ON A COMBINATORIAL PROBLEM IN LATIN SQUARES

P. ERDŐS and A. GINZBURG[1]

1. Denote by S_n an arbitrary latin square with n elements $\{a_1, a_2, \ldots, a_n\}$. A row and column of this square, intersecting on the main diagonal (i.e. diagonal beginning at the left lower corner) will be called corresponding.

After striking out $n - c$ arbitrary rows and corresponding columns, a square T_c with $c \times c$ entries remains. Such a square will be called a principal minor. It is clearly determined by denoting its c elements belonging to the main diagonal.

Denote by $k_{i_1, i_2, \ldots, i_q}$ ($i_1, i_2, \ldots, i_q = 1, 2, \ldots, n$ all different) the number of columns in T_c containing the elements $a_{i_1}, a_{i_2}, \ldots, a_{i_q}$ simultaneously. Let $k^{(q)}$ be the minimum of $k_{i_1, i_2, \ldots, i_q}$. We shall consider the following problem:

Assuming that n and $k^{(q)}$ are two given positive integers, what is the minimal c (denoted by b), such that from an arbitrary S_n at least one T_c can be obtained with the prescribed $k^{(q)}$.

The problem is solved by a method used already in [1] and [2].

The question for the case of $k^{(2)}$ arises in connection with so called generalized normal multiplication tables of groups (and other systems) [3], [4], [5]. Such tables are complete (i.e. the product of any two group elements appears explicitly in them) if and only if $k^{(2)} \geq 1$. E.g. the following

10	9	8	6	5	2	0
8	7	6	4	3	0	13
5	4	3	1	0	12	10
4	3	2	0	14	11	9
2	1	0	13	12	9	7
1	0	14	12	11	8	6
0	14	13	11	10	7	5

is a generalized normal multiplication table of the group Z_{15} (the cyclic group of order 15). The multiplication is performed according to the rule

$$g_{ij} g_{jk} = g_{ik},$$

[1] Technion, Israel Institute of Technology, Haifa.

where g_{ij} is the element placed at the intersection of the i-th column and j-th row.

It can be directly inspected that in the above table $k^{(2)} = 1$ and it is really complete. It can also be shown that for $n = 15$ and $k^{(2)} = 1$, $b \geqq 7$.

2. From the definition of b follows directly

$$\binom{b}{q} b \geqq k^{(q)} \binom{n}{q}. \tag{1}$$

Assuming that the main diagonal is occupied by one element a_1, one improves (1) to

$$\binom{b-1}{q} b \geqq k^{(q)} \binom{n-1}{q}.$$

The following theorem gives an upper bound for b when $k^{(q)} = 1$.

Theorem. *In any given n by n latin square there can be found a principal minor of order not more than*

$$C n^{\frac{q}{q+1}} (\log n)^{\frac{1}{q+1}}.$$

(C a sufficiently large absolute constant) containing every q-tuple $(a_{i_1}, a_{i_2}, \ldots, a_{i_q})$ $(i_1, i_2, \ldots, i_q = 1, 2, \ldots, n$ all different) in some column.

Proof. We shall show that if $2t = \left[C n^{\frac{q}{q+1}} (\log n)^{\frac{1}{q+1}}\right]$ elements are chosen at random on the main diagonal, then all but $o\left(\binom{n}{2t}\right)$ of the principal minors so obtained will contain every q-tuple in some column.

For this it will suffice to show that the number of principal minors in which a given q-tuple $(a_1, a_2, \ldots, a_q)$ does not occur in any of its columns is $o\left(\dfrac{\binom{n}{2t}}{n^q}\right)$. We shall now estimate this number.

First we choose t elements at random. This can be done in $\binom{n}{t}$ ways.

Denote the chosen columns by $i_1, i_2, \ldots, i_t$. In every i_s $(1 \leqq s \leqq t)$ the elements $a_1, a_2, \ldots, a_q$ occur in the rows denoted correspondingly by $j_1^{(s)}$, $j_2^{(s)}, \ldots, j_q^{(s)}$. When choosing the remaining t elements on the diagonal we have to take care that none of the t q-tuples $(j_1^{(s)}, j_2^{(s)}, \ldots, j_q^{(s)})$ occurs amongst the t chosen elements, for otherwise $(a_1, a_2, \ldots, a_q)$ would occur in a column of our minor.

It is easy to show that there are at least $\dfrac{t}{q^2 - q + 1}$ of these q-tuples which are disjoint (this follows from the fact that there are at most q q-tuples which contain the same element). Denote the number of disjoint q-tuples by u. The number of t-tuples not containing any of the u q-tuples equals by a simple sieve process:

$$\binom{n-t}{t} - \binom{u}{1}\binom{n-t-q}{t-q} + \binom{u}{2}\binom{n-t-2q}{t-2q} - \cdots \tag{2}$$

It can be shown that the sum (2) is $o\left(\frac{\binom{n-t}{t}}{n^q}\right)$ if $2t = \left[Cn^{\frac{q}{q+1}}(\log n)^{\frac{1}{q+1}}\right]$ where C is a sufficiently large absolute constant. Our proof of this fact uses standard probabilistic arguments and is inelegant and therefore we supress it. (A proof due to Prof. N. G. DE BRUIJN is given in Addendum).

Now the total number of ways of choosing $2t$ elements on the diagonal so that no column of the obtained principal minor should contain the fixed q-tuple $(a_1, a_2, \ldots, a_q)$ is less than

$$\binom{n}{t} \cdot o\left(\frac{\binom{n-t}{t}}{n^q}\right) \cdot \frac{1}{\binom{2t}{t}} = o\left(\frac{\binom{n}{2t}}{n^q}\right).$$

Since there are $\binom{n}{q}$ q-tuples we obtain for all but $o\left(\binom{n}{2t}\right)$ choices principal minors of order $2t$ with every q-tuple in some column.

This completes the proof.

For $q = 1$ there is an explicit formula for the sum (2) (see [6] p. 316). In this case $u = t$ and $\sum_{v=0}^{t} (-1)^v \binom{t}{v}\binom{n-t-v}{t-v} = \binom{n-2t}{t}$.

Now $$\frac{\binom{n}{t}\binom{n-2t}{t}}{\binom{n}{2t}\binom{2t}{t}} = \frac{n!\,(n-2t)!\,(n-2t)!\,(2t)!\,t!\,t!}{(n-t)!\,t!\,(n-3t)!\,t!\,n!\,(2t)!} =$$

$$= \frac{(n-2t)(n-2t-1)\ldots(n-3t+1)}{(n-t)(n-t-1)\ldots(n-2t+1)} = \left(1 - \frac{t}{n-t}\right)\left(1 - \frac{t}{n-t-1}\right)\ldots$$

$$\ldots\left(1 - \frac{t}{n-2t+1}\right) < \left(1 - \frac{t}{n}\right)^t < e^{-\frac{t^2}{n}}.$$

For $2t = \left[Cn^{\frac{1}{2}}(\log n)^{\frac{1}{2}}\right]$ $e^{-\frac{t^2}{n}} = o\left(\frac{1}{n}\right)$ if $C > 2$.

3. At present we can not decide if this theorem is close to being best possible (from (1) it follows that in any case $b > n^{q/q+1}$). It seems though that it will not be easy to improve it with the method of this paper. Following a suggestion of Prof. H. HANANI we can show that for any p prime or a power of a prime a quadratic table of $p^2 + p + 1$ by $p^2 + p + 1$ can be constructed containing $p^3 + p^2 + p + 1$ elements, such that any pair of these elements occurs at least in one column of the table and no element occurs more than once in one column or one row of it. This can be done as follows: it is well known that from $p^2 + p + 1$ elements $p^2 + p + 1$ $p + 1$-tuples can be formed with every pair of elements in one (and only one) $p + 1$-tuple. Now replace every one of the above p^2+p+1 elements by p new elements and a „zero". The total number of the obtained elements will now be p^3+p^2+p+1 and they are divided in p^2+p+1 p^2+p+1-tuples. Every pair of the new elements occur clearly in one of the p^2+p+1-tuples. (Some of the pairs occur in $p+1$ such p^2+p+1-tuples.) It is easy to see that the replacing can be performed in such a way, that no element occurs twice in one row of the obtained quadratic table. This table can now be extended to a latin square, since it fulfils the condition of RYSER [7].

4. A number of unsolved problems arise in connection with the above one:

1) To find bounds for b in case when $k^{(q)}>1$.
2) Given three positive integers n, $k^{(q)}$, d. What is the minimal c such that from an arbitrary S_n at least one T_c can be obtained (if any) with

$$\max(k_{i_1,i_2,\ldots,i_q})-k^{(q)}\leqq d\,.$$

3) Given an arbitrary S_n. What is the c of the maximal minor (not necessarily principal) in which all elements are different.

Addendum

The following proof is due to Prof. N. G. DE BRUIJN.

$$\Sigma=\binom{m}{t}-\binom{u}{1}\binom{m-q}{t-q}+\binom{u}{2}\binom{m-2q}{t-2q}-\ldots=$$

$$=\frac{1}{2\pi i}\int(1+x)^m x^{t-1-m}\left[1-\frac{1}{(1+x)^q}\right]^u dx\,,$$

where the integration is performed along a circle around 0. There is a saddle point near $x=\frac{m}{t}$, so we take the radius of the circle equal to $\frac{m}{t}$. The contribution of the saddle point is about $\left[1-\left(1+\frac{m}{t}\right)^{-q}\right]^u$ times what it would be if $u=0$. If $u=0$ it has the value $\binom{m}{t}$, so under the assumption

$$t=C_1 m^{\frac{q}{q+1}}(\log m)^{\frac{1}{q+1}}\,,\quad u=\theta t\,,\quad \frac{1}{q^2-q+1}\leqq\theta\leqq 1\,,$$

u and q are integers, $q=O(1)$, we find for Σ

$$\Sigma\sim\binom{m}{t}\exp\left[-\left(\frac{t}{m}\right)^q u\right]=\binom{m}{t}\exp\left(-\theta C_1^{q+1}\log m\right).$$

So indeed it is $o\left(m^{-q}\binom{m}{t}\right)$ if C_1 is large enough.

(Received July 13, 1963)

BIBLIOGRAPHY

[1] Erdős, P.: "Graph theory and probability." I.: *Can. J. Math.* **11** (1959) 34—38. II.: *Can. J. Math.* **13** (1961) 346—352.
[2] Erdős, P.: "Some remarks on the theory of graphs." *Bull. Amer. Math. Soc.* **53** (1947) 292—294.
[3] Tamari, D.: "Les images homomorphes des groupoides de Brandt et l'immersion des semi-groupes." *Comptes rendus* **229** (1949) 1291—93.
[4] Tamari, D.: "Représentations isomorphes par de systèmes de relations. Systèmes associatifs." *Comptes rendus* **232** (1951) 1332—34.
[5] Ginzburg, A.: "Systèmes multiplicatifs de relations. Boucles quasiassociatives." *Comptes rendus* **250** (1960) 1413—16.
[6] Netto, E.: *Lehrbuch der Kombinatorik.* II. Auflage. Chelsea P. C. N. Y.
[7] Ryser, H. J.: "A combinatorial theorem with an application to latin rectangles." *Proc. Amer. Math. Soc.* **2** (1951) 550—552.

ОБ ОДНОЙ КОМБИНАТОРНОЙ ПРОБЛЕМЕ ЛАТИНСКИХ КВАДРАТОВ

P. ERDŐS и A. GINZBURG

Резюме

Авторы занимаются до сих пор не исследованными свойствами латинских квадратов. Оценивают сверху порядок миноров, обладающих некоторыми свойствами. Авторы указывают на то, что исследованные ими проблемы связаны с, так называемой, обобщенной нормальной таблицей операций. В конце работы отмечены открытые проблемы, из них особенно третья кажется интересной.