Studia Scientiarum Mathematicarum Hungarica 3 (1968) 459—464.

ON RANDOM MATRICES II

by

P. ERDŐS and A. RÉNYI

§ 0. Introduction

This paper is a continuation of our paper [1]. Let $\mathcal{M}(n)$ denote the set of all n by n zero-one matrices; let us denote the elements of a matrix $M_n \in \mathcal{M}(n)$ by ε_{jk} $(1 \leqq j \leqq n;\ 1 \leqq k \leqq n)$. Let p denote an arbitrary permutation $p = (p_1, p_2, \ldots, p_n)$ of the integers $(1, 2, \ldots, n)$ and Π_n the set of all $n!$ such permutations. Let us put for each $p \in \Pi_n$

$$\varepsilon(p) = \varepsilon_{1p_1} \cdot \varepsilon_{2p_2} \ldots \varepsilon_{np_n}. \tag{0.1}$$

Thus the permanent $\operatorname{perm}(M_n)$ of M_n can be written in the form

$$\operatorname{perm}(M_n) = \sum_{p \in \Pi_n} \varepsilon(p) \tag{0.2}$$

Thus each $\varepsilon(p)$ $(p \in \Pi_n)$ is a term of the expansion of $\operatorname{perm}(M_n)$.

Let us call two permutations $p' = (p'_1, \ldots, p'_n)$ and $p'' = (p''_1, \ldots, p''_n)$ $(p' \in \Pi_n, p'' \in \Pi_n)$ *disjoint* if $p'_k \neq p''_k$ for $k = 1, 2, \ldots, n$. Let now define (for each $M_n \in \mathcal{M}(n)$) $\nu = \nu(M_n)$ as the largest number of pairwise disjoint permutations $p^{(1)}, \ldots, p^{(\nu)}$ such that $\varepsilon(p^{(i)}) = 1$ $(i = 1, 2, \ldots, \nu)$. Clearly

$$\operatorname{perm}(M_n) \geqq \nu(M_n) \tag{0.3}$$

thus $\nu(M_n) \geqq 1$ is equivalent to $\operatorname{perm}(M_n) > 0$.

Let us denote by $\mathcal{M}(n, N)$ the set of those n by n zero-one matrices, among the n^2 elements of which exactly N elements are equal to 1 and the remaining $n^2 - N$ to 0 $(0 < N < n^2)$. Let us choose at random a matrix $M_{n,N}$ from the set $\mathcal{M}(n, N)$ with uniform distribution, i.e. so that each of the $\binom{n^2}{N}$ elements of $\mathcal{M}(n, N)$ has the same probability $\binom{n^2}{N}^{-1}$ to be chosen.

Let us denote by $P(n, N, r)$ the probability of the event

$$\nu(M_{n,N}) \geqq r \qquad (r = 1, 2, \ldots).$$

Clearly $P(n, N, 1)$ is the probability of the event $\operatorname{perm}(M_{n,N}) > 0$.

In [1] we have shown that if

$$N_1(n) = n \log n + cn + o(n) \tag{0.4}$$

where c is any fixed real number, one has

$$\lim_{n \to \infty} \mathsf{P}(n, N_1(n), 1) = e^{-2e^{-c}}. \tag{0.5}$$

This implies that if $\omega(n)$ tends arbitrarily slowly to $+\infty$ for $n\to+\infty$ and

$$N_1^*(n)=n\log n+\omega(n)n \tag{0.6}$$

then

$$\lim_{n\to\infty}\mathsf{P}(n, N_1^*(n), 1)=1. \tag{0.7}$$

In the present paper we shall extend this result, and prove the following

THEOREM 1. *For any fixed natural number r, if*

$$N_r^*(n)=n\log n+(r-1)n\log\log n+n\omega(n) \tag{0.8}$$

where $\omega(n)$ tends arbitrarily slowly to $+\infty$ for $n\to+\infty$, we have

$$\lim_{n\to+\infty}\mathsf{P}(n, N_r^*(n), r)=1. \tag{0.9}$$

Clearly (0. 7) is the special case $r=1$ of (0. 9). (0. 5) can be generalized in a similar way (see Theorem 2). Evidently, the interesting case is when $\omega(n)$ tends slower to $+\infty$ than $\log\log n$.

The method of the proof of Theorem 1 and 2 follows the same pattern as that in [1].

In § 2 we formulate — similarly as in [1] — an analogous result for random zero-one matrices with independent elements, while in § 3 we add some remarks and mention some related open problems.

§ 1. Random matrices with a prescribed number of zeros and ones

We prove in this § Theorem 1. We suppose $r\geqq 2$ as the theorem was proved for $r=1$ in [1].

Suppose that M is an n by n zero-one matrix belonging to the set $\mathcal{M}(n, N_r^*(n))$ where $N_r^*(n)$ is defined by (0. 8), and suppose that $\nu(M)\leqq r-1$.

Clearly we can delete from each row and column of such a matrix $r-1$ suitably selected ones so that the permanent of the remaining matrix M' should be equal to 0. As regards the matrix M' we distinguish two cases: either the deletion can be made so that M' contains a row or a column which consists of zeros only, or not. Let us denote by $Q_1(n, r)$ the probability of the first case, and by $Q_2(n, r)$ the probability of the second case. Clearly if a row (column) of M' consists of zeros only, the corresponding row (column) of M contains at most $r-1$ ones. Conversely, if M contains such a row or column, then clearly $\nu(M)\leqq r-1$. Thus $Q_1(n, r)$ is equal to the probability of the event that in M there is at least one row or column which contains at most $r-1$ ones. Thus we have

$$Q_1(n,r)\leqq 2n\sum_{j=0}^{r-1}\binom{n}{j}\frac{\binom{n^2-n}{N_r(n)-j}}{\binom{n^2}{N_r(n)}}=O(e^{-\omega(n)})=o(1). \tag{1.1}$$

Let us pass now to the second case. Let k be the least number such that one can find in M' either k columns and $n-k-1$ rows, or k rows and $n-k-1$ columns, which contain all the ones of M'; according to the theorem of Frobenius (see [2] and [3]) as perm $(M')=0$, such a k exists, and $1 \leqq k \leqq \left[\frac{n-1}{2}\right]$ because the case $k=0$ has already been taken into account (this was our first case). We may suppose that all ones of M' are covered by k columns and $n-k-1$ rows (the probability of the other case when the ones of M' are covered by k rows and $n-k-1$ columns being the same by symmetry). It follows — as in [1] — that M' contains a submatrix C' consisting of $k+1$ rows and k columns, such that each column of C' contains at least two ones. Let C be the corresponding submatrix of M. It follows that

$$Q_2(n,r) \leqq 2 \sum_{k=1}^{\left[\frac{n-}{2}\right]} q_k \tag{1.2}$$

where $q_k \left(1 \leqq k \leqq \left[\frac{n-1}{2}\right]\right)$ is the probability of the event that M contains a $k+1$ by k submatrix C such that each column of C contain at least two ones, and the submatrix D of M formed by the same rows as C and by those columns which do not intersect C, contains at most $r-1$ ones in each row. Evidently

$$q_k \leqq \binom{n}{k}\binom{n}{k+1}\binom{k+1}{2}^k \sum_{j=0}^{(k+1)(r-1)} \frac{\binom{(k+1)(n-k)}{j}\binom{n(n-k-1)+k(k-1)}{N_r^*-2k-j}}{\binom{n^2}{N_r^*}}. \tag{1.3}$$

It follows from (1.2) and by an asymptotic evaluation of the expression at the right hand side of (1.3) that

$$Q_2(n,r)=o(1). \tag{1.4}$$

As

$$1-\mathsf{P}(n, N_r^*(n), r) = Q_1(n,r)+Q_2(n,r) \tag{1.5}$$

it follows in view of (1.1) and (1.4) that (0.9) holds. Thus Theorem 1 is proved.

By the same method we can prove the following result, which generalizes (0.5) for $r \geqq 2$.

THEOREM 2. *If*

$$N_r(n) = n\log n+(r-1)n\log\log n+cn+o(n) \tag{1.6}$$

where $r \geqq 1$ *is an integer and* c *is any real number, we have*

$$\lim_{n\to+\infty} \mathsf{P}(n, N_r(n), r) = e^{-\frac{2e^{-c}}{(r-1)!}}. \tag{1.7}$$

§ 2. Random zero-one matrices with independent elements

Similarly as in [1] let us consider now random n by n matrices $M=(\varepsilon_{ij})$ $(1\leqq i,j\leqq n)$ such that the ε_{ij} are independent random variables which take on the values 1 and 0 with probabilities p_n and $(1-p_n)$. It can be shown that the following result is valid:

THEOREM 3. *For any fixed natural number r, put*

$$p_n = \frac{\log n + (r-1)\log\log n + \omega(n)}{n} \tag{2.1}$$

where $\omega(n)$ tends arbitrarily slowly to $+\infty$ and let M be an n by n random matrix the elements of which are independent random variables, taking on the values 1 *and* 0 *with probability p_n and $1-p_n$ respectively. Then the probability of $\nu(M)\geqq r$ tends to* 1 *for $n\to+\infty$.*

Note that the special case $r=1$ of Theorem 3 is contained in Theorem 2 of our previous paper [1].

As the idea of the proof is essentially the same as that of (0. 9), and the computation even somewhat simpler, we omit the proof of Theorem 3. Theorem 3 can be sharpened in the same way as Theorem 2 sharpens Theorem 1.

§ 3. Remarks and open problems

Let us put

$$\mu(n,k) = \min_{\substack{\nu(M_n)=k \\ M_n\in\mathcal{M}(n)}} \left(\operatorname{perm}(M_n)\right). \tag{3.1}$$

Clearly $\mu(n,1)=1$ and $\mu(n,2)=2$; however,for $k\geqq 3$ the question concerning the value of $\mu(n,k)$ is open. We have clearly $\mu(k,k)=k!$ and

$$\mu(k,k-1) = k!\left(\frac{1}{2!}-\frac{1}{3!}+\ldots+\frac{(-1)^k}{k!}\right) \tag{3.2}$$

but the value of $\mu(n,k)$ for $n\geqq k+2$ is not known. Clearly for determining $\mu(n,k)$ it is sufficient to consider those matrices M_n which contain exactly k ones in each row and in each column. As each such matrix is the sum of k disjoint permutation matrices, i.e. for such a matrix we have $\nu(M_n)=k$, thus the problem of determining $\mu(n,k)$ is the same as the problem raised by RYSER (see [7], p. 77) concerning the minimum of the permanent of n by n zero-one matrices having exactly k ones in each row and each column. Of course for particular values of n and k one can determine $\mu(n,k)$ (e.g. $\mu(5,3)=12$), but what would be of real interest is the asymptotic behaviour of $\mu(n,k)$ for fixed $k\geqq 3$ and $n\to+\infty$.

Let us put

$$\liminf_{n\to\infty} \sqrt[n]{\mu(n,k)} = \mu_k. \tag{3.3}$$

It seems likely that $\mu_k > 1$ for $k \geqq 3$. One reason for this conjecture is that if the conjecture of VAN DER WAERDEN is true, we have

$$\mu(n,k) \geqq \frac{k^n n!}{n^n} \geqq \left(\frac{k}{e}\right)^n \tag{3.4}$$

i.e. $\mu_k \geqq \frac{k}{e} > 1$ for $k \geqq 3$. We guess that μ_k is even larger than $\frac{k}{e}$.

If in particular M_n is the matrix defined by $\varepsilon_{j,j} = \varepsilon_{j,j+1} = \varepsilon_{j,j-1} = 1$ (we put $\varepsilon_{j,m} = \varepsilon_{j,m-n}$ for $m > n$) and $\varepsilon_{jl} = 0$ if $|l-j| \geqq 2$, then it can be easily shown that perm $(M_n) = L_n + 2$ where L_n is the n-th LUCAS number, i.e. the n-th term of the Fibonacci-type sequence

$$1, 3, 4, 7, 11, 18, \ldots \tag{3.5}$$

and

$$\lim_{n\to\infty} \sqrt[n]{L_n} = \frac{\sqrt{5}+1}{2} > \frac{3}{e}. \tag{3.6}$$

As regards $\mu(n,k)$, at present it is known only that

$$\lim_{n\to+\infty} \mu(n,3) = +\infty. \tag{3.7}$$

This was conjectured by MARSHALL HALL and proved by R. SINKHORN [8]. As a matter of fact, SINKHORN proved $\mu(n,3) \geqq n$ for all $n \geqq 3$. Of course (3. 7) implies $\lim_{n\to+\infty} \mu(n,k) = +\infty$ for $k = 4, 5, \ldots$ too.

An interesting open problem is the following: evaluate asymptotically $\mathsf{P}(n, n\log n + (r-1)n\log\log n, r)$ if r is not constant, but increases together with n.

There is a striking analogy between Theorem 1 and the following well known result (see e.g. [4]): If $N_r^*(n)$ balls are placed at random into n urns, and $N_r^*(n)$ is given by (0. 8) (with $\omega(n) \to +\infty$) then the probability of each urn containing at least r balls, tends to 1 for $n \to +\infty$. The relation between this problem and that of § 1 is made clear by the following remark. If we interpret the rows (columns) of M as urns and the ones as balls, then there are n urns, and each of the $N_r^*(n)$ „balls" falls with the same probability $1/n$ in any of the „urns".

In another paper ([5]) we have proved the following theorem (Theorem 1 of [5]): a random graph $\Gamma(n, N)$ with n vertices where n is even and $N = \frac{1}{2} n \log n + n\,\omega(n)$ edges where $\omega(n) \to +\infty$ for $n \to +\infty$, contains a factor of degree one with probability tending to 1 for $n \to +\infty$.

Theorem 1 of the present paper suggests the following problem: does a random graph $\Gamma(n, N)$ where n is even and

$$N = \frac{1}{2} n \log n + \frac{r-1}{2} n \log\log n + \omega(n) n$$

where $\omega(n) \to +\infty$, contain at least r *disjoint* factors of degree one with probability tending to 1 for $n \to \infty$? To prove this, besides the method of [5] the results of [6] have to be used.

REFERENCES

[1] ERDŐS, P. and RÉNYI A.: On random matrices, *Magyar Tud. Akad. Mat. Kutató Int. Közl* **8** (1964) 455—461.
[2] FROBENIUS, G.: Über zerlegbare Determinanten, *Sitzungsberichte der Berliner Akademie* 1917, 274—277.
[3] KÖNIG, D.: Graphok és matrixok, *Mat. Fiz. Lapok* **38** (1931) 116—119.
[4] ERDŐS, P. and RÉNYI, A.: On a classical problem of probability theory, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **6** (1961) 215—220.
[5] ERDŐS, P. and RÉNYI, A.: On the existence of a factor of degree one of a connected random graphs, *Acta Math. Acad. Sci. Hungar.* **17** (1966) 359—368.
[6] ERDŐS, P. and RÉNYI, A.: On the strength of connectedness of random graphs, *Acta Math. Acad. Sci. Hungar.* **12** (1961) 261—267.
[7] RYSER, H. J.: *Combinatorial mathematics,* Carus Math. Monographs, No. 14. Wiley, 1965.
[8] SINKHORN, R.: Concerning a conjecture of Marshall Hall (in print).

Mathematical Institute of the Hungarian Academy of Sciences, Budapest

(Received March 12, 1968.)