All-Even Latin Squares

by

Roland Häggkvist
University of Umeå

and

Jeannette C.M. Janssen
Université de Québec à Montréal and Concordia University

November 1993

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 $k \leq n-7$ is asymptotically equal to 2^{-k}.

Resumé: Les carrés latins entièrement pairs sont des carrés latins dont toutes les lignes sont des permutations pairs. On définit des rectangles latins entièrement pairs de manière analogue. On démontre ici que la proportion de carrés latin qui sont entièrement pairs est au plus c^n, où $\sqrt{\frac{3}{4}} < c < 1$. Ce résultat répond à une question posée pendant la séance de problèmes de la British Combinatorial Conference 1993. On montre aussi que la proportion de rectangles latins de taille $k \times n$ avec $k \leq n-7$ qui sont entièrement pairs est asymptotiquement 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 [J].

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, [CK], Cameron and Kantor study the group generated by the permutations given by the rows of a latin square. A result by Cameron [C1] shows that this group is almost always the symmetric or alternating group. Cameron and Kantor then showed 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 work 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, [C2]).

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. Is it 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 $\mathcal{L}(n)$ denote the number of latin squares of order n, and $\mathcal{L}^+(n)$ the number of all-even such squares.

Theorem 1.1

For all $\alpha < \frac{1}{2}$, $n > \frac{4}{\frac{1}{2}-\alpha}$,

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

Corollary.

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

Name (tulip.cs.concordia.ca:janssen): jeanette 331 Password required for jeanette. Password: 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 $\left(\frac{1}{2}\right)^n$. 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 $\left(\frac{1}{2}\right)^k$.

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 $V = \{v_1, v_2, \ldots, v_n\}$, $W = \{w_1, w_2, \ldots, w_n\}$, and with $v_i \sim w_j$ precisely when integer j does not occur in the i-th 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 i-th element of that row. A possible extension of R to a latin square is then a collection of 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 $k+1,\ldots,n$ 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 $\mathcal{L}(k,n)$ denote the number of

$k \times n$ latin rectangles. For each vector $\mathrm{p} \in \{-1,1\}^k$, denote $\mathcal{L}^{\mathrm{p}}(k,n)$ to be the number of such rectangles which have the property that for each i, $1 \le i \le k$, the sign of the permutation given by their i-th row is equal to p_i. Let $\mathrm{p}^+ \in \{-1,1\}^k$ be the vector $(1,1,\ldots,1)$, then $\mathcal{L}^{\mathrm{p}^+}(k,n)$ is the number of all-even latin rectangles of size $k \times n$.

Theorem 2.1.

For all $1 \le k \le n$,

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

and hence when $k \ge n-7$,

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

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 $\mathcal{L}^+(1,n) = \frac{1}{2}n! = \frac{1}{2}\mathcal{L}(1,n)$. Now suppose the statement is true for k. 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. Then 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 even possible $k+1$-th rows of R and the number of odd such rows is given by the determinant of H. However, by the Hadamard theorem,

$$|\det(H)| \le (n-k)^{\frac{n}{2}},$$

and by the Van der Waerden theorem (see [E] for a proof),

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

Then the above argument shows that for each L, $|\Sigma^+(R) - \Sigma^-(R)| \le (n-k)^{\frac{n}{2}}$ and $\Sigma^+(R) + \Sigma^-(R) \ge \left(\frac{n-k}{e}\right)^n$, and thus

$$\frac{1}{2}(\Sigma(R) - (n-k)^{\frac{n}{2}}) \le \Sigma^+(R) \le \frac{1}{2}(\Sigma(R) + (n-k)^{\frac{n}{2}}),$$

and

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

and the same inequalities hold for $\Sigma^-(R)$. Using the induction hypothesis we can then complete the proof by a straightforward deduction argument. When $k\ge n-7$ then $\frac{e}{\sqrt{n-r}}\le\frac{e}{\sqrt{8}}<1$, for all $0\le r\le k-1$, and thus

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

when n goes to infinity.

3. Proof of the Main Theorem

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

Lemma 3.1.

Let $k=\alpha n$, $\alpha<\frac{1}{2}$. Let $\mathbf{p},\mathbf{p}'\in\{-1,1\}^k$ be such that they differ in exactly one coordinate. Then $|\mathcal{L}^{\mathbf{p}}|\le 3\,|\mathcal{L}^{\mathbf{p}'}|$.

The proof of this lemma is quite technical and therefore will be omitted in this extended abstract. This proof is based on the definition of a map from $\mathcal{L}^{\mathbf{p}}$ to $\mathcal{L}^{\mathbf{p}'}$ which can then be shown to be at worst three-to-one.

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

$$\begin{aligned}
\mathcal{L}(n) &= \sum_{\ell=0}^{k} \sum_{\substack{\mathbf{p}\in\{-1,1\}^k \\ \mathbf{p}\text{ contains }\ell\text{ -1's}}} |\mathcal{L}^{\mathbf{p}}| \\
&\geq \sum_{\ell=0}^{k} \sum_{\substack{\mathbf{p}\in\{-1,1\}^k \\ \mathbf{p}\text{ contains }\ell\text{ -1's}}} \left(\frac{1}{3}\right)^{\ell} |\mathcal{L}^{\mathbf{p}^+}| \\
&= \sum_{\ell=0}^{k} \binom{k}{\ell} \left(\frac{1}{3}\right)^{\ell} |\mathcal{L}^{\mathbf{p}^+}| \\
&= \left(1+\frac{1}{3}\right)^{k} |\mathcal{L}^{\mathbf{p}^+}|
\end{aligned}$$

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

4. References

[C1] P.J. Cameron *Almost all quasigroups have rank 2* Discrete Math. **106/107** (1992) pp. 111–115

[C2] P.J. Cameron,editor *Problems of the Fourteenth British Combinatorial Conference* (1993)

[CK] P.J. Cameron and W.M. Kantor *Random permutations: Some group-theoretic aspects* (1993) preprint

[E] G.P. Egorichev *The Solution of the Van der Waerden Problem for Permanents* Dokl. Akad. Nauk. SSR **258** (1981) pp. 1041–1044

[J] Jeannette C.M. Janssen *On Even and Odd Latin Squares* (1993) J. Combin. Th. A, to appear

Roland Häggkvist
Dept of Mathematics
University of Umeå
S-901 87 Umeå
Sweden
Roland.Haggkvist@ mathdept.umu.se

Jeannette Janssen
Dept of Computer Science
Concordia University
1455 de Maisonneuve Blvd. W.
Montréal, Québec H3G 1M8
jeanette@ cs.concordia.ca