ELSEVIER
Discrete Mathematics 157 (1996) 199–206
DISCRETE MATHEMATICS

All-even latin squares

Roland Häggkvist[a], Jeannette C.M. Janssen[b,c,*]

[a] *Department of Mathematics, University of Umeå, 8-901 87 Umeå, Sweden*
[b] *LaCIM, Université de Québec à Montréal, CICMA, Québec, Canada H3G 1M8*
[c] *Department of Computer Science, Concordia University, 1455 de Maisonneuve Blvd. W., Montreal, Québec, Canada H3G 1M8*

Received 1 July 1994; revised 29 November 1994

Abstract

All-even latin squares are latin squares of which all rows are even permutations. All-even latin rectangles are defined accordingly. In this paper it is proved that the proportion of latin squares of order n which are all-even is at most c^n, where $\sqrt{\frac{3}{4}} < c < 1$. This result answers a question posed at the problem session of the 1993 British Combinatorial Conference. It is also shown that the proportion of all-even $k \times n$ latin rectangles with $k \leqslant n - 7$ is asymptotically equal to 2^{-k}.

Résumé

Les carrés latins complètement pairs sont les carrés latins dont chaque ligne et chaque colonne est une permutation paire. Nous démontrons que la proportion de carrés latins d'ordre n qui sont complètement pairs est majorée par c^n, où $\sqrt{\frac{3}{4}} < c < 1$. Ce résultat fournit la réponse à une question posée pendant la session de problèmes du colloque British Combinatorial Conference en 1993. Nous montrons également que la proportion de rectangles latins de dimension $k \times n$, $k \leqslant n - 7$, qui sont complètement pairs est asymptotiquement égale à 2^{-k}.

1. Introduction

A latin square of order n is an $n \times n$ array of the elements of $\{1, \ldots, n\}$ such that in each row and each column each element occurs exactly once. Hence each row and each column of a latin square represents a permutation. Recently, the signs of the permutations that constitute a latin square have been studied in the context of invariant theory of superalgebras, graph theory, and permutation group theory. For a general treatment of this topic and some background, the reader is referred to [5].

* Corresponding author. E-mail: jeanette@cs.concordia.ca.

SSDI 0012-365X(95)00263-4

An *all-even* latin square is a latin square for which all permutations given by its rows are even. In a paper on the group-theoretic aspects of random permutations, [3], Cameron and Kantor study the group generated by the permutations given by the rows of a latin square. A result by Cameron [1] shows that this group is almost always the symmetric or alternating group. Cameron and Kantor show that, if the limit of the proportion of latin squares which are all-even is zero, then the alternating group can be struck out from this statement. This observation gave rise to the posing of the following question at the 1993 British Combinatorial Conference, as a subsidiary problem to a problem proposed by Cameron titled 'the rows of a latin square'.

Problem (Cameron, [2]). *It is known that, for almost all latin squares of order n (i.e., a proportion tending to 1 as $n \to \infty$), the rows of the square (regarded as permutations) generate S_n or A_n. It is true that we almost always obtain the symmetric, rather than the alternating, group?*

The main theorem of this paper gives an affirmative answer to this question. Let $L(n)$ denote the number of latin squares of order n, and $L^+(n)$ the number of all-even such squares.

Theorem 1.1. *For all $\alpha < \frac{1}{2}$, $n > \frac{4}{(1/2)-\alpha}$,*

$$\frac{L^+(n)}{L(n)} \leqslant \left(\frac{3}{4}\right)^{\alpha n}.$$

Corollary. *For almost all latin squares of order n, the permutations given by its rows generate the symmetric group S_n.*

The proof of Theorem 1.1 is given in Section 3. Note that if the permutations given by the rows of a latin square of order n would exhibit asymptotic behaviour similar to that of any collection of n random permutations of order n, then one would expect the proportion of all-even latin squares to be close to $(\frac{1}{2})^n$. Our theorem gives the expected exponential behaviour, even though the base is significantly larger than $\frac{1}{2}$.

For latin rectangles we do obtain a result that indicates 'quasi-random' behaviour. A *latin rectangle* of size $k \times n$ is a $k \times n$ array of the elements of $\{1, \ldots, n\}$ such that in no row or column the same element occurs twice. Hence a latin rectangle can be seen as a collection of rows from a latin square. An all-even latin rectangle is a latin rectangle of which each row defines an even permutation. In Section 2 a result is given which shows that for latin rectangles of size $k \times n$ with k at most $n - 7$, the proportion of all-even latin rectangles asymptotically assumes the expected 2^{-k}.

The proofs in this paper rely on the graph-theoretical representation of a latin square, and the completion graph, defined below, plays a crucial role.

Definition. Let R be a $k \times n$ latin rectangle. The *completion graph* G_R of R is the graph with bipartition (V, W) where $V = \{v_1, v_2, \dots, v_n\}$, $W = \{w_1, w_2, \dots, w_n\}$, and with $v_i \sim w_j$ precisely when integer j does not occur in the ith column of R.

Since each column of R contains k elements, and each element occurs k times in R, G_R is regular of degree $n - k$. A matching in the completion graph of R represents a possible $(k + 1)$-th row of R; for each edge (v_i, w_j) of the matching, let j be the ith element of that row. A possible extension of R to a latin square is then a collection of disjoint matchings, and hence an edge colouring of G_R. If L is a latin square, then we define G_L^k to be the completion graph of the latin rectangle formed by the first k rows of L. Whenever applicable, we will consider the edges of G_L^k to be coloured according to the matchings given by rows $k + 1, \dots, n$ of L.

2. A partial result

Using standard bounds on the permanent and the determinant we obtain the following theorem. This theorem only gives the required convergence for latin rectangles of size up to $n - 7 \times n$, but the strength of the convergence in this case makes the result worth stating. First we introduce some terminology. For each latin rectangle R, let $\Sigma(R)$ denote the number of possible next rows of R, i.e., the number of permutations that do not give a conflict with the entries of the columns of R, and $\Sigma^+(R)$, $\Sigma^-(R)$ the number of even or odd such rows, respectively. Let $L(k, n)$ denote the number of $k \times n$ latin rectangles. For each vector $\boldsymbol{p} \in \{-1, 1\}^k$, denote $L^{\boldsymbol{p}}(k, n)$ to be the number of such rectangles which have the property that for each i, $1 \leqslant i \leqslant k$, the sign of the permutation given by their ith row is equal to p_i. Let $\boldsymbol{p}^+ \in \{-1, 1\}^k$ be the vector $(1, 1, \dots, 1)$, then $L^{\boldsymbol{p}^+}(k, n)$ is the number of all-even latin rectangles of size $k \times n$.

Theorem 2.1. *For all* $1 \leqslant k \leqslant n$, *and for all* $\boldsymbol{p} \in \{-1, 1\}^k$,

$$\prod_{r=0}^{k-1}\left(\frac{1}{2} - \frac{1}{2}\left(\frac{e}{\sqrt{n-r}}\right)^n\right) \leqslant \frac{L^{\boldsymbol{p}}(k,n)}{L(k,n)} \leqslant \prod_{r=0}^{k-1}\left(\frac{1}{2} + \frac{1}{2}\left(\frac{e}{\sqrt{n-r}}\right)^n\right),$$

and hence for $k \leqslant n - 7$,

$$\frac{L^{\boldsymbol{p}^+}(k,n)}{L(k,n)} \sim 2^{-k},$$

when $n \to \infty$.

Proof. Let n be fixed. The proof is by induction on k. A latin rectangle of size $1 \times n$ is just a permutation, and thus $L^+(1, n) = \frac{1}{2}n! = \frac{1}{2}L(1, n)$. Now suppose the statement is true for $k - 1$. Let R be a latin rectangle of size $k \times n$. Each matching in the completion graph of R represents a possible $(k + 1)$-th row of R. Let H be the biadjacency matrix of the completion graph, i.e. $H_{ij} = 1$ precisely when $v_i \sim w_j$, and 0 otherwise. H is a 0-1 matrix with row- and column sums equal to $n - k$. The permanent of H counts the number of matchings in the completion graph, and hence the number of possible ways to extend R to a $(k+1) \times n$ latin rectangle. A matching contributes a positive term to the determinant of H if the permutation given by that matching is even, and a negative one if the permutation is odd. Hence the difference between the number of possible $(k+1)$-th rows of R which are even and the number of rows which are odd is given by the determinant of H. By the Hadamard theorem,

$$|\det(H)| \leqslant (n-k)^{n/2}.$$

This result from linear algebra is based on the fact that the volume of a parallelepiped is at most the product of the length of its spanning vectors. By the Bang–Friedland lower bound on the permanent of a doubly stochastic matrix (cf. [4]),

$$\operatorname{per}(H) \geqslant \left(\frac{n-k}{e}\right)^n.$$

The inequalities show that for each L, $|\Sigma^+(R) - \Sigma^-(R)| \leqslant (n-k)^{n/2}$ and $\Sigma^+(R) + \Sigma^-(R) \geqslant ((n-k)/e)^n$, and thus

$$\tfrac{1}{2}(\Sigma(R) - (n-k)^{n/2}) \leqslant \Sigma^+(R) \leqslant \tfrac{1}{2}(\Sigma(R) + (n-k)^{n/2})$$

and

$$\left(\frac{1}{2} - \frac{1}{2}\left(\frac{e}{\sqrt{n-k}}\right)^n\right) \leqslant \frac{\Sigma^+(R)}{\Sigma(R)} \leqslant \left(\frac{1}{2} + \frac{1}{2}\left(\frac{e}{\sqrt{n-k}}\right)^n\right),$$

and the same inequalities hold for $\Sigma^-(R)$. Using the induction hypothesis we can now complete the proof of the right-hand side of the inequality of Theorem 2.1 with the following argument. Here $\boldsymbol{p}$ is a vector in $\{-1, 1\}^{k+1}$, and without loss of generality we assume that its last coordinate is equal to $+1$. By $\boldsymbol{p}'$ we denote here the vector in $\{-1, 1\}^k$ that agrees in its coordinates with the first k coordinates of $\boldsymbol{p}$.

$$\begin{aligned}
\frac{L^p(k+1,n)}{L(k+1,n)} &\leqslant \max_R \frac{\Sigma^+(R)}{\Sigma(R)} \frac{L^{p'}(k,n)}{L(k,n)} \\
&\leqslant \left(\frac{1}{2} + \frac{1}{2}\left(\frac{e}{\sqrt{n-k}}\right)^n\right) \frac{L^{p'}(k,n)}{L(k,n)} \\
&\leqslant \left(\frac{1}{2} + \frac{1}{2}\left(\frac{e}{\sqrt{n-k}}\right)^n\right) \prod_{r=0}^{k-1} \left(\frac{1}{2} + \frac{1}{2}\left(\frac{e}{\sqrt{n-r}}\right)^n\right) \\
&= \prod_{r=0}^{k} \left(\frac{1}{2} + \frac{1}{2}\left(\frac{e}{\sqrt{n-r}}\right)^n\right).
\end{aligned}$$

The left-hand side of the inequality follows by analogous arguments.

We $k \geqslant n-7$ then $\frac{e}{\sqrt{n-r}} \leqslant \frac{e}{\sqrt{8}} < 1$, for all $0 \leqslant r \leqslant k-1$, and thus, when $n \to \infty$,

$$\frac{L^p(k,n)}{L(k,n)} \sim 2^{-k}$$

for any vector $\boldsymbol{p} \in \{-1,1\}^k$, and thus also for $\boldsymbol{p}^+$.

3. Proof of the main theorem

The proof of Theorem 1.1 follows directly from the next lemma. Fix n. For each $k \leqslant n$ and each vector $\boldsymbol{p} = (p_1, p_2, \ldots, p_k) \in \{-1,1\}^k$ we define $\mathscr{L}^p$ to be the set of $n \times n$ latin squares which have the property that for each $i, 1 \leqslant i \leqslant k$, the sign of the permutation given by their ith row is equal to p_i. Note that there is a slight deviation from the definitions in the previous section, as we now prescribe only the signs of the first k rows of and $n \times n$ latin square.

Lemma 3.1. *Let k,n be integers such that $k = \alpha n$ and $n > \frac{4}{(1/2)-\alpha}$ for some positive $\alpha < \frac{1}{2}$. Let $\boldsymbol{p},\boldsymbol{p}' \in \{-1,1\}^k$ be such that they differ in exactly one coordinate. Then $|\mathscr{L}^p| \leqslant 3|\mathscr{L}^{p'}|$.*

Fix n, let k be as in the statement of this lemma, and let $\boldsymbol{p}^+ \in \{-1,1\}^k$ be the vector $(1,1,\ldots,1)$. If $\boldsymbol{p} \in \{-1,1\}^k$ is a vector with exactly l coordinates equal to -1, then by Lemma 3.1, $|\mathscr{L}^p| \geqslant (\frac{1}{3})^l |\mathscr{L}^{p^+}|$. Now

$$\begin{aligned} L(n) &= \sum_{l=0}^{k} \sum_{\substack{p \in \{-1,1\}^k \\ p \text{ contains } l\ -1\text{'s}}} |\mathscr{L}^p| \\ &\geqslant \sum_{l=0}^{k} \sum_{\substack{p \in \{-1,1\}^k \\ p \text{ contains } l\ -1\text{'s}}} \left(\frac{1}{3}\right)^l |\mathscr{L}^{p^+}| = \sum_{l=0}^{k} \binom{k}{l} \left(\frac{1}{3}\right)^l |\mathscr{L}^{p^+}| \\ &= (1+\tfrac{1}{3})^k |\mathscr{L}^{p^+}|. \end{aligned}$$

So $|\mathscr{L}^{p^+}| \leqslant (\frac{3}{4})^{\alpha n} L(n)$, and since $L^+(n) \leqslant |\mathscr{L}^{p^+}|$, this completes the proof of the main theorem 3.

In order to give the proof of Lemma 3.1 we will need some definitions and a lemma.

Definition. Let L be a latin square of order n, and let σ be the permutation given by row k of L. A *crossing pair at level* k of L is a pair $(i,j), 0 \leqslant i < j \leqslant n$, such that both edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$ are present in G_L^{k-1}, the completion graph of the first $k-1$ rows of L. In other words, v_i and v_j are contained in a 4-cycle in G_L^{k-1} which had two edges of colour k.

Lemma 3.2. *Let $k = \alpha n, \alpha < \frac{1}{2}$. Then each latin square of order n contains at least $(\frac{1}{2} - \alpha)n^2$ crossing pairs at level k.*

Proof. Let k, n be as in the statement of the lemma. Fix L, a latin square of order n. Let σ denote the permutation given by the kth row of L. Consider G_L^k, the completion graph of the first k rows of L. This graph is regular of degree $n - k$ and has $2n$ vertices and hence $n(n-k) = (1-\alpha)n^2$ edges. Of all pairs (i, j) with $1 \leqslant i < j \leqslant n$, either zero, one or two of the edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$ are present in G_L^k. If two edges are present then (i, j) is a crossing pair at level k. But if all pairs (i, j) are given one edge then there are still $(1-\alpha)n^2 - \binom{n}{2} \geqslant (\frac{1}{2} - \alpha)n^2$ edges left over, and hence there are at least $(\frac{1}{2} - \alpha)n^2$ crossing pairs.

Proof of Lemma 3.1. Fix α, k, n and vectors $p, p' \in \{-1, 1\}^k$ such that they satisfy the conditions of Lemma 3.1. We will prove the lemma by designing a map $\bar{\varphi}$ from $\mathscr{L}^p$ to $\mathscr{L}^{p'}$ and then show that $\bar{\varphi}$ maps at most three latin squares to the same image. Without loss of generality, we assume that the coordinate where p and p' differ is the kth one. Let $\underline{\mathscr{L}}^p$ be the set consisting of all latin squares in $\mathscr{L}^p$ and their crossing pairs. So $\underline{\mathscr{L}}^p = \{(L, (i, j)) \mid L \in \mathscr{L}^p, (i, j) \text{ a crossing pair for } L\}$. Now first we define a map $\varphi : \underline{\mathscr{L}}^p \to \underline{\mathscr{L}}^{p'}$. Consider $(L, (i, j)) \in \underline{\mathscr{L}}^p$, and let σ be the permutation representing row k of L. Since (i, j) is a crossing pair for L, both edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$ are present in G_L^{k-1}, the completion graph of the latin rectangle formed by the first $k-1$ rows of L. Let s and t be the colours of edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$, respectively, in the colouring of G_L^{k-1} induced by L. We distinguish three different cases. An st-cycle is a cycle in the subgraph of G_L^{k-1} induced by colours s and t. Since this subgraph consists of two disjoint matchings, each vertex is contained in exactly one st-cycle.

(1) $s = t$

(2) $s \neq t$ and vertices v_i and v_j are contained in two different st-cycles.

(3) $s \neq t$ and vertices v_i and v_j are contained in the same st-cycle.

The image of $(L, (i, j))$ under φ is given by a recolouring of G_L^{k-1}.

In case 1, we assign colour k to edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$, and colour s to edges $(v_i, w_{\sigma(i)})$ and $(v_j, w_{\sigma(j)})$.

In case 2, we recolour the st-cycle that contains vertex v_j (and hence also vertex $w_{\sigma(i)}$), switching colours s and t on all edges of the cycle. Now edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$ both have colour s, and we proceed to recolour as in case 1.

In case 3, we recolour in a similar way the st-cycle that contains v_i and v_j (and hence also $w_{\sigma(i)}$ and $w_{\sigma(j)}$). But now we switch colours only on that part of the cycle that lies between vertex $w_{\sigma(i)}$ and $w_{\sigma(j)}$ and that does not contain v_i and v_j. Next we assign colour s to edge $(v_i, w_{\sigma(i)})$, colour t to edge $(v_j, w_{\sigma(j)})$, and, as in the other cases, colour k to edges $(v_i, w_{\sigma(j)})$ and $(v_j, w_{\sigma(i)})$. It is a straightforward exercise to check that in all three cases, the recolouring again has the property that each colour represents a matching in the graph.

$\varphi(L,(i,j))$ is the latin square obtained by such a recolouring, i.e. the latin square with first $k-1$ rows identical to L and the last $n-k+1$ rows given by the recolouring of G_L^{k-1}. We make a number of observations.

— $\varphi(L,(i,j)) = (L',(i,j))$ is in $\mathscr{L}^{p'}$, because the first $k-1$ rows of L and L' are identical, and thus also their signs, and row k of L' differs from row k of L only by a switch of $\sigma(i)$ and $\sigma(j)$, so these two rows have opposite sign. It is easy to check that (i,j) is also a crossing pair for L'.

— If it is known whether the original colouring was of case 1, 2 or 3, then it is possible to reconstruct the original colouring from its image under φ. But case 1 and case 3 might give the same image. Hence φ is at most two-to-one.

Next we will use φ to define $\bar{\varphi}$. To do so we make use of a network N. N has nodes, a source s, a sink t, and nodes representing the elements of $\mathscr{L}^p$ and $\mathscr{L}^{p'}$. Edges go from s to each element of $\mathscr{L}^p$, from each element of $\mathscr{L}^{p'}$ to t, and from $L \in \mathscr{L}^p$ to $L' \in \mathscr{L}^{p'}$ precisely when there exists a pair (i,j) such that $(L',(i,j)) = \varphi(L,(i,j))$. The capacities on the edges are given by the function u.

$$u(s,L) = 1 \quad \text{for all } L \in \mathscr{L}^p,$$

$$u(L,t) = 3 \quad \text{for all } L \in \mathscr{L}^{p'},$$

$$u(L,L') = 1 \quad \text{for all edges } (L,L') \text{ with } L \in \mathscr{L}^p \text{ and } L' \in \mathscr{L}^{p'}.$$

We define a flow f from s to t. Here $d^+(L)$ denotes the out-degree, i.e. the number of out-going edges, of node L, and $L \to L'$ indicates that L and L' are connected by an edge directed from L to L'.

$$f(s,L) = 1 \quad \text{for all } L \in \mathscr{L}^p,$$

$$f(L,L') = \frac{1}{d^+(L)} \quad \text{for all edges } (L,L') \text{ with } L \in \mathscr{L}^p \text{ and } L' \in \mathscr{L}^{p'}$$

$$f(L',t) = \sum_{L \to L'} f(L,L') \quad \text{for all } L \in \mathscr{L}^{p'}.$$

It follows directly from the definition that f is a feasible flow. We now argue that, for n large enough, f is also compatible with the given capacities, in other words, for each edge $(a,b), f(a,b) \leqslant u(a,b)$. For the edges (s,L) and the edges (L,L') this is obvious. We observe that the recolouring of G_L^{k-1} which defines φ can create at most $2n$ new crossing pairs, as colour k is changed on only two edges, and each edge of colour k is contained in at most n crossing pairs. Recall also that φ is at most two-to-one. Hence for any two latin squares $L \in \mathscr{L}^p$ and $L' \in \mathscr{L}^{p'}$ which are joined by an edge in N their degrees are related by the inequality $d^-(L') \leqslant 2(d^+(L) + 2n)$ ($d^-(KL)$ is the in-degree of L). Consider $L' \in \mathscr{L}^p$, and let $d = \min_{L \sim L'} d^+(L)$. By the previous, $d^-(L') \leqslant 2d + 4n$, and by Lemma 3.2, $d \geqslant (\frac{1}{2} - \alpha)n^2$. Now the value of the incoming flow at L' is:

$$\sum_{L \to L'} f(L, L') = \sum_{L \to L'} \frac{1}{d^+(L)} \leqslant \sum_{L \to L'} \frac{1}{d} \leqslant \frac{2d + 4n}{d}$$
$$= 2 + \frac{4n}{d} \leqslant 2 + \frac{4n}{(\frac{1}{2} - \alpha)n^2}.$$

Since $n > \frac{4}{(1/2) - \alpha}$, this last term is smaller than three, so the flow f is compatible with the capacities.

The value of f is $|\mathscr{L}^p|$, so a maximal flow in N has value at least $|\mathscr{L}^p|$. But the cut defined by $\{s\}$ has value $|\mathscr{L}^p|$, so by the max-flow min-cut theorem f is maximal. Now since the capacities have integer values, there exists also an integer valued maximal flow. Call this flow $\bar{f}$. Since all edges (L, L') have capacity 1 and at each node $L \in \mathscr{L}^p$ the in-flow of any maximal flow is equal to 1, $\bar{f}$ gives a unique assignment from $\mathscr{L}^p$ to $\mathscr{L}^{p'}$. This assignment is used to define $\bar{\varphi}$: $\bar{\varphi}(L) = L'$ precisely when $\bar{f}(L, L') = 1$. Since $\bar{f}$ is compatible with the capacities and integer valued, a node $L' \in \mathscr{L}^{p'}$ can receive a positive flow from at most three nodes of $\mathscr{L}^p$, and hence $\bar{\varphi}$ is at most three-to-one. This proves the assumption of the lemma.

Acknowledgements

This work was done while the second author was a visitor at Umeå University in Sweden. She wishes to thank this University, especially the Mathematics Department, for the support and hospitality.

References

[1] P.J. Cameron, Almost all quasigroups have rank 2, Discrete Math. 106/107 (1992) 111–115.
[2] P.J. Cameron, ed., Problems of the Fourteenth British Combinatorial Conference, Discrete Math. 138 (1995) 405–411.
[3] P.J. Cameron and W.M. Kantor, Random permutations: Some group-theoretic aspects, preprint.
[4] S. Friedland, A lower bound for the permanent of a doubly stochastic matrix, Ann. Math. 110 (1979) 167–176.
[5] Jeannette C.M. Janssen, On even and odd latin squares, J. Combin. Theory Ser. A 69 (1995) 173–181.