Lecture XI. Improved Results on the Number of Latin Rectangles

In this continuation of the seventh lecture I shall try to present a corrected version of my paper in the 1978 Journal of Combinatorial Theory, Series A. The principal result of that paper is that the number $N_{k,n}$ of $k \times n$ Latin rectangles satisfies

$$(1) \qquad N_{k,n} \sim (n!)^k \prod_{j=1}^{k-1} \left(1 - \frac{j}{n}\right)^n \sim (n!)^k e^{-\frac{k(k-1)}{2} - \frac{k^3}{6n}}$$

as $n \to \infty$, uniformly for $k \leq C\sqrt{n}$, with C an absolute constant. This confirms the conjecture of Erdös and Kaplansky that their formula

$$(2) \qquad N_{k,n} \sim (n!)^k e^{-\frac{k(k-1)}{2}}$$

does not hold beyond $k = o(n^{1/3})$.

Recently Godsil and McKay (1983) have obtained much more precise results by a completely different method. In particular they proved that

$$(3) \qquad N_{k,n} = \left[(n!)^k \prod_{j=1}^{k-1} \left(1 - \frac{j}{n}\right)^n\right]\left(1 - \frac{k}{n}\right)^{-\frac{n}{2}} e^{-\frac{k}{2} + O\left(\frac{k^7}{n^6} + \frac{1}{n}\right)}$$

uniformly for $k = O(n^{1-\delta})$ for any fixed $\delta > 0$, and they suggested the possibility that the error term could be improved to $O(\frac{1}{n} + k(\frac{k}{n})^t)$ for arbitrarily large t. For small k their result is much more precise even than (3). It is not clear whether my method has any hope of yielding results comparable to theirs. Briefly, my approach to improving on the results of Lecture VII is to show that, in a rather weak sense, the two factors under the expectation sign are approximately uncorrelated. It would be useful to show that this holds to a much better approximation. The construction used here has some hope of accomplishing this, which is the only real obstacle to obtaining substantially better results than (1). It also seems likely that this construction will be useful whenever we are interested in accurate approximations to probabilities concerning random permutations.

My present aim is to prove (1) by reducing it to a very weak form of the approximate independence I have just mentioned. One possible approach is to try to evaluate the second term on the right-hand side of (VII.40) by conditioning on I, J, $\Pi(I)$, and $\Pi(J)$. For this purpose let us start by computing $P(CD^*)$ and $P(DD^*)$. By the definition of C and D^* in (VII.17) and (VII.20) we have

(4)
$$\begin{aligned} P(CD^*) &= P\{\Pi(I) \in S^c(I)S^c(J) \ \&\ \Pi(J) \in S(I)S(J)\} \\ &= \frac{1}{[n(n-1)]^2} \sum_{\substack{1 \le i,j \le n \\ i \ne j}} |S^c(i)S^c(j)| \cdot |S(i)S(j)| \\ &= \frac{1}{[n(n-1)]^2} \sum_{\substack{1 \le i,j \le n \\ i \ne j}} [n-2k+|S(i)S(j)|] \cdot [|S(i)S(j)|] \\ &= \frac{1}{[n(n-1)]^2} [nk(k-1)(n-2k) + \sum_{\substack{1 \le i,j \le n \\ i \ne j}} |S(i)S(j)|^2]. \end{aligned}$$

I have used the fact that

(5)
$$\sum_{\substack{1 \le i,j \le n \\ i \ne j}} |S(i)S(j)| = nk(k-1),$$

since each of the numbers in $\{1,\ldots,n\}$ occurs in k columns and thus in $k(k-1)$ ordered pairs of columns. For later use observe that

(6)
$$\sum_{\substack{1 \le i,j \le n \\ i \ne j}} |S(i)S(j)|^2 \le n(k-1)k^2,$$

since, for each i, the sum over j is maximized when k-1 columns other than the i^{th} contain the same symbols as the i^{th} column. Similarly

(7) $$P(DD^*) = P\{\pi(I) \in S(I)S^c(J) \ \&\ \pi(J) \in S^c(I)S(J)\}$$

$$= \frac{1}{[n(n-1)]^2} \sum_{i,j} [k - |S(i)S(j)|]^2$$

$$= \frac{1}{[n(n-1)]^2} [k^2 n(n-2k+1) + \sum_{i,j} |S(i)S(j)|^2].$$

From (4) and (7) it follows that

(8) $$P(CD^*) - P(DD^*) = -\frac{k(n-k)}{n(n-1)^2}.$$

The fact that $\bar{W}$, the number of coincidences in columns other than I and J, is approximately uncorrelated with the events CD* and DD* will be expressed by rewriting (VII.36) in the form

(9) $$E\, h(W) - \mathcal{B}_{n,p} h = (n-1)E(V_{n,p}h)(\bar{W})[\mathcal{I}(CD^*) - \mathcal{I}(DD^*)]$$

$$= (n-1)E[(V_{n,p}h)(\bar{W}'')(\mathcal{I}(CD^*) - \mathcal{I}(DD^*)]$$

$$+ (n-1)E[(V_{n,p}h)(\bar{W}) - (V_{n,p}h)(\bar{W}'')][\mathcal{I}(CD^*) - \mathcal{I}(DD^*)].$$

Here $\bar{W}''$ is a random variable having the same distribution as $\bar{W}$ but independent of I, J, $\pi(I)$, $\pi(J)$ and thus also of CD* and DD*. This will be constructed in such a way that $\bar{W}''$ will equal $\bar{W}$ with high probability. In this way I shall try to obtain an adequate upper bound for the second term on the r.h.s. of (9). Using (8), that identity can be rewritten as

(10) $$E\, h(W) - \mathcal{B}_{n,p} h = -\frac{k(n-k)}{n(n-1)} E(V_{n,p}h)(\bar{W}) + R_1 + R_2,$$

where

(11) $$R_1 = (n-1)E[(V_{n,p}h)(\bar{W}) - (V_{n,p}h)(\bar{W}'')]\mathcal{I}(CD^*)$$

and

(12) $$R_2 = (n-1)E[(V_{n,p}h)(\bar{W}) - (V_{n,p}h)(\bar{W}'')]\mathcal{I}(DD^*).$$

The immediate task is to prove that, for $h = h_0$,

$$|R_1| + |R_2| = O\left(\frac{k^3}{n^2} \mathcal{B}_{n,p} h_0\right). \tag{13}$$

Then it will follow easily from (10) that

$$P\{W=0\} = (1 - \frac{k}{n})^n (1 + O(\frac{k}{n})), \tag{14}$$

which will imply (1). If better bounds can be obtained for R_1 and R_2, it will be possible to obtain better results from (10) by iteration.

The random variable $\tilde{W}''$ will be constructed in the following way. Again it will be necessary to work with a richer probability space. We shall construct random permutations Π and Π'' and random points I, J, I'', J'' of $\{1,\ldots,n\}$ subject to $I \neq J$ and $I'' \neq J''$ with the following properties:

(i) $((\Pi,I,J), (\Pi'',I'',J''))$ is an exchangeable pair

(ii) The conditional distribution of (Π'',I'',J'') given $(I,J,\Pi(I),\Pi(J))$ is uniform over the set of all $n!n(n-1)$ possibilities.

(iii) Except possibly for $i \in \{I,J,I'',J''\}$ and two other values of i, $\Pi(i) = \Pi''(i)$.

Then $\tilde{W}''$ will be related to Π'', I'', and J'' in the same way that W is related to Π, I, and J, that is

$$\tilde{W}'' = \sum_{i \notin \{I'',J''\}} \mathcal{J}\{\Pi''(i) \in S(i)\}. \tag{15}$$

The following is an outline of the construction of the exchangeable pair (Π,I,J), (Π'',I'',J'').

a) Choose two independent ordered pairs (I,J) and (K,L) of distinct elements of $\{1,\ldots,n\}$, each uniformly distributed over the set of all $n(n-1)$ possibilities. The random permutation Π will be specified in part by the condition that

$$\Pi(I) = K \quad \text{and} \quad \Pi(J) = L. \tag{16}$$

b) Choose the random permutation Π'' and the random ordered pair (I'',J'') independently uniformly distributed, independent of I, J, K, and L. This will insure that condition (ii) above is satisfied.

c) For all

(17) $$i \in \{I,J,I'',J'',\Pi''^{-1}\Pi(I),\Pi''^{-1}\Pi(J)\}^c$$

define

(18) $$\Pi(i) = \Pi''(i).$$

This will insure that condition (iii) above is satisfied.

d) Complete the specification of the random permutation Π in a way that is symmetric under exchange of (Π,I,J) and (Π'',I'',J''), thus insuring the exchangeability required in (i) above.

I have verified the possibility of d) above by a detailed consideration of roughly thirty cases. Here I shall discuss only two of these cases. The first, which I shall call the regular case, occurs with probability $1 - O(\frac{1}{n})$. The second is typical of the few cases where it seems at first that some difficulty may arise in complying with d).

Case 1: The regular case

This case is characterized by the conditions

(19) $$\{I,J\} \cap \{I'',J''\} = \emptyset$$

and

(20) $$\{\Pi(I),\Pi(J)\} \cap \{\Pi''(I),\Pi''(J),\Pi''(I''),\Pi''(J'')\} = \emptyset.$$

In this case we complete the definition of Π by setting

(21) $$\Pi(I'') = \Pi''(I),\ \Pi(J'') = \Pi''(J)$$

and

(22) $$\Pi\Pi''^{-1}\Pi(I) = \Pi''(I''),\ \Pi\Pi''^{-1}\Pi(J) = \Pi''(J'').$$

Then Π is a permutation because, by c), outside $Q = \{I,J,I'',J'',\Pi''^{-1}\Pi(I),\Pi''^{-1}\Pi(J)\}$ it coincides with Π'' and inside Q its values are a permutation of those of Π''. Conditions (19), (21), and (22) are symmetric under exchange of (Π,I,J) and (Π'',I'',J''). Also (19), (20), and (21) imply the condition

(23) $$\{\Pi''(I''),\Pi''(J'')\} \cap \{\Pi(I''),\Pi(J''),\Pi(I),\Pi(J)\}$$

dual to (20). The probability of this regular case is $(n)_6/[n_{(2)}]^3 = 1 - O(\frac{1}{n})$.

Case 2: (An example)

Suppose it happens that, in carrying out the choices prescribed in a), b), and c),

(24) $$I'' = I \quad \text{but} \quad J'' \neq J$$

and

(25) $$\Pi(I) = \Pi''(J'')$$

but

(26) $$\Pi(J) \notin \{\Pi''(I),\Pi''(J)\}.$$

In this case we complete the definition of Π by

(27) $$\Pi(J'') = \Pi''(J)$$

and

(28) $$\Pi\Pi''^{-1}\Pi(J) = \Pi''(I).$$

Observe that, once we have made these choices, (26) is redundant since (24) and (27) imply that

(29) $$\Pi''(J) = \Pi(J'') \neq \Pi(J),$$

which implies that

(30) $$\Pi''^{-1}\Pi(J) \neq J$$

and consequently

(31) $$\Pi''(I) = \Pi(\Pi''^{-1}\Pi(J)) \neq \Pi(J).$$

I have used the fact that Π defined in this way is a permutation. To prove this, observe first that the set Q introduced in Case 1 reduces to four points: $Q = \{I,J,J'',\Pi''^{-1}\Pi(J)\}$ since $I'' = I$ by (24) and $\Pi''^{-1}\Pi(I) = J''$ by (25). As in Case 1, Π is a permutation because, outside Q, it coincides with Π'' and, inside Q, its values $\Pi(I)$, $\Pi(J)$, $\Pi(J'') = \Pi''(J)$ and $\Pi\Pi''^{-1}\Pi(J) = \Pi''(I)$ are a permutation of the values of Π'' inside Q, which are $\Pi''(I)$, $\Pi''(J)$, $\Pi''(J'') = \Pi(I)$, and $\Pi''\Pi''^{-1}(J) = \Pi(J)$. This definition is not symmetric under exchange of (Π,I,J) and (Π'',I'',J'') and could not be because the dual of (25) contradicts (24) and (26).

However this can be paired with the dual case. To see this, let us write down the duals of the defining relations (24), (25), (27), and (28). Of course (24) is self-dual and, for the others, we obtain

(25') $$\Pi(J) = \Pi''(I)$$

(27') $$\Pi(J'') = \Pi''(J)$$

and

(28') $$\Pi(I) = \Pi''\Pi^{-1}\Pi''(J'').$$

The set Q introduced in Case 1 is reduced to $Q = \{I,J,J'',\Pi''^{-1}\Pi(I)\}$. We can rewrite (28') as

(28") $$\Pi\Pi''^{-1}\Pi(I) = \Pi''(J'').$$

As before (27') and (28") complete the definition of Π, now in the presence of the condition (25'), in addition to (24).

Now let us look at the problem of obtaining a bound for the contribution of the regular case to R_1 when $h = h_0$, that is, a bound for

(32) $$R_1^* = (n-1)E[(V_{n,p}h_0)(\bar{W}) - (V_{n,p}h_0)(\bar{W}'')]\mathscr{I}(CD^*)Z,$$

where

(33) $$Z = \begin{cases} 1 & \text{if the regular case occurs} \\ 0 & \text{otherwise.} \end{cases}$$

In order to exploit the fact that, in (32), $\bar{W} = \bar{W}''$ with high probability, let $\bar{\bar{W}}$ be the number of coincidences in columns outside Q (which was defined in (22)), that is

(34) $$\bar{\bar{W}} = \sum_{i \notin Q} \mathscr{I}\{\Pi(i) \in S(i)\}$$

and let

(35) $$W_1 = \bar{W} - \bar{\bar{W}} = \sum_{i \in Q\{I,J\}^c} \mathscr{I}\{\Pi(i) \in S(i)\}$$

and

(36) $$W_1'' = \bar{W}'' - \bar{\bar{W}} = \sum_{i \in Q\{I,J\}^c} \mathscr{I}\{\Pi''(i) \in S(i)\}.$$

Then we can rewrite R_1^* as

(37) $$R_1^* = (n-1)E[(V_{n,p}h_0)(\bar{\bar{W}}+W_1) - (V_{n,p}h_0)(\bar{\bar{W}}+W_1'')]\mathscr{I}(CD^*)Z$$

and conclude that

(38) $$|R_1^*| \leq (n-1)E(V_{n,p}h_0)^*(\bar{\bar{W}})\mathscr{I}(CD^* \cap \{W_1+W_1'' > 0\})Z$$

where

(39) $$(V_{n,p}h_0)^*(w) = \sup_{0 \leq \ell \leq 4} |(V_{n,p}h_0)(w+\ell)|.$$

Now

(40) $$P(CD^* \cap \{W_1+W_1'' > 0\}) = O\left(\frac{k^3}{n^3}\right)$$

and the event occurring on the left-hand side is determined by the random set Q and $\Pi \upharpoonright Q$ and $\Pi'' \upharpoonright Q$ (the restrictions of Π and Π'' to Q). Thus

(41) $$|R_1^*| = O\left(C_{n,k} \frac{k^3}{n^2}\right)$$

where

(42) $$C_{n,k} = \max_{q,\gamma,\gamma''} E((V_{n,p}h_0)^*(\bar{\bar{W}})|Q = q, \Pi \upharpoonright Q = \gamma, \& \Pi'' \upharpoonright Q = \gamma'').$$

Of course the bounds in non-regular cases are even smaller and R_2 is analogous to R_1 so that

$$|R_1| + |R_2| = 0\left(C_{n,k}\frac{k^3}{n^2}\right). \tag{43}$$

Thus, by (10)

$$\begin{aligned} P\{W = 0\} &= E\, h_0(W) \\ &= \mathcal{B}_{n,p}h_0 - \frac{k(n-k)}{n(n-1)} E\,(V_{n,p}h_0)(\bar{W}) + 0\left(C_{n,k}\frac{k^3}{n^2}\right). \end{aligned} \tag{44}$$

The principal task that remains is to prove that

$$C_{n,k} = 0((1 - \tfrac{k}{n})^n) \tag{45}$$

for $k = o(n^{\frac{1}{2}})$. For this purpose we must show that results analogous to those of Lecture VII hold in a wider setting. With r a positive integer not exceeding 6, let $m = n - r$ and suppose we fix a kxn Latin rectangle $\mathcal{L}$ and let Π be a random 1 - 1 function on $\{1,\dots,m\}$ to an arbitrary m-element subset $\mathcal{X}$ of $\{1,\dots,n\}$ and let

$$W = \sum_{i=1}^{m} \mathcal{I}\{\Pi(i) \in S(i)\}. \tag{46}$$

The conditional distribution of $\bar{\bar{W}}$ in (42) is a special case of the distribution of such a W. We want to show that, with this modification, instead of (VII.22) and (VII.23) we still have

$$\left|P^{\Pi}(C) - \frac{(n-W)k}{n(n-1)}\right| = 0\left(\frac{k}{n^2}\right) \tag{47}$$

and

$$\left|P^{\Pi}(D) - \frac{W(n-k)}{n(n-1)}\right| = 0\left(\frac{k}{n^2}\right) \tag{48}$$

where the implied constant does not depend on $\mathcal{L}$. Of course it is understood that

(49) $$C = \{\Pi(I) \notin S(I) \ \& \ \Pi(J) \in S(I)\}$$

and

(50) $$D = \{\Pi(I) \in S(I) \ \& \ \Pi(J) \notin S(I)\}$$

where (I,J) is uniformly distributed over the set of all ordered pairs of distinct elements of $\{1,\dots,m\}$, independent of Π. The inequality (47) follows from the fact that

(51) $$(n-W-r)k \leq |\{(i,j): 1 \leq i,\ j \leq m \ \& \ \Pi(i) \notin S(i) \ \& \ \Pi(j) \in S(i)\}| \leq (n-W)k,$$

and (48) follows from

(52) $$W(n-k-r) \leq |\{(i,j): 1 \leq i,\ j \leq m \ \& \ \Pi(i) \in S(i) \ \& \ \Pi(j) \notin S(i)\}| \leq W(n-k).$$

Now let us look at the effect of these modifications of (VII.22) and (VII.23) on the remaining calculations in Lecture VII. First, each of the two terms in square brackets on the left-hand side of (VII.28) and of (VII.31) is multiplied by $1 + O(\frac{1}{n})$. This leads to an extra error term in (VII.36) of the order of

$$\frac{k}{n} E[|(U_{n,p}h)(W)| + |(U_{n,p}h)(W-1)|].$$

This change and changes arising from small changes in the probabilities of CD* and DD* clearly do not affect the order to magnitude of the final results of Lecture VII. In particular, (45) holds just as it would if the expectation in (42) were unconditional.

I shall conclude this lecture by trying to describe the present state of my understanding of this approach to the problem of counting Latin rectangles. Two possible improvements have occurred to me since the earlier pages were written. First, the leading term on the right-hand side of (10) can be simplified to the point where it is not completely intractable. Second, in trying to bound the remainder terms R_1 and R_2 defined by (11) and (12), it should be possible to exploit the possibility that $\bar{W}$ and $\bar{W}''$ are nearly exchangeable, even conditionally given CD* (or given DD*).

The first term on the right-hand side of (10) can be simplified in the following way. The conditional distribution of $\bar{W}$ given W is simple because it is obtained by dropping two randomly selected summands from W. Applying this and simplifying, we obtain

(53) $$E\,(V_{n,p}h)(\bar{W}) = E\,(\tilde{V}_{n,p}h)(W)$$

where

(54) $$(\tilde{V}_{n,p}h)(w) = \frac{n}{k}\sum_{\ell=0}^{n} \frac{w!(n-w)!}{\ell!(n-\ell)!}\left(\frac{k}{n-k}\right)^{\ell-w}\beta(w,\ell)h(\ell)$$

with

(55) $$\beta(w,\ell) = \gamma(w,\ell) + 2\,\frac{k}{n-k}\,\gamma(w-1,\ell) + \left(\frac{k}{n-k}\right)^2\gamma(w-2,\ell)$$

and, for $w \in \{0,\ldots,n-2\}$,

(56) $$\gamma(w,\ell) = \frac{(w+1)}{n(n-1)}\,\frac{n-k}{k}\,[\mathcal{B}_{n,p}h_{C^c_{w+1}} - \mathcal{I}\{\ell > w+1\}] - \frac{n-w-1}{n(n-1)}\,[\mathcal{B}_{n,p}h_{C^c_{w}} - \mathcal{I}\{\ell > w\}],$$

while $\gamma(w,\ell) = 0$ otherwise. Although this may look fairly complicated, some computations are simplified. In particular, for any positive integer j,

(57) $$(\tilde{V}^j_{n,p}h)(w) = \left(\frac{n}{k}\right)^j \sum_{\ell=0}^{n} \frac{w!(n-w)!}{\ell!(n-\ell)!}\left(\frac{k}{n-k}\right)^{\ell-w}\beta^j(w,\ell)h(\ell),$$

where β^j is the j^{th} power of the matrix β, and consequently

(58) $$\mathcal{B}_{n,p}(\tilde{V}^j_{n,p}h) = \left(\frac{n}{k}\right)^j \sum_{\ell=0}^{n}\binom{n}{\ell}\left(\frac{k}{n}\right)^{\ell}\left(1-\frac{k}{n}\right)^{n-\ell}\sum_{w=0}^{n}\beta^j(w,\ell)h(\ell).$$

These considerations should enable us to make substantial progress if we can show that the remainders R_1 and R_2 defined in (11) and (12) are very small. It may be helpful to change the notation slightly, rewriting (10) in the form

(59) $$E\,h(W) = \mathcal{B}_{n,p}h - \frac{k(n-k)}{n(n-1)}\,E\,(\tilde{V}_{n,p}h)(W) + Rh,$$

where

(60) $$Rh = (n-1)\, E\, [(V_{n,p}h)(\tilde{W}) - (V_{n,p}h)(\tilde{W}'')][\mathscr{I}(CD^*) - \mathscr{I}(DD^*)].$$

This can further be rewritten as

(61) $$E\, h(W) = \mathscr{B}_{n,p}[I + \frac{k(n-k)}{n(n-1)} \tilde{V}_{n,p}]^{-1}h + R^*h,$$

where

(62) $$R^*h = R[I + \frac{k(n-k)}{n(n-1)} \tilde{V}_{n,p}]^{-1}h.$$

Here, of course, I is the appropriate identity operator. The inverse can be approximated by use of

(63) $$\left[1 + \frac{k(n-k)}{n(n-1)} \tilde{V}_{n,p}\right]^{-1} = \sum_{j=0}^{\infty} \left(- \frac{k(n-k)}{n(n-1)}\right)^j \tilde{V}^j_{n,p},$$

with the aid of (57).

Intuitively it is fairly clear that there is some cancellation in the first bracket in (60), but I do not yet have any notion of the extent of this cancellation. For definiteness I shall discuss only the case $h = h_0$. We have seen that Rh_0 is of the order of $\frac{k^3}{n^2}(1- \frac{k}{n})^n$, at least for $k = o(n^{\frac{1}{2}})$. This used little more than the following facts:

(i) $P(CD^*) + P(DD^*) = O((\frac{k}{n})^2)$

(ii) $|\tilde{W} - \tilde{W}''| \leq 4$ and $P\{|\tilde{W} - \tilde{W}''| \geq j\} = O((\frac{k}{n})^j)$.

(iii) $\tilde{W}''$ has roughly the distribution of W, which can in turn be approximated by a binomial distribution with parameters n and $p = \frac{k}{n}$.

and

(iv) $\mathscr{B}_{n,p}\tilde{V}_{n,p}h_0 = O((1 - \frac{k}{n})^n)$.

However it is highly plausible that, even conditionally given $\mathscr{I}(CD^*) - \mathscr{I}(DD^*)$ and $\bar{\bar{W}}$, the random variables $\tilde{W}$ and $\tilde{W}''$ are nearly exchangeable. This should lead to a reduction of the order of magnitude of the bound for Rh_0, but I have not checked the details. However I have verified that this would imply that

(64) $$N_{k,n} = \left[(n!)^k \prod_{j=1}^{k-1} (1 - \frac{j}{n})^n\right] e^{\frac{k^2}{4n} + o(\frac{k^2}{n})},$$

in agreement with the leading part of Godsil and McKay's improvement on my result, which I have quoted in (3).

It might be useful to study the order of magnitude of Rh_0, perhaps, by simulation.