \binom{n}{2}\mathbb{E}\boldsymbol{N_2}$ by linearity of expectation, so the upper bound on $\mathbb{E}\boldsymbol{N}$ in Theorem 1 immediately follows from Theorem 3. (Then, the a.a.s. upper bound on $\boldsymbol{N}$ follows from Markov's inequality). We doubt that the bound on $\mathbb{E}\boldsymbol{N_2}$ in Theorem 3 is sharp; Conjecture 1 suggests that $\mathbb{E}\boldsymbol{N_2} \sim 1/2$, and we expect that moreover $\boldsymbol{N_2}$ has an asymptotic Poisson distribution with this mean.

The second ingredient for Theorem 1 is a bound for the lower tail probability of the number of intercalates in a random Latin square.

Theorem 4. *There is a constant C such that the following holds. Let $\boldsymbol{N} = N(\boldsymbol{L})$ be the number of intercalates in a uniformly random Latin square $\boldsymbol{L} \in \mathcal{L}$. Suppose $\varepsilon \ge C \log^{1/3} n / n^{1/6}$. Then*

$$\Pr\left(\boldsymbol{N} < \frac{n^2}{4}(1-\varepsilon)\right) \le \exp\left(-\Omega\left(\varepsilon^2 \frac{\sqrt{n}}{\log n}\right)\right).$$

Clearly Theorem 4 implies the a.a.s. lower bound on $\boldsymbol{N}$ in Theorem 1, and because $\boldsymbol{N} \ge 0$ this in turn implies the lower bound on $\mathbb{E}\boldsymbol{N}$.

When studying random combinatorial structures with little independence, an indispensable technique is the analysis of "switching" operations that make local changes to an object. One defines switchings that affect some parameter in a controllable way, then estimates the number of ways to switch to and from each object, to understand the relative likelihood of each possible value of the parameter. Switchings underpin the proofs of both Theorem 3 and Theorem 4.

Latin squares are quite “rigid” objects, so one cannot easily define switching operations that make only small changes to a Latin square. In [3], Cavenagh, Greenhill and Wanless managed to overcome this difficulty when studying two fixed rows of a random Latin square. They considered switchings that make wide-ranging, complicated changes to the whole Latin square, but have a controllable effect on the two rows of interest. We prove Theorem 3 with a simpler switching operation in a similar spirit. The details are in Section 3.

To prove Theorem 4, we use Theorem 3 and some ideas from [17]. A $k \times n$ *Latin rectangle* is a $k \times n$ array of the numbers from 1 to n, where each number appears once in each row and not more than once in each column. We denote the set of all $k \times n$ Latin rectangles by $\mathcal{L}_k$.

For $k \leq n$, any $k \times n$ Latin rectangle can be extended to a $n \times n$ Latin square. The number of ways to do this does not depend too much on the Latin rectangle. Indeed, for a $k \times n$ Latin rectangle $L \in \mathcal{L}_k$ let $\mathcal{L}^*(L) \subseteq \mathcal{L}$ be the set of $n \times n$ Latin squares whose first k rows coincide with L. The following estimate is proved with standard upper and lower bounds on the permanent, and is proved in Appendix A.

Proposition 5. *For Latin rectangles $L, L' \in \mathcal{L}_k$,*

$$\frac{\mathcal{L}^*(L)}{\mathcal{L}^*(L')} \leq e^{O\left(n \log^2 n\right)},$$

uniformly over k.

So, the strategy is to find a lower bound on the number of intercalates in a random $k \times n$ Latin rectangle (for some k to be determined) that holds with very high probability. We will then be able to apply Proposition 5 to show that the number of intercalates in the first k rows of a random Latin square satisfies the same bound with high probability. We can use the union bound to show that this holds simultaneously for many choices of k rows, which gives a lower bound for the total number of intercalates in a random Latin square.

In [17], McKay and Wanless studied the number of intercalates in a random Latin rectangle. Using their methods, we will prove the following estimate.

Lemma 6. *There is a constant C such that the following holds. Let $\boldsymbol{L} \in \mathcal{L}_k$ be a uniformly random $k \times n$ Latin rectangle, conditioned on the event that no row is involved in more than K intercalates. Let $\boldsymbol{N} = N(\boldsymbol{L})$ be the number of intercalates in $\boldsymbol{L}$. If $k \geq \sqrt{n}$ and $t \geq Ck^2(K/n + k/K)$, then*

$$\Pr\left(\boldsymbol{N} \leq \frac{k^2}{4} - t\right) \leq e^{-\Omega\left(t^2/k^2\right)}.$$

Note that Theorem 3 and the union bound imply that with high probability no row is involved in many intercalates, which will give us an appropriate value of K with which to apply Lemma 6. In Section 4 we prove Lemma 6, and in Section 5 we give the details of how to combine Proposition 5, Lemma 6 and Theorem 3 to obtain Theorem 4.

3 Proof of Theorem 3

Note that any two rows i, j of a Latin square $L \in \mathcal{L}$ define a permutation $\sigma_{i,j}(L)$ on the columns of L: column x maps to the column y with $L_{i,y} = L_{j,x}$. Note that this permutation is a derangement; it has no fixed points $x \mapsto x$. We will be concerned with the permutation $\sigma_{1,2}(L)$ defined by the first two rows. This permutation decomposes into cycles, the set of which we denote $C(L)$. (For our purposes a cycle is a set of columns). Let $C^\alpha(L) \subseteq C(L)$ be the set of cycles of length α, and for a column x let $c_x(L) \in C(L)$ be the cycle which contains x. Note that $C^2(L)$ is the set of intercalates in the first two rows of L.

We first define two primitive switching operations on a Latin square, chosen such that they have a controllable effect on the intercalate count in the first two rows.

Definition 7. Consider a Latin square L.

- For any cycle $c \in C(L)$, we can obtain a new Latin square $\mathrm{fix}_c(L)$ by exchanging the contents of rows 1 and 2, for each column in c. We also write $\mathrm{fix}_x(L)$ to denote $\mathrm{fix}_{c_x(L)}(L)$.
- Just as two rows i, j of L define the permutation $\sigma_{i,j}(L)$, every two columns x and y also define a permutation $\tau_{x,y}(L)$ of rows (with row i mapping to the row j which satisfies $L_{j,x} = L_{i,y}$). In the cycle decomposition of $\tau_{x,y}(L)$, if rows 1 and 2 are in different cycles c_1 and c_2, then we say $\{x, y\}$ is a *flippable* pair, and write $\{x, y\} \in \mathrm{FL}(L)$. We can obtain a new Latin square $\mathrm{flip}_{\{x,y\}}(L)$ by exchanging column x and y for each row in c_2.

$$L = \begin{array}{|c|c|c|c|c|}\hline 1 & \mathbf{5} & \mathbf{3} & 4 & 2 \\ \hline 4 & \mathbf{3} & \mathbf{5} & 2 & 1 \\ \hline 2 & & 4 & & \\ \cline{1-1}\cline{3-3} 3 & & 2 & & \\ \cline{1-1}\cline{3-3} 5 & & 1 & & \\ \cline{1-1}\cline{3-3} \end{array} \qquad \mathrm{fix}_{\{2,3\}}(L) = \begin{array}{|c|c|c|c|c|}\hline 1 & \mathbf{3} & \mathbf{5} & 4 & 2 \\ \hline 4 & \mathbf{5} & \mathbf{3} & 2 & 1 \\ \hline 2 & & 4 & & \\ \cline{1-1}\cline{3-3} 3 & & 2 & & \\ \cline{1-1}\cline{3-3} 5 & & 1 & & \\ \cline{1-1}\cline{3-3} \end{array}$$

Figure 1. We show the effect of the fix operation. (Not all cells are depicted). Note that $\{1, 3\}$ was not flippable in L but is flippable in $\mathrm{fix}_{\{2,3\}}(L)$. Also note that $\sigma_{1,2}(L) = \sigma_{1,2}\big(\mathrm{fix}_{\{2,3\}}(L)\big) = (1\,4\,5)(2\,3)$.

$$L = \begin{array}{|c|c|c|c|c|}\hline 1 & 3 & 5 & 4 & 2 \\ \hline \mathbf{4} & 5 & \mathbf{3} & 2 & 1 \\ \hline \mathbf{2} & & 4 & & \\ \cline{1-1}\cline{3-3} \mathbf{3} & & \mathbf{2} & & \\ \cline{1-1}\cline{3-3} 5 & & 1 & & \\ \cline{1-1}\cline{3-3} \end{array} \qquad \mathrm{flip}_{\{1,3\}}(L) = \begin{array}{|c|c|c|c|c|}\hline 1 & 3 & 5 & 4 & 2 \\ \hline \mathbf{3} & 5 & \mathbf{4} & 2 & 1 \\ \hline \mathbf{4} & & \mathbf{2} & & \\ \cline{1-1}\cline{3-3} \mathbf{2} & & \mathbf{3} & & \\ \cline{1-1}\cline{3-3} 5 & & 1 & & \\ \cline{1-1}\cline{3-3} \end{array}$$

Figure 2. We show the effect of the flip operation. Note that $\sigma_{1,2}(L) = (1\,4\,5)(2\,3)$ and $\sigma_{1,2}\Big(\mathrm{flip}_{\{1,3\}}(L)\Big) = (1\,2\,3\,4\,5)$.

We will be using the flip operation to merge two cycles into a larger cycle, and we will be using the fix operation to make a pair of columns from different cycles flippable, if necessary. To justify this, we make a number of simple observations about the properties of the fix and flip operations.

Fact 8. The operations in Definition 7 have the following consequences.

1. Suppose $\{x, y\} \in \mathrm{FL}(L)$, and suppose $c_x(L) \neq c_y(L)$, with say $c_x(L) \in C^\alpha(L)$ and $c_y(L) \in C^\beta(L)$. Let $L' = \mathrm{flip}_{\{x,y\}}(L)$. Then

$$c_x(L') = c_y(L') = c_x(L) \cup c_y(L) \in C^{\alpha+\beta}(L').$$

Also, $C(L)\backslash\{c_x(L), c_y(L)\} = C(L')\backslash\{c_x(L')\}$. That is, flipping with x and y merges $c_x(L)$ and $c_y(L)$ and leaves the other cycles unaffected.

2. If $c \in C^2(L)$ is an intercalate, then $\sigma_{1,2}(L) = \sigma_{1,2}(\text{fix}_c(L))$. That is, the fix operation does not change the induced permutation.

3. Suppose $c_x(L) \neq c_y(L)$ and $\{x,y\} \in \text{FL}(L)$ (respectively, $\{x,y\} \notin \text{FL}(L)$). Let $L' = \text{fix}_x(L)$. Then $\{x,y\} \notin \text{FL}(L')$ (respectively $\{x,y\} \in \text{FL}(L')$). That is, the fix operation changes the flippability of $\{x,y\}$.

4. For any cycle c, we have $\text{fix}_c(\text{fix}_c(L)) = L$. For any $\{x,y\} \in \text{FL}(L)$, we have $\text{flip}_{\{x,y\}}\Big(\text{flip}_{\{x,y\}}(L)\Big) = L$. That is, the fix and flip operations are both involutions.

5. Suppose $\{x,y\} \in \text{FL}(L)$ and $c_x(L) \neq c_y(L)$, with $c_y(L) \in C^2(L)$. Let $\sigma' = \sigma_{1,2}\Big(\text{flip}_{\{x,y\}}(L)\Big)$. Then $(\sigma')^2(x) = y$.

With these observations in mind we can define a compound operation that merges an intercalate with another cycle, regardless of flippability.

Definition 9. For columns x, y with $c_x(L) \neq c_y(L)$ and $c_y(L) \in C^2(L)$ define

$$\text{join}_{x,y}(L) = \begin{cases} \text{flip}_{\{x,y\}}(L) & \text{if } \{x,y\} \in \text{FL}(L), \\ \text{flip}_{\{x,y\}}(\text{fix}_y(L)) & \text{if } \{x,y\} \notin \text{FL}(L). \end{cases}$$

If also $c_x(L) \in C^2(L)$ this is a *double* join, otherwise it is a *single* join. Note that a double join is not in general symmetric in x and y; we have $\text{join}_{x,y}(L) = \text{join}_{y,x}(L)$ if and only if $\{x,y\} \in \text{FL}(L)$.

Let $N^\alpha(L) = |C^\alpha(L)|$ be the number of cycles of length α. Let $\mathcal{L}(s) \subseteq \mathcal{L}$ be the set of Latin squares L with s intercalates in the first two rows (that is, with $N^2(L) = s$). We make some observations about the join operation.

Fact 10. Single and double joins have the following consequences.

1. A single join always decreases $N^2(\cdot)$ by exactly one, and the merged cycle has length greater than 4.

2. A double join always decreases $N^2(\cdot)$ by exactly two, and the merged cycle has length 4.

3. For $L \in \mathcal{L}(s+1)$, the number of Latin squares $L' \in \mathcal{L}(s)$ which we can reach with a single join is
$$\big(n - 2N^2(L)\big) \times 2N^2(L) = 2(s+1)(n - 2(s+1)).$$
(Choose a column x not in an intercalate and a column y in an intercalate).

4. For $L \in \mathcal{L}(s+2)$, the number of Latin squares $L' \in \mathcal{L}(s)$ which we can reach with a double join is at least
$$2N^2(L) \times 2\big(N^2(L) - 1\big)/2 = 2\big(s^2 + 3s + 2\big) \geq 2s^2.$$
(Choose a column x in an intercalate and a column y in a different intercalate. Since (x,y) and (y,x) may produce the same join, we then divide by 2 for a lower bound).

5. For $L' \in \mathcal{L}(s)$, the number of Latin squares $L \in \mathcal{L}(s+1)$ which can reach L' with a single join is at most
$$2\big(n - 2N^2(L) - 3N^3(L) - 4N^4(L)\big) \leq 2(n-2s).$$
(For $\sigma' = \sigma_{1,2}(L')$, choose a column x in a cycle with length greater than 4, and let $y = (\sigma')^2(x)$. If $\{x,y\} \in \mathrm{FL}(L')$ then flip, and then either fix or don't).

6. For $L' \in \mathcal{L}(s)$, the number of Latin squares $L \in \mathcal{L}(s+2)$ which can reach L' with a double join is at most
$$2 \times 4N^4(L) \leq 2n.$$
(For $\sigma' = \sigma_{1,2}(L')$, choose a column x in a 4-cycle, let $y = (\sigma')^2(x)$, flip if possible and then either fix or don't).

Let $J(s)$ be the number of ways to single join from a Latin square in $\mathcal{L}(s+1)$ to one in $\mathcal{L}(s)$. We have
$$\begin{aligned} 2(s+1)(n-2(s+1))|\mathcal{L}(s+1)| = J(s) &\leq 2(n-2s)|\mathcal{L}(s)|, \\ \frac{|\mathcal{L}(s+1)|}{|\mathcal{L}(s)|} &\leq \frac{n-2s}{(s+1)(n-2s-2)}. \end{aligned}$$
Similarly, double-counting the number of ways to double join from a Latin square in $\mathcal{L}(s+2)$ to one in $\mathcal{L}(s)$, we obtain
$$\frac{|\mathcal{L}(s+2)|}{|\mathcal{L}(s)|} \leq \frac{n}{s^2}.$$
So,
$$\frac{|\mathcal{L}(s+1)|}{|\mathcal{L}(s)|} \leq \frac{1}{s+1}\left(1 + O\left(\frac{1}{n}\right)\right) \tag{1}$$
for $2s \leq n/2$, and $|\mathcal{L}(s+2)|/|\mathcal{L}(s)| \leq 1$ for $2s \geq n/2$ (for large n). It follows that for $t \leq n/4$
$$\Pr(\boldsymbol{N_2} = t) \leq \frac{|\mathcal{L}(t)|}{|\mathcal{L}(0)|} \leq \prod_{s=0}^{t-1} \frac{|\mathcal{L}(s+1)|}{|\mathcal{L}(s)|} = \frac{1}{t!} e^{O(t/n)}$$
and
$$\Pr\left(t \leq \boldsymbol{N_2} \leq \frac{n}{4}\right) \leq O(1) \sum_{s=t}^{n/4} \frac{1}{s!} \leq O\left(\frac{1}{t!}\right) \sum_{r=0}^{\infty} \frac{1}{t^r} = O\left(\frac{1}{t!}\right) = e^{-\Omega(t \log t)}.$$
For $t > n/4$ we have $\Pr(\boldsymbol{N_2} = t) = O(1/((n/4)!))$ and
$$\Pr(\boldsymbol{N_2} \geq t) \leq O\left(\frac{n}{(n/4)!}\right) = e^{-\Omega(n \log n)} = e^{-\Omega(t \log t)}. \tag{2}$$
It therefore follows that $\Pr(\boldsymbol{N_2} \geq t) = e^{-\Omega(t \log t)}$ for all t.

We now bound $\mathbb{E}\boldsymbol{N_2}$. By (1), for $1 \leq t \leq n/4$ we have $t \Pr(\boldsymbol{N_2} = t) \leq (1 + o(1)) \Pr(\boldsymbol{N_2} = t-1)$, so using (2) and noting that $\boldsymbol{N_2} \leq n/2$,
$$\begin{aligned} \mathbb{E}\boldsymbol{N_2} &\leq 0 \Pr(\boldsymbol{N_2} = 0) + (1+o(1)) \sum_{t=1}^{n/4} \Pr(\boldsymbol{N_2} = t-1) + \frac{n}{2} \Pr\left(\boldsymbol{N_2} > \frac{n}{4}\right) \\ &\leq 0 + (1 + o(1)) + \frac{n}{2} e^{-\Omega(n \log n)} \to 1. \end{aligned}$$

4 Proof of Lemma 6

Let $\mathcal{L}_k^K \subseteq \mathcal{L}_k$ be the set of Latin rectangles L in which no row is involved in more than K intercalates. (We say these Latin rectangles are "good"). Let $\mathcal{L}_k^K(s) \subseteq \mathcal{L}_k^K$ be the set of good Latin rectangles with exactly s intercalates.

To prove Lemma 6 we use essentially the same switching as in [17], designed to increase the number of intercalates by exactly 1.

Definition 11. Consider a Latin rectangle $L \in \mathcal{L}_k^K$. For a row i and a cyclically ordered set of columns $(x\,y\,z)$, we obtain a new $k \times n$ array $L' = \mathrm{rot}^i_{(x\,y\,z)}(L)$ by swapping the symbols in positions (i,x), (i,y), (i,z) in a cyclic fashion: $L'_{i,x} = L_{i,z}$, $L'_{i,y} = L_{i,x}$, $L'_{i,z} = L_{i,x}$. We call this the *rotate* operation. Note that L' might not be a Latin rectangle, because we might have caused a column to contain two of the same symbol.

Now, we define the *twist* operation. For a Latin rectangle $L \in \mathcal{L}_k^K$, a row i and distinct columns x, y, z, x', y', z', let $L' = \mathrm{rot}^i_{(x\,y\,z)}\Big(\mathrm{rot}^i_{(x'\,y'\,z')}(L)\Big)$. Suppose the following conditions are satisfied.

- The rectangle L' is a Latin rectangle, and it is good (that is, $L' \in \mathcal{L}_k^K$).
- The positions (i,y), (i,z), (i,y'), (i,z') are involved in no intercalates in L or in L'
- The positions (i,x) and (i,x') are involved in no intercalates in L, and in L' there is an intercalate involving both (i,x) and (i,x'). This is the only intercalate involving (i,x) or (i,x') in L'.

Then we define the twist of L by $\mathrm{twist}^i_{\{(x,y,z),(x',y',z')\}}(L) = L'$.

$$L = \begin{array}{|c|c|c|c|c|c|} \hline \mathbf{1} & \mathbf{3} & \mathbf{5} & \mathbf{4} & \mathbf{2} & \mathbf{6} \\ \hline \multicolumn{1}{c}{} & \multicolumn{1}{c|}{} & 2 & 3 & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} \\ \cline{3-4} \end{array} \qquad \mathrm{twist}^1_{\{(3,1,2),(4,6,5)\}}(L) = \begin{array}{|c|c|c|c|c|c|} \hline \mathbf{5} & \mathbf{1} & \mathbf{3} & \mathbf{2} & \mathbf{6} & \mathbf{4} \\ \hline \multicolumn{1}{c}{} & \multicolumn{1}{c|}{} & 2 & 3 & \multicolumn{1}{c}{} & \multicolumn{1}{c}{} \\ \cline{3-4} \end{array}$$

Figure 3. We show the effect of the twist operation to create an intercalate involving $(1,3)$ and $(1,4)$.

Lemma 12. *The number of good Latin rectangles $L' \in \mathcal{L}_k^K(s+1)$ which we can reach via a twist from a specific good Latin rectangle $L \in \mathcal{L}_k^K(s)$ is at least*

$$\frac{1}{2}k^2n^4\left(1 - O\left(\frac{1}{k} + \frac{k}{n} + \frac{K}{n} + \frac{s}{kK}\right)\right).$$

Proof. Let $\Psi(L)$ be the set of rows of L involved in exactly K intercalates. We have $|\Psi(L)| \le 4s/K$. Now, choose rows i and j not in $\Psi(L)$, in which we will create an intercalate. There are

$$\left(k - \frac{4s}{K}\right)\left(k - \frac{4s}{K} - 1\right) = k^2\left(1 - O\left(\frac{s}{kK} + \frac{1}{k}\right)\right)$$

ways to do this. (Since we chose rows involved in at most $K-1$ intercalates, we do not need to worry about violating the goodness condition).

Next, choose distinct columns x, y, x', y'. To create an intercalate in columns x and x', let z' be the unique column with $L_{j,x} = L_{i,z'}$, and let z be the column with $L_{j,x'} = L_{i,z}$. There are $n^4(1 + O(1/n))$ ways to make these choices, but some of these do not give rise to a valid twist operation. Let $L' = \mathrm{rot}^i_{(x\,y\,z)}\Big(\mathrm{rot}^i_{(x'\,y'\,z')}(L)\Big)$; the possible violations are as follows.

- The symbol $L_{i,x}$ might already appear in column y (so that L' is not a Latin rectangle). For any x', y, y' there are at most k choices of x with this property, so we should subtract kn^3 for our upper bound. Similarly $L_{i,x'}$, $L_{i,y}$, $L_{i,y'}$, $L_{i,z}$ or $L_{i,z'}$ might appear in column y', z, z', x or x' respectively. We should therefore subtract $6kn^3$.

- We might have $z' \in \{x', y, y'\}$. For any x', y, y' there are at most 3 choices of x that cause this. Similarly we might have $z \in \{x, y, y'\}$. We should subtract $6n^3$ to compensate for both.

- One of the positions (i, x), (i, x'), (i, y), (i, y'), (i, z) or (i, z') might already be involved in an intercalate. We should subtract $6Kn^3$ to compensate for this.

- There might be an intercalate involving (i, y) in L'. This can only occur if for one of the $k-1$ non-y columns (w, say) in L' which contain the symbol $L_{i,x}$ (in row $q \neq i$, say), we have $L'_{i,w} = L'_{q,y}$. For any x, x', y' there are at most k choices of y for which this occurs. Similarly, putting $L_{i,y}$, $L_{i,z}$, $L_{i,x'}$, $L_{i,y'}$ or $L_{i,z'}$ in position (i, z), (i, x), (i, y'), (i, z') or (i, x') respectively might create an intercalate involving that position (other than the one given by positions (i, x), (i, x'), (j, x), (j, x')). Similar logic shows that for each of the 6 cases, we should subtract kn^3 to compensate.

If the above violations do not occur then we can use i, x, y, z, x', y', z' to twist, so the number of valid ways to twist is at least

$$\begin{aligned}\frac{1}{2}k^2\left(1 - O\left(\frac{s}{kK} + \frac{1}{k}\right)\right)&\left(n^4\left(1 + O\left(\frac{1}{n}\right)\right) - O\big(Kn^3\big) - O\big(kn^3\big) - O\big(n^3\big)\right)\\ &= \frac{1}{2}k^2n^4\left(1 - O\left(\frac{1}{k} + \frac{k}{n} + \frac{K}{n} + \frac{s}{kK}\right)\right).\end{aligned}$$

(We divide by 2 to compensate for the fact that we can exchange $(x\,y\,z)$ and $(x'\,y'\,z')$ to give the same twist). $\square$

Remark. Note that there are a number of simpler switching operations one could have defined in place of the twist operation. For instance, one could redefine the rotate operation to use cycles of 2 columns rather than cycles of 3 columns. However, (the analogue of) Lemma 12 would not hold with this simpler switching operation; there would be less freedom to choose a way to switch, and in fact there are Latin rectangles from which it is not possible to create exactly one intercalate using the simpler switching (see [17] for an example). This situation is analogous to the use of 6-cycle switchings rather than 4-cycle switchings in the analysis of random regular graphs (see for example [14]).

Lemma 13. *The number of good Latin rectangles $L \in \mathcal{L}_k^K(s-1)$ from which we can twist to a specific good Latin rectangle $L' \in \mathcal{L}_k^K(s)$ is at most $2sn^4$.*

Proof. Twisting from L must have created one of the s intercalates in L' as its main intercalate, operating in one of its two rows. The columns $\{x, x'\}$ are determined by the intercalate that was created, and there are at most n^4 choices of y, y', z, z' that could have been used. So the number of Latin rectangles L that can twist to L' is at most $2sn^4$. $\square$

We can use Lemmas 12 and 13 to give an upper and lower bound on the number of ways to twist from a Latin rectangle in $\mathcal{L}_k^K(s-1)$ to a Latin rectangle in $\mathcal{L}_k^K(s)$. For $s = O\big(k^2\big)$, $k \geq \sqrt{n}$ and $Ck^2(K/n + k/K) \leq k^2/4$ for large C, we obtain

$$\frac{\big|\mathcal{L}_k^K(s-1)\big|}{\big|\mathcal{L}_k^K(s)\big|} \leq \frac{s}{k^2/4}\exp\left(O\left(\frac{K}{n} + \frac{k}{K}\right)\right),$$

so for $t \geq 0$,

$$\frac{\left|\mathcal{L}_k^K\left(k^2/4-s\right)\right|}{\left|\mathcal{L}_k^K\left(k^2/4\right)\right|} \leq \prod_{r=0}^{s-1} \frac{\left|\mathcal{L}_k^K\left(k^2/4-r-1\right)\right|}{\left|\mathcal{L}_k^K\left(k^2/4-r\right)\right|} \leq \prod_{r=0}^{s-1}\left(\left(\frac{k^2/4-r}{k^2/4}\right)\exp\left(O\left(\frac{K}{n}+\frac{k}{K}\right)\right)\right).$$

For $0 \leq r \leq k^4/8$ we have $\left(k^2/4-r\right)/\left(k^2/4\right) = \exp\left(-\Theta\left(r/k^2\right)\right)$; it follows that for $s \leq k^2/8$,

$$\begin{aligned}
\Pr\left(\boldsymbol{N} = k^2/4-s\right) &\leq \frac{\left|\mathcal{L}_k^K\left(k^2/4-s\right)\right|}{\left|\mathcal{L}_k^K\left(k^2/4\right)\right|} \\
&\leq \exp\left(-\left(\sum_{r=0}^{s-1}\Theta\left(\frac{r}{k^2}\right)\right)+O\left(s\left(\frac{K}{n}+\frac{k}{K}\right)\right)\right) \\
&= \exp\left(-\Omega\left(\frac{s^2}{k^2}\right)+O\left(s\left(\frac{K}{n}+\frac{k}{K}\right)\right)\right).
\end{aligned}$$

If $Ck^2(K/n+k/K) \leq t \leq k^2/8$ for large C, then

$$\Pr\left(\boldsymbol{N} < k^2/4-t\right) \leq \sum_{s=t}^{k^2/8} e^{-\Omega\left(s^2/k^2\right)} = e^{-\Omega\left(t^2/k^2\right)}.$$

The case $k^2/8 < t \leq k^2/4$ follows trivially, because in this case

$$\Pr\left(\boldsymbol{N} < k^2/4-t\right) \leq \Pr\left(\boldsymbol{N} < k^2/8\right) = e^{-\Omega\left(\left(k^2\right)^2/k^2\right)} = e^{-\Omega\left(t^2/k^2\right)}.$$

5 Proof of Theorem 4

The constant C in the theorem statement will be a function of some other constant C_0, to be determined. For some $\varepsilon \geq C\log^{1/3} n/n^{1/6}$, let $k = C_0\sqrt{n}\log n/\varepsilon$ and let $K = \varepsilon n/C_0$.

Let $\mathcal{E}$ be the event that none of the first k rows of $\boldsymbol{L}$ are involved in more than K intercalates, in the Latin rectangle induced by the first k rows. Certainly $\mathcal{E}$ occurs if every pair of distinct rows (among the first k) has at most $K/(k-1)$ intercalates, because for each row there are $k-1$ possible pairs of rows involving that row. By Theorem 3 and the union bound (and symmetry considerations),

$$1-\Pr(\mathcal{E}) = k^2\exp\left(-\Omega\left(\frac{K}{(k-1)}\log\frac{K}{(k-1)}\right)\right) = \exp\left(-\Omega\left(\frac{K}{k}\log\frac{K}{k}\right)\right) = \exp\left(-\Omega\left(\varepsilon^2\frac{\sqrt{n}}{\log n}\right)\right).$$

Let $\boldsymbol{N}_k$ be the number of intercalates in the first k rows of $\boldsymbol{L}$. Noting that $C_0K/n \leq \varepsilon$ and $Ck/K \leq C_0^2\varepsilon$, for large C_0 and much larger C the conditions in Lemma 6 are satisfied. Combining Lemma 6 and Proposition 5,

$$\Pr\left(\boldsymbol{N}_k < (1-\varepsilon/2)k^2/4 \,\middle|\, \mathcal{E}\right) = e^{-\Omega\left(\varepsilon^2k^2\right)}e^{O\left(n\log^2 n\right)} = e^{-\Omega\left(\varepsilon^2k^2\right)}$$

for large C_0. Note that $\varepsilon^2k^2 \gg \varepsilon^2\sqrt{n}/\log n$ so

$$\Pr\left(\boldsymbol{N}_k < (1-\varepsilon/2)k^2/4\right) \leq \exp\left(-\Omega\left(\varepsilon^2\frac{\sqrt{n}}{\log n}\right)\right) \tag{3}$$

unconditionally. To transfer this result from the first k rows to the whole of $\boldsymbol{L}$, we need the following covering lemma.

Lemma 14. *For any $k \ll n$ and any $M \gg (n \log n/k)^2$ there exist k-subsets $F_i, \dots, F_M$ of $[n]$, such that every pair $\{i,j\} \subseteq [n]$ is included in*

$$M\left(\frac{k}{n}\right)^2 \left(1 + O\left(\log n / \left(\sqrt{M} k/n\right) + k/n\right)\right) = M\left(\frac{k}{n}\right)^2 (1 + o(1))$$

of the F_i.

Proof. Let $\boldsymbol{F}_1, \dots, \boldsymbol{F}_M$ be independent uniformly random sets of k rows. For a given pair of rows and some index i, the probability that $\boldsymbol{F}_i$ contains that pair is

$$p = \binom{n}{k-2} \Big/ \binom{n}{k} = \left(\frac{k}{n}\right)^2 \left(1 + O\left(\frac{k}{n}\right)\right).$$

By the Chernoff bound and the union bound, a.a.s. every pair is contained in

$$Mp + O\left(\sqrt{Mp} \log n\right) = Mp\left(1 + O\left(\frac{\log n}{\sqrt{Mp}}\right)\right).$$

of the $\boldsymbol{F}_i$. Therefore there exists a specific choice of the F_is that satisfies the requirements of the lemma. ☐

We apply Lemma 14 with $M = n^2$, say, to obtain sets $F_1, \dots, F_M$. By the union bound and symmetry, the subrectangle given by the rows of each F_i contains at least $(1 - \varepsilon/2)k^2/4$ intercalates, except with the probability in (3). Noting that $k/n + \log n / \left(\sqrt{M} k/n\right) \ll \varepsilon$, this implies

$$\begin{aligned} \boldsymbol{N} &\geq \frac{M(1 - \varepsilon/2)k^2/4}{M(k/n)^2 (1 + o(\varepsilon))} \\ &\geq (1 - \varepsilon)\frac{n^2}{4}. \end{aligned}$$

6 Proof of Theorem 2

Fix a box $T = I \times X \times Q$ (there are $(2^n)^3 = 8^n$ possible choices). We will show that the bound on $N_T(\boldsymbol{L})$ in Theorem 2 holds with probability $o(8^{-n})$, which will allow us to apply the union bound over choices of T.

For a Latin square L, we define a bipartite graph $G_Q(L)$ as follows. Both parts have n vertices (we abuse notation and say the vertex set is $[n] \sqcup [n]$); one of the parts is identified with the set of rows of the Latin square and the other part is identified with the set of columns. For each row i and column x such that $L_{i,x} \in Q$, we put an edge between i and x in $G_Q(L)$. Now, the number of ones $N_T(L)$ in T is just the number of edges $e_{G_Q(L)}(I, X)$ between I and X in $G_Q(L)$.

Let $\mathcal{G}_d$ be the set of d-regular bipartite graphs on $[n] \sqcup [n]$. For $G \in \mathcal{G}_{|Q|}$, let $|\mathcal{L}^*(G)|$ be the number of of Latin squares L with $G_Q(L) = G$. We can use standard bounds on the permanent to prove that $|\mathcal{L}^*(G)|$ does not vary very much with with G. See Appendix A for details.

Proposition 15. *For a set of symbols Q and $|Q|$-regular bipartite graphs G and G',*

$$\frac{|\mathcal{L}^*(G)|}{|\mathcal{L}^*(G')|} \le e^{O\left(n \log^2 n\right)}$$

uniformly over Q.

So, $G_Q(\boldsymbol{L})$ is not too far from the uniform distribution on $\mathcal{G}_{|Q|}$, and events that hold with very high probability for a uniformly random $\boldsymbol{G} \in \mathcal{G}_{|Q|}$ also hold with very high probability for $G_Q(\boldsymbol{L})$.

It is possible to obtain discrepancy tail bounds for random regular (bipartite) graphs using switchings of the type in [14, Theorem 2.2]. Such a bound would nearly provide the result we are after (although there would be difficulties for very dense graphs). However, at the range of probabilities we are interested in, regular bipartite graphs comprise a non-negligible proportion of all bipartite graphs with the appropriate number of edges, and (modulo an enumeration theorem for regular bipartite graphs) this enables a simpler approach. Let $\mathbb{B}(n,p)$ be the random graph distribution on the vertex set $[n] \sqcup [n]$, where each of the n^2 possible edges between the parts are present with independent probability p.

Lemma 16. *For any d (potentially depending on n), let $p = d/n$. The probability a random graph $\boldsymbol{B} \in \mathbb{B}(n,p)$ is d-regular is $e^{-O(n \log n)}$. Also, conditioning on this event gives the uniform distribution on $\mathcal{G}_d$.*

To prove Lemma 16 we will use the following very recent theorem of Liebenau and Wormald [15].

Theorem 17. *For any d (potentially depending on n), the number $|\mathcal{G}_d|$ of d-regular bipartite graphs on $[n] \sqcup [n]$ is asymptotic to*

$$e^{-1/2}\binom{n}{d}^{2n}\binom{n^2}{dn}^{-1}.$$

Proof of Lemma 16. The probability $\boldsymbol{B}$ has exactly $dn = pn^2$ edges is

$$\binom{n^2}{pn^2}p^{pn^2}(1-p)^{(1-p)n^2} \asymp \frac{1}{n\sqrt{p(1-p)}} = e^{-o(n)}.$$

(here we used Stirling's approximation). By symmetry, each graph with dn edges is equally likely. By Theorem 17, the fraction of such graphs which are d-regular is

$$(1+o(1))e^{-1/2}\binom{n}{pn}^{2n} \Bigg/ \binom{n^2}{pn^2}^{2} = (O(p(1-p)n))^{-n} \ge e^{-O(n \log n)}. \qquad \square$$

Now, discrepancy in $\mathbb{B}(n,p)$ (for $p = |Q|/n$) is very easy to study. Indeed, for $\boldsymbol{B} \in \mathbb{B}(n,p)$ the law of $e_{\boldsymbol{B}}(I,X)$ is the binomial distribution $\mathrm{Bin}(|I||X|, p)$ with mean $|I||X|p = \operatorname{vol} T/n$. Let $\boldsymbol{G} \in \mathcal{G}_{|Q|}$ be a uniformly random $|Q|$-regular bipartite graph. By a binomial large deviation inequality (for example

[10, Theorem 2.1]), Proposition 15 and Lemma 16, we have

$$\begin{aligned}\Pr\left(\left|N_T(\boldsymbol{L})-\frac{\operatorname{vol}T}{n}\right|>t\right)&=\Pr\left(\left|e_{G_Q(\boldsymbol{L})}(I,X)-\frac{\operatorname{vol}T}{n}\right|>t\right)\\&\le\Pr\left(\left|e_{\boldsymbol{G}}(I,X)-\frac{\operatorname{vol}T}{n}\right|>t\right)e^{O\left(n\log^2 n\right)}\\&\le\Pr\left(\left|e_{\boldsymbol{B}}(I,X)-\frac{\operatorname{vol}T}{n}\right|>t\right)e^{O\left(n\log^2 n+n\log n\right)}\\&=\exp\left(-\Omega\left(\frac{t^2}{\operatorname{vol}T/n+t}\right)+O\left(n\log^2 n\right)\right).\end{aligned}$$

If t is a large multiple of $\sqrt{\operatorname{vol}T}\log n+n\log^2 n$, then this probability is $e^{-\Omega\left(n\log^2 n\right)}=o(8^{-n})$.

7 Concluding remarks

We have shown that the number of intercalates $\boldsymbol{N}$ in a uniformly random $n\times n$ Latin square a.a.s. satisfies $(1-o(1))n^2/4\le\boldsymbol{N}\le fn^2$, for any $f\to\infty$, and we showed that $(1+o(1))n^2/4\le\mathbb{E}\boldsymbol{N}\le(1+o(1))n^2/2$. In doing so we obtained an exponentially-decaying estimate for the lower tail of $\boldsymbol{N}$ and an exponential upper-tail estimate for the number of intercalates in two fixed rows. We also proved that random Latin squares typically have relatively low discrepancy.

There are a number of related problems that remain open. First, there is the task of reducing the a.a.s. upper bound on $\boldsymbol{N}$ to $(1+o(1))n^2/4$ or at least to $O\left(n^2\right)$. The most obvious way of approaching this would be to imitate our proof of the lower bound, and show that for some k satisfying $\sqrt{n}\log n\ll k$, with very high probability a random $k\times n$ Latin rectangle does not have too many intercalates. The tools from [17] can accomplish this conditioned on the nonexistence of certain "problematic configurations" of intercalates, but showing these configurations are unlikely appears to be a surprisingly difficult task.

Second, there is the problem of understanding the existence and number of substructures other than intercalates in random Latin squares. McKay and Wanless [17] conjecture that the number of 3×3 Latin subsquares should have expectation $\Theta(1)$, and similar logic would suggest that a.a.s. there are no Latin subsquares of larger order. A proof of either of these facts would be interesting.

Third, there is the task of making further progress towards Conjecture 2. Even a slight improvement over our Theorem 2 would be interesting, because such an improvement would have to avoid the error introduced by theorems of the type in Appendix A.

Finally, it would be interesting to prove analogous results for more general types of random designs, such as Latin cubes or Steiner triple systems. Unfortunately, results of the type in Appendix A are not readily available in these cases, which considerably limits the (already very limited) tools at one's disposal.

References

[1] L. Brégman, Some properties of nonnegative matrices and their permanents, *Soviet Mathematics Doklady* **14** (1973), 945–949.

[2] P. J. Cameron, Almost all quasigroups have rank 2, *Discrete Mathematics* **106** (1992), 111–115.

[3] N. J. Cavenagh, C. Greenhill, and I. M. Wanless, The cycle structure of two rows in a random Latin square, *Random Structures & Algorithms* **33** (2008), no. 3, 286–309.

[4] G. Egorychev, The solution of Van der Waerden's problem for permanents, *Advances in Mathematics* **42** (1981), no. 3, 299–305.

[5] P. Erdős and A. Rényi, On random graphs I, *Publ. Math. Debrecen* **6** (1959), 290–297.

[6] D. I. Falikman, Proof of the Van der Waerden conjecture regarding the permanent of a doubly stochastic matrix, *Mathematical Notes* **29** (1981), no. 6, 475–479.

[7] R. Häggkvist and J. C. Janssen, All-even Latin squares, *Discrete Mathematics* **157** (1996), no. 1, 199–206.

[8] K. Heinrich and W. Wallis, The maximum number of intercalates in a Latin square, **Combinatorial mathematics VIII**, Springer, 1981, pp. 221–233.

[9] M. T. Jacobson and P. Matthews, Generating uniformly distributed random Latin squares, *Journal of Combinatorial Designs* **4** (1996), no. 6, 405–437.

[10] S. Janson, T. Łuczak, and A. Ruciński, **Random graphs**, Cambridge University Press, 2000.

[11] A. D. Keedwell and J. Dénes, **Latin squares and their applications**, second ed., Elsevier, 2015.

[12] A. Kotzig, C. Lindner, and A. Rosa, Latin squares with no subsquares of order two and disjoint Steiner triple systems, *Utilitas Mathematica* **7** (1975), 287–294.

[13] A. Kotzig and J. Turgeon, On certain constructions for Latin squares with no Latin subsquares of order two, *Discrete Mathematics* **16** (1976), no. 3, 263–270.

[14] M. Krivelevich, B. Sudakov, V. H. Vu, and N. C. Wormald, Random regular graphs of high degree, *Random Structures & Algorithms* **18** (2001), no. 4, 346–363.

[15] A. Liebenau and N. Wormald, The degree sequence of a random graph, and asymptotic enumeration of graphs with given degrees, private communication, 2016.

[16] N. Linial and Z. Luria, Discrepancy of high-dimensional permutations, *arXiv preprint arXiv:1512.04123* (2015).

[17] B. D. McKay and I. M. Wanless, Most Latin squares have many subsquares, *Journal of Combinatorial Theory, Series A* **86** (1999), no. 2, 323–347.

[18] M. McLeish, On the existence of Latin squares with no subsquares of order two, *Utilitas Mathematica* **8** (1975), 41–53.

[19] A. O. Pittenger, Mappings of Latin squares, *Linear algebra and its applications* **261** (1997), no. 1, 251–268.

[20] D. A. Preece, Latin squares as experimental designs, **Latin squares: New developments in the theory and applications** (A. D. Keedwell and J. Dénes, eds.), Annals of Discrete Mathematics, vol. 46, North-Holland, Amsterdam, 1991, pp. 317–341.

A Proofs of Proposition 5 and Proposition 15

We can interpret a Latin square as a 1-factorization of $K_{n,n}$ (that is, an edge colouring with n colours). The correspondence is that the edge between vertex i in the first part and vertex x in the second part receives colour q if $L_{i,x} = q$.

Let $\phi(G)$ be the number of 1-factors (perfect matchings) of a graph G. The Egorychev-Falikman theorem [4, 6] (previously known as the Van der Waerden conjecture) and Brégman's theorem [1] (previously known as Minc's conjecture) give lower and upper bounds on $\phi(G)$ for a d-regular bipartite graph G:

$$n!\left(\frac{d}{n}\right)^n \leq \phi(G) \leq (d!)^{n/d}.$$

We can therefore give bounds on the number of ways to choose a 1-factorization by choosing its 1-factors one-by-one:

$$\prod_{k=1}^{d} n!\left(\frac{k}{n}\right)^n \leq \Phi(G) \leq \prod_{k=1}^{d} (k!)^{n/k}.$$

Now, Stirling's inequality gives

$$\frac{(k!)^{n/k}}{n!(k/n)^n} \leq \frac{\left(\Theta\left(\sqrt{k}(k/e)^k\right)\right)^{n/k}}{\sqrt{n}(n/e)^n(k/n)^n} \leq \exp\left(O\left(\frac{n(\log k+1)}{k}\right)\right),$$

so using the approximation $\sum_{i=1}^{d} 1/i = \Theta(\log d + 1)$ for the harmonic series,

$$\prod_{k=1}^{d} \frac{(k!)^{n/k}}{n!(k/n)^n} = e^{O\left(n\left(\log^2 d+1\right)\right)}.$$

We have the following as a consequence.

Proposition 18. *Let G and G' be d-regular bipartite graphs on $n+n$ vertices. Then*

$$\frac{\Phi(G)}{\Phi(G')} \leq e^{O\left(n\left(\log^2 d+1\right)\right)}.$$

Now, in the notation of Proposition 15, note that $\mathcal{L}^*(G)$ is the number of 1-factorizations of G, times the number of 1-factorizations of its complement. For Proposition 5, we need to exchange the role of symbols and rows in our correspondence between Latin squares and 1-factorizations of $K_{n,n}$: put an edge coloured i between x and q if $L_{i,x} = q$. Then, $\mathcal{L}^*(L)$ is the number of 1-factorizations in the complement of a certain k-regular bipartite graph, which is an $(n-k)$-regular bipartite graph. Therefore both Proposition 15 and Proposition 5 follow from Proposition 18.