A MAGYAR TUDOMÁNYOS AKADÉMIA
MATEMATIKAI KUTATÓ INTÉZETÉNEK
KÖZLEMÉNYEI
VIII. ÉVFOLYAM, A SOROZAT, 3. FÜZET
1963

★

ТРУДЫ
МАТЕМАТИЧЕСКОГО ИНСТИТУТА
АКАДЕМИИ НАУК ВЕНГРИИ
ТОМ VIII, СЕРИЯ A, ВЫПУСК 3.
1963

★

PUBLICATIONS
OF THE
MATHEMATICAL INSTITUTE
OF THE
HUNGARIAN ACADEMY OF SCIENCES
VOLUME VIII, SERIES A, FASC. 3.
1963

Separatum

ON RANDOM MATRICES

by
P. ERDŐS and A. RÉNYI

AKADÉMIAI KIADÓ • BUDAPEST •
1964

ON RANDOM MATRICES

by

P. ERDŐS and A. RÉNYI

Introduction

In the present paper we deal with certain random $0-1$ matrices. Let $\mathscr{M}(n, N)$ denote the set of all n by n square matrices among the elements of which there are exactly N elements ($n \leqq N \leqq n^2$) equal to 1, all the other elements are equal to 0. The set $\mathscr{M}(n, N)$ contains clearly $\binom{n^2}{N}$ such matrices; we consider a matrix M chosen at random from the set $\mathscr{M}(n, N)$, so that each element of $\mathscr{M}(n, N)$ has the same probability $\binom{n^2}{N}^{-1}$ to be chosen. We ask now how large N has to be, for a given large value of n, in order that the permanent of the random matrix M should be different from zero with probability $\geqq \alpha$ where $0 < \alpha < 1$. By other words if $M = (\varepsilon_{jk})$ we want to evaluate asymptotically the probability $P(n, N)$ of the event that there exists at least one permutation $j_1, j_2, \ldots, j_n$ of the numbers $1, 2, \ldots, n$ such that the product $\varepsilon_{1j_1} \cdot \varepsilon_{2j_2} \ldots \varepsilon_{nj_n}$ should be equal to 1. A second way to formulate the problem is as follows: we shall say that two elements of a matrix are in independent position if they are not in the same row and not in the same column. Now our question is to determine the probability that the random matrix M should contain n elements which are all equal to 1 and are pairwise in independent position. A third way to state the problem is: what is the probability of the event that the permanent of the random $0-1$ matrix M should be positive?

We prove in § 1 (Theorem 1) that if

$$N(n) = n \log n + cn + o(n) \tag{1}$$

where c is an arbitrary real constant, then

$$\lim_{n \to +\infty} P(n, N(n)) = e^{-2e^{-c}}. \tag{2}$$

This implies that if

$$\lim_{n \to +\infty} \frac{N_1(n) - n \log n}{n} = +\infty, \tag{3}$$

then

$$\lim_{n \to +\infty} P(n, N_1(n)) = 1, \tag{4}$$

while if

$$\lim_{n \to +\infty} \frac{N_2(n) - n \log n}{n} = -\infty, \tag{5}$$

then

$$\lim_{n\to+\infty} P(n, N_2(n)) = 0\,. \tag{6}$$

This result can be interpreted also in the following way, in terms of graph theory. Let $\Gamma_{n,N}$ be a bichromatic random graph containing n red and n blue vertices, and N edges which are chosen at random among the n^2 possible edges connecting two vertices having different colour (so that each of the $\binom{n^2}{N}$ possible choices has the same probability). Then $P(n, N)$ is equal to the probability that the random graph $\Gamma_{n,N}$ should contain a factor of degree 1, i.e. $\Gamma_{n,N}$ should have a subgraph which contains all vertices of $\Gamma_{n,N}$ and n disjoint edges, i.e. n edges which have no common endpoint.

Clearly if the permanent of a matrix M consisting of zeros and ones is positive, then the matrix M does not contain a row or column all elements of which are equal to 0 (called in what follows for the sake of brevity a 0-row resp. 0-column), but conversely, if M does not contain a 0-row, nor a 0-column, it is not sure that its permanent is different from 0. However, from our result it follows that this is "almost" sure. As a matter of fact, Theorem 1 can be interpreted as follows: if $P(n, N)$ denotes the probability that perm $(M) > 0$ and $Q(n, N)$ the probability that M does not contain a 0-row or a 0-column, then if $N = N(n)$ is chosen so that for $n \to \infty$ we should have $Q(n, N(n)) \to 1$, then we have also $P(n, N(n)) \to 1$.

One can state this result somewhat vaguely also in the following way: if the permanent of a random matrix with elements 0 and 1 is equal to 0, then under the conditions of Theorem 1 this in most cases is due to the presence of a 0-row or a 0-column.

In § 2 we deal with a somewhat simpler variant of the problem, when the elements ε_{ij} $(1 \leqq i \leqq n,\ 1 \leqq j \leqq n)$ of the matrix M are *independent* random variables each taking on the values 0 and 1 with probability $1 - p$ and p respectively. The results obtained are analogous to those of § 1. In § 3 we add some remarks and mention some unsolved problems.

Besides elementary combinatorial and probabilistic arguments similar to that used by us in our previous work on random graphs (see [1], [2], [3], [4], [5]) our main tool in proving our results is the well-known theorem of D. KÖNIG (see [6]), which is nowadays well known in the theory of linear programming, according to which if M is an n by n matrix, every element of which is either 0 or 1, then the minimal number of lines (i.e. rows or columns) which contain all the 1-s, is equal to the maximal number of 1-s in independent position. As a matter of fact, for our purposes we need only the special case of this theorem, proved already by G. FROBENIUS [7], concerning the case when the maximal number of ones in independent position is equal to n.

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

Let $P(n, N)$ denote the probability of the event that the random matrix M $(M \in \mathcal{M}(n, N))$ has a positive permanent. According to the theorem of FROBENIUS—KÖNIG (see [6] and [7]) $1 - P(n, N)$ is equal to the probability that there exists a number k such that there can be found k rows and $n - k - 1$

columns of M which contain all the ones ($0 \leqq k \leqq n-1$). If we denote by $Q_k(n, N)$ the probability that there can be found k rows and $n-k-1$ columns or k columns and $n-k-1$ rows which contain all the ones, and k is the least number with this property, then clearly

$$0 \leqq 1 - P(n, N) = \sum_{k=0}^{\left[\frac{n-1}{2}\right]} Q_k(n, N). \tag{1.1}$$

Now we shall prove that if

$$N(n) = n \log n + cn + o(n) \tag{1.2}$$

where c is a real constant, then

$$\lim_{n\to\infty} \sum_{k=1}^{\left[\frac{n-1}{2}\right]} Q_k(n, N(n)) = 0, \tag{1.3}$$

further that

$$\lim_{n\to\infty} Q_0(n, N(n)) = 1 - e^{-2e^{-c}}. \tag{1.4}$$

Clearly (1.1), (1.3) and (1.4) imply that

$$\lim_{n\to\infty} P(n, N(n)) = e^{-2e^{-c}}, \tag{1.5}$$

which is the result we want to prove. Thus it remains only to prove (1.3) and (1.4). Let us consider first (1.4). Clearly $1 - Q_0(n, N(n))$ is equal to the probability of the event that the random matrix M does not contain a 0-row or a 0-column. Thus we have

$$1 - Q_0(n, N(n)) = \sum_{i=0}^{2n} (-1)^i S_i \tag{1.6}$$

where $S_0 = 1$ and

$$S_i = \sum_{h=0}^{i} \binom{n}{h}\binom{n}{i-h} \frac{\binom{(n-h)\ (n-i+h)}{N(n)}}{\binom{n^2}{N(n)}} \quad (i = 1, 2, \ldots, 2n), \tag{1.7}$$

further for each $l \geqq 0$

$$\sum_{i=0}^{2l+1} (-1)^i S_i \leqq 1 - Q_0(n, N(n)) \leqq \sum_{i=0}^{2l} (-1)^i S_i. \tag{1.8}$$

As clearly for each fixed value of i and for $n \to \infty$, if $N(n)$ is defined by (1.2) we have

$$S_i = \frac{2^i e^{-ci}}{i!}\left(1 + o(1)\right), \tag{1.9}$$

it follows that

$$\lim_{n\to\infty}\left(1-Q_0(n,N(n))\right)=\sum_{i=0}^{\infty}(-1)^i\frac{2^i e^{-ci}}{i!}=e^{-2e^{-c}}. \tag{1.10}$$

Thus (1.4) is proved. Now let us prove (1.3).

Let us suppose that M is a matrix such that all the ones of M are contained in k columns and $n-k-1$ rows ($k\geqq 1$), and k is the least number with this property. Then the matrix M can be partitioned into four matrices A, B, C, D as shown by Fig. 1, so that D consists only of zeros. Then clearly each column of C contains at least two ones, because if a column of C would contain not more than a single 1, then by leaving out this column and adding the row in which this 1 is contained, we would get a system of $k-1$ columns and $n-k$ rows which contain all the ones, in contradiction to our supposition of the minimum property of k.

	k	$n-k$
$n-k-1$	A	B
$k+1$	C	D

Fig. 1.

Thus it follows that

$$Q_k(n,N)\leqq 2\binom{n}{k}\binom{n}{k+1}\binom{k+1}{2}^k\frac{\binom{n(n-k-1)+k(k-1)}{N-2k}}{\binom{n^2}{N}} \tag{1.11}$$

and thus, that

$$Q_k(n,N(n))\leqq\left(\frac{A\log^2 n}{\sqrt{n}}\right)^k \quad \text{for} \quad k=1,2,\ldots,\left[\frac{n-1}{2}\right] \tag{1.12}$$

where A is a positive constant depending only on c. Thus we obtain

$$\sum_{k=1}^{\left[\frac{n-1}{2}\right]}Q_k(n,N(n))\leqq\frac{A\log^2 n}{\sqrt{n}-A\log^2 n}. \tag{1.13}$$

From (1.13) we obtain (1.3) and this completes the proof of (1.5).

Thus we obtained the following

Theorem 1. *Let $\mathscr{M}(n,N)$ denote the set of all n by n square matrices, among the n^2 elements of which N are equal to 1 and the other n^2-N to 0. Let M be selected at random from the set $\mathscr{M}(n,N)$ so that each of the $\binom{n^2}{N}$ elements of the set $\mathscr{M}(n,N)$ has the same probability $\binom{n^2}{N}^{-1}$ to be selected. Let $P(n,N)$ denote*

the probability of the event that the permanent of the random matrix M is positive. Then if

$$N(n) = n \log n + cn + o(n)$$

where c is any real constant, we have

$$\lim_{n\to\infty} P(n, N(n)) = e^{-2e^{-c}}.$$

§ 2. Random matrices with independent elements

In this § we prove the following theorem which is a variant of Theorem 1.

Theorem 2. *Let $M_n(p)$ be a random n by n matrix whose elements ε_{ij} $(1 \leqq i \leqq n;\ 1 \leqq j \leqq n)$ are independent random variables such that*

$$\mathbf{P}(\varepsilon_{ij} = 1) = p \quad \text{and} \quad \mathbf{P}(\varepsilon_{ij} = 0) = 1 - p. \tag{2.1}$$

Let $P_n(p)$ denote the probability of the event that the permanent of the random matrix $M_n(p)$ is positive. Then we have for

$$p_n = \frac{\log n + c}{n} + o\left(\frac{1}{n}\right) \tag{2.2}$$

$$\lim_{n\to\infty} P_n(p_n) = e^{-2e^{-c}}. \tag{2.3}$$

Proof of Theorem 2. The proof follows step by step the proof of Theorem 1. We have

$$0 \leqq 1 - P_n(p) \leqq \sum_{k=0}^{\left[\frac{n-1}{2}\right]} Q_{k,n}(p) \tag{2.4}$$

where $Q_{k,n}(p)$ denotes the probability that there can be found k rows and $n - k - 1$ columns, or k columns and $n - k - 1$ rows of $M_n(p)$ which contain all the 1-s, and k is the least number with this property. In this case we have

$$1 - Q_{0,n}(p) = \sum_{i=0}^{2n} (-1)^i S_i^* \tag{2.5}$$

where $S_0^* = 1$ and

$$S_i^* = \sum_{h=0}^{i} \binom{n}{h}\binom{n}{i-h}(1-p)^{in-h(i-h)}. \tag{2.6}$$

Thus we have for each fixed value of i if (2.2) holds

$$\lim_{n\to\infty} S_i^* = \frac{2^i e^{-ic}}{i!} \tag{2.7}$$

and therefore

$$\lim_{n\to\infty} (1 - Q_{0,n}(p_n)) = e^{-2e^{-c}}. \tag{2.8}$$

On the other hand we have now for $k = 1, 2, \ldots, \left[\frac{n-1}{2}\right]$

$$Q_{k,n}(p) \leqq 2\binom{n}{k}\binom{n}{k+1}\binom{k+1}{2}^k p^{2k}(1-p)^{(k+1)(n-k)} \tag{2.9}$$

and thus

$$Q_{k,n}(p_n) \leqq \left(\frac{B\log^2 n}{\sqrt{n}}\right)^k \quad \text{for} \quad k = 1, 2, \ldots, \left[\frac{n-1}{2}\right], \tag{2.10}$$

where the constant B depends on c only.

Thus

$$\lim_{n\to\infty} \sum_{k=1}^{n} Q_{k,n}(p_n) = 0 \tag{2.11}$$

and Theorem 2 follows.

§ 3. Some further remarks

The results of §§ 1 and 2 could be generalized for rectangular matrices of size m by n where $m < n$. In this case the question is: what is the probability that a random matrix of size m by n consisting of zeros and ones should contain m elements in independent position, which are all equal to 1?

Another possible generalization of our results would be to determine the probability distribution of the maximal number of ones in independent position in a random square matrix.

One may ask what can be said about the distribution of the *value* of the permanent of a random square matrix, under conditions of Theorems 1 and 2? It is easy to compute in both cases the mean value of the permanent perm (M); we have evidently under conditions of Theorem 1

$$\mathbf{E}(\mathrm{perm}(M)) = n!\,\frac{\binom{n^2-n}{N(n)-n}}{\binom{n^2}{N(n)}}$$

and under conditions of Theorem 2

$$\mathbf{E}\big(\mathrm{perm}(M_n(p_n))\big) = n!\,p_n^n.$$

It is easy to see, that these expressions are of the form $e^{n\log\log n + O(n)}$ and thus tend rather rapidly to $+\infty$. However one can not draw any conclusion from this fact, because as is easily seen, the variance of the permament is still much larger than the square of the mean value. An interesting related problem is of course to evaluate under the conditions of Theorem 1 and 2 the probability of the determinant of the random matrix being different from 0.

Another problem arises in connection with the graph-theoretical interpretation of the questions discussed in the present paper: To compute the probability that a random graph having n vertices and N edges should contain a factor of the first degree? We hope to return to these problems in another paper.

(Received November 11, 1963)