ON TWO PROBLEMS OF INFORMATION THEORY

by

PAUL ERDŐS and ALFRÉD RÉNYI

§ 1. Introduction

The first problem[1] which will be discussed in this paper can be formulated as follows: Suppose we are given n coins, which look quite alike, but of which some are false. (For instance suppose that the right coins consist of gold, while the false coins consist mainly of silver and are covered only by a thin layer of gold.) The false coins have a smaller weight than the right coins; the weights a and $b < a$ of both the right and false coins are known. A scale is given by means of which any number $\leqq n$ of coins can be weighed together. Thus if we select an arbitrary subset of the coins and put them together on the scale, then the scale shows us the total weight of these coins, from which it is easy to compute the number of false coins among those weighed. The question is what is the minimal number $A(n)$ of weighings by means of which the right and false coins can be separated? It can be seen by an elementary information-theoretical argument that (denoting by $\log_2 x$ the logarithm with base 2 of x)

$$A(n) \geqq \frac{n}{\log_2 (n+1)}. \tag{1.1}$$

As a matter of fact, the amount of information needed is $\log_2 2^n = n$ bits, because the subset of the coins consisting of the false coins may be any of the 2^n subsets of the set of all n coins; on the other hand if we put $k \leqq n$ coins on the balance, the number of false coins among them may have the values $0, 1, \ldots, k$ and thus the amount of information given by each weighing can not exceed $\log_2(k+1) \leqq \log_2(n+1)$. Thus s weighings can give us at most $s \log_2(n+1)$ bits, and thus to get the necessary amount of information (that is n bits) it is necessary that $s \log_2(n+1)$ should be not less than n; thus we obtain (1.1). On the other hand, a trivial upper estimate is

$$A(n) \leqq n \tag{1.2}$$

because if we put the coins one by one after another on the scale then clearly these n weighings are sufficient. The inequality (1.2) is best possible for $n = 1$, 2 and 3, but already for $n = 4$ we have $A(4) = 3$. As a matter of fact

[1] This problem was proposed for $n = 5$ by H.S. SHAPIRO [1] and for arbitrary n by N.J. FINE [2].

if we label the 4 coins by the numbers 1, 2, 3, 4 then the following 3 weighings are always sufficient: we put first the coins 1, 2, 3 on the scale, then the coins 1, 3, 4 and finally the coins 1, 2 and 4. Let the number of false coins among the coins 1, 2, 3 be f_1, that among 1, 3, 4 be f_2 and that among 1, 2, 4 be f_3. The following table gives us the false coins:

f_1	f_2	f_3	1	2	3	4
0	0	0	—	—	—	—
1	1	1	+	—	—	—
1	0	1	—	+	—	—
1	1	0	—	—	+	—
0	1	1	—	—	—	+
2	1	2	+	+	—	—
2	2	1	+	—	+	—
1	2	2	+	—	—	+
2	1	1	—	+	+	—
1	1	2	—	+	—	+
1	2	1	—	—	+	+
3	2	2	+	+	+	—
2	2	3	+	+	—	+
2	3	2	+	—	+	+
2	2	2	—	+	+	+
3	3	3	+	+	+	+

Note that among the possible 64 triples f_1, f_2, f_3 $(0 \leqq f_j \leqq 3,\ j = 1, 2, 3)$ only 16 are possible and each corresponds to a different distribution of the false coins.

It is easy to see that in general one has

$$A(nm) \leqq A(n) \cdot m \tag{1.3}$$

(because if we have nm coins we may determine by $A(n)$ weighings from each group of n coins the false ones). Thus from the above example one gets

$$A(4n) \leqq 3n$$

and as $A(n)$ is evidently monotonic, we obtain

$$A(n) \leqq \left\{ \frac{3n}{4} \right\} + 2 \tag{1.4}$$

where $\{x\}$ stands for the least integer $\geqq x$

It may be guessed[2] from this that one has

$$\lim_{n\to+\infty} \frac{A(n)}{n} = 0 . \tag{1.5}$$

This is in fact true; moreover we shall prove in § 1 that the lower estimate (1.1) gives the correct order of magnitude of $A(n)$. We shall prove namely in § 2 (Theorem 1) that for any $\delta > 0$ we have for $n \geqq n_0(\delta)$

$$A(n) \leqq (1 + \delta) \frac{n \cdot \log_2 9}{\log_2 n} \tag{1.6}$$

It remains an open question whether the limit

$$\lim_{n\to+\infty} \frac{A(n) \log_2 n}{n} = \alpha \tag{1.7}$$

exists, and if it exists, what is its value? We shall prove in § 4 (Theorem 3) that

$$\liminf_{n\to+\infty} \frac{A(n) \log_2 n}{n} \geqq 2 . \tag{1.8}$$

It follows from (1.8) that if the limit α in (1.7) exists one has $2 \leqq \alpha \leqq \log_2 9 \approx 3{,}17$. We shall prove in § 5 that if the problem is modified so that we are contented with finding a method of weighing which leads to the separation of the false coins with a prescribed probability $p < 1$ which may be arbitrarily near to 1, (supposing that all the 2^n possibilities have same probability) then $\frac{2n}{\log_2 n}(1 + \varepsilon)$ weighings are sufficient for any $\varepsilon > 0$ if n is large (Theorem 4).

Let us return now to the original problem of determining $A(n)$. This problem may be formulated as follows: We have to guess an unknown sequence of n digits, each digit being equal to 0 or 1. We have the right to select arbitrary „testing" sequences of zeros and ones of length n and with respect of each such sequence we are told what is the number of places in which a 1 stands both in the sequence to be guessed and in our testing sequence. The minimal number of testing sequences by means of which the unknown sequence can be uniquely determined whatever it may be, is equal to $A(n)$.

This reformulation of our first problem shows its connection with the second problem which will be discussed in this paper and which is as follows: Suppose we want to guess an unknown sequence of n digits, each digit being either 0 or 1. Information concerning the unknown sequence may be obtained in the following way: We have the right to select arbitrarily „testing" sequences of digits consisting of zeros and ones and we are told the number of places in which the two sequences coincide. Let $B(n)$ denote the minimal number of sequences by means of which we can determine the unknown sequence, whatever it may be. The problem is to determine the asymptotic behaviour of $B(n)$. Clearly we have

$$B(n) \geqq \frac{n}{\log_2 (n + 1)} . \tag{1.9}$$

[2] This conjecture was stated in [2].

The inequality (1.9) is obtained by a similar information-theoretical argument as that which leads us to (1.1). We have here the same trivial upper estimate

$$B(n) \leqq n . \tag{1.10}$$

As a matter of fact, if we select the n testing sequences 11 . . .1, 011 . . . 1, 1011 . . . 1, . . ., 111 . . . 101 then if k is the number of places in which the sequence 11 . . . 1 and the unknown sequence coincide, then the number of coincidences between the sequence 011 . . . 1 with the unknown sequence is either $k - 1$ or $k + 1$ according to whether the first digit of the unknown sequence is 1 or 0. Thus by the $2nd$, $3rd$, . . ., n—th testing sequences we can determine the first $n - 1$ digits of the unknown sequence; the last one can be determined because the total number k of ones in the unknown sequence is known from the first comparison. We have clearly $B(n) = n$ for $n = 1, 2, 3, 4$ and $B(5) = 4$ as can be seen from the following example: using the testing sequences

11111

11100

01010

01101

we can guess any sequence of 5 zero-or-one digits. As a matter of fact we get for the number of coincidences the following values for the 16 sequences consisting of not more than two ones:

sequence	coincidence with			
	11111	11100	01010	01101
00000	0	2	3	2
00001	1	1	2	3
00010	1	1	4	1
00100	1	3	2	3
01000	1	3	4	3
10000	1	3	2	1
00011	2	0	3	2
00101	2	2	1	4
01001	2	2	3	4
10001	2	2	1	2
00110	2	2	3	2
01010	2	2	5	2
10010	2	2	3	0
01100	2	4	3	4
10100	2	4	1	2
11000	2	4	3	2

It is unnecessary to try the other 16 sequences with 3 or more ones, because these are obtained by replacing 1 by 0 and 0 by 1 in the above 16 sequences, and this changes the number of coincidences from x to $5 - x$.

We shall prove for $B(n)$ the same inequality as obtained for $A(n)$; viz. we obtain in § 3 (Theorem 2) for any $\delta > 0$ that for $n \geqq n_1(\delta)$

$$B(n) \leqq (1 + \delta) \frac{n \log_2 9}{\log_2 n} . \tag{1.11}$$

Here again the question remains open whether the limit

$$\lim_{n \to +\infty} \frac{B(n) \log_2 n}{n} = \beta \tag{1.12}$$

exists, and if so what its value is. We shall show in § 4 (Theorem 5) by the same method which we have used to prove Theorem 3 that

$$\liminf_{n \to +\infty} \frac{B(n) \log_2 n}{n} \geqq 2 . \tag{1.13}$$

Thus if the limit β in (1.12) exists, then certainly $2 \leqq \beta \leqq \log_2 9 \approx 3{,}17$. We shall prove also in § 5 that if we modify our second problem so that we want to determine a fixed but unknown sequence of n zero-or-one digits by the number of coincidences with certain testing sequences and we are contented with finding it with probability $p < 1$ which may be arbitrarily near to 1 then $\frac{2n}{\log_2 n}(1 + \varepsilon)$ testing sequences are sufficient, (Theorem 6), for any $\varepsilon > 0$ if n is large enough.

Finally let us mention the following geometric interpretation of both problems. To any sequence of zeros and ones there corresponds a vertex of the unit cube C_n of n-dimensional space. The function $B(n)$ can be interpreted as follows: $B(n)$ denotes the least number such that by selecting $B(n)$ suitable chosen vertices of C_n each vertex of C_n is uniquely determined by its distances from the chosen $B(n)$ vertices.

Now let us interpret any sequence of n zeros and ones as a vector of the n-dimensional space leading from the origin to one of the vertices of C_n. With this interpretation $A(n)$ denotes the least number such that by selecting $A(n)$ vectors $v_1, v_2, \ldots, v_{A(n)}$ leading to suitably chosen vertices of C_n each vector v leading to a vertex of C_n is uniquely determined by its projection on the $A(n)$ chosen vectors, i. e. by the $A(n)$ numbers $(v, v_1), \ldots, (v, v_{A(n)})$ where (v, w) denotes the inner product of the vectors v and w.

We prove our Theorems 1 and 2 by the same method, consisting in a random selection of the testing sequences.

§ 2. An upper estimate for $A(n)$

Our first problem can be formulated as follows: What is the least value $A(n)$ of s such that there exists a matrix M having s rows and n columns and consisting of zeros and ones, such that if we select an arbitrary subset e of the set E of the columns of M, and form the row-sums of the submatrix $M(e)$ consisting of the selected colums of M, and denote by v_e the column-vector consisting of these row-sums, then the vectors v_e and $v_{e'}$ are different if e and e' are different subsets of E. We shall call such a matrix an A-matrix.

Thus $A(n)$ is the least value of s such that there exists an A-matrix with n columns and s rows. Clearly the matrix corresponding to the example given in the introduction for $n = 4$ is the A-matrix

$$\begin{matrix} 1110 \\ 1011 \\ 1101 \end{matrix} \tag{2.1}$$

The $2^4 = 16$ possible column-vectors v_e are in this case

$$\begin{matrix} 0\ 1\ 1\ 1\ 0\ 2\ 2\ 1\ 2\ 1\ 1\ 2\ 2\ 2\ 3\ 3 \\ 0\ 1\ 0\ 1\ 1\ 1\ 2\ 2\ 1\ 1\ 2\ 2\ 3\ 2\ 2\ 3 \\ 0\ 1\ 1\ 0\ 1\ 2\ 1\ 2\ 1\ 2\ 1\ 2\ 2\ 3\ 2\ 3 \end{matrix}$$

and all are different, thus the matrix (2.1) is in fact an A-matrix.

In order to estimate $A(n)$ we shall prove that if we choose M at random so that the sn elements of M are independent random variables, each taking on the values 0 and 1 with probability $\frac{1}{2}$, then the random matrix M will have the required property with positive probability (in fact with probability tending to 1 for $n \to +\infty$) provided that $s > (1+\delta)\dfrac{n \log_2 9}{\log_2 n}$.

This can be proved as follows: Let $\mathbf{P}_{s,n}(A)$ denote the probability that a random matrix M of order $s \times n$ is an A-matrix, and put $\mathbf{Q}_{s,n}(A) = 1 - \mathbf{P}_{s,n}(A)$. Let $A(e_1, e_2)$ (where e_1 and e_2 are different subsets of the set E of columns of M) denote the event that the row-sum vectors v_{e_1} and v_{e_2} are identical. Evidently if $v_{e_1} = v_{e_2}$ and the sets e_1 and e_2 are not disjoint, then putting $e_1' = e_1 - e_1 e_2$ and $e_2' = e_2 - e_1 e_2$, we have $v_{e_1'} = v_{e_2'}$. (Here and in what follows the product of sets denotes their intersection and the difference $e - f$ of two sets e and f denotes the set of elements of e which do not belong to f). It follows that is M is not an A-matrix, then there exist *disjoint* subsets e_1 and e_2 of the set of its columns such that $v_{e_1} = v_{e_2}$. Thus we obtain that

$$\mathbf{Q}_{s,n}(A) \leqq \sum_{e_1 \cdot e_2 = \varnothing} \mathbf{P}(A(e_1, e_2)) \tag{2.2}$$

where the summation has to be extended over every pair of disjoint subsets e_1 and e_2 of the set E of the columns of M and $\varnothing$ denotes the empty set.

It follows that

$$\mathbf{Q}_{s,n}(A) \leqq \sum_{1 \leqq k_1 + k_2 \leqq n} \frac{n!}{k_1! k_2! (n - k_1 - k_2)!} \left(\frac{\sum_{l=0}^{\min(k_1, k_2)} \binom{k_1}{l}\binom{k_2}{l}}{2^{k_1 + k_2}} \right)^s \tag{2.3}$$

By the well known identity

$$\sum_{l=0}^{\min(k_1, k_2)} \binom{k_1}{l}\binom{k_2}{l} = \binom{k_1 + k_2}{k_1}$$

we obtain

$$\mathbf{Q}_{s,n}(A) \leqq \sum_{1 \leqq k_1 + k_2 \leqq n} \frac{n!}{k_1! k_2! (n - k_1 - k_2)!} \left(\frac{\binom{k_1 + k_2}{k_1}}{2^{k_1 + k_2}} \right)^s .$$

It follows

$$\mathbf{Q}_{s,n}(A) \leqq \sum_{r=1}^{n} \binom{n}{r} \sum_{k=0}^{r} \frac{\binom{r}{k}^{s+1}}{2^{rs}} . \tag{2.4}$$

As

$$\binom{r}{k} \leqq \binom{r}{\left[\frac{r}{2}\right]} \qquad (k = 0, 1, \ldots, r) \tag{2.5}$$

further $\binom{r}{\left[\frac{r}{2}\right]} \leqq \frac{2^r}{\sqrt{r+1}}$ for $r = 3, 4, \ldots$ (this follows easily by induction) we obtain

$$\mathbf{Q}_{s,n}(A) \leqq \frac{4n^2}{2^s} + \sum_{r=3}^{n} \binom{n}{r} \frac{2^r}{(r+1)^{\frac{s}{2}}} . \tag{2.6}$$

Now we choose $s \sim \frac{\alpha n}{\log_2 n}$. As we have

$$\sum_{r \leqq \frac{n}{\log_2^2 n}} \binom{n}{r} 2^r = O(2^{c \frac{n \log\log n}{\log^2 n}})$$

where $c > 0$ is a constant, it follows that

$$\mathbf{Q}_{s,n}(A) \leqq \sum_{r > \frac{n}{\log_2^2 n}} \binom{n}{r} \frac{2^r}{(r+1)^{\frac{s}{2}}} + o(1) . \tag{2.7}$$

Taking into account that $\sum_{r=0}^{n} \binom{n}{r} 2^r = 3^n$, we obtain

$$\mathbf{Q}_{s,n}(A) \leqq 2^{n\left(\log_2 3 - \frac{\alpha}{2}\right) + o(n)} \tag{2.8}$$

provided that $s = s(n) \sim \frac{\alpha n}{\log_2 n}$ where $\alpha > 2 \log_2 3 = \log_2 9$. It follows

$$\lim_{n \to +\infty} \mathbf{Q}_{s(n),n}(A) = 0 . \tag{2.9}$$

Now clearly if $Q_{s(n),n}(A) < 1$ then $P_{s(n),n}(A) > 0$; as $P_{s,n}(A)$ is the probability that the random matrix M is an A-matrix, it follows that if $\delta > 0$ and $s > \frac{n \log_2 9}{\log_2 n}$ then for $n \geqq n_0(\delta)$ there exists an A-matrix of order $s \times n$ which implies $A(n) \leqq s$. Thus we proved the following

Theorem 1. *For any $\delta > 0$ we have for $n \geqq n_0(\delta)$*

$$A(n) \leqq (1 + \delta) \frac{n \log_2 9}{\log_2 n} . \tag{2.10}$$

§ 3. An upper estimate for $B(n)$

Let $u = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ and $u' = (\varepsilon_1', \varepsilon_2', \ldots, \varepsilon_n')$ be row-vectors consisting of n components, each of which is either 0 or 1. Let us put $c(u, u') = n - \sum_{i=1}^{n} (\varepsilon_i - \varepsilon_i')^2$ Thus $c(u, u')$ is the number of „coincidences" of the vectors u and u', i.e. the number of columns of the $2 \times n$ matrix $\begin{pmatrix} \varepsilon_1 & \ldots & \varepsilon_n \\ \varepsilon_1' & \ldots & \varepsilon_n' \end{pmatrix}$ which consist of equal elements. By the usual notation $\| u \|^2 = \sum_{i=1}^{n} \varepsilon_i^2$ we have

$$c(u, u') = n - \| u - u' \|^2. \tag{3.1}$$

Let now M be a matrix having s rows and n columns, and consisting of elements 0 and 1. Let $u_1, \ldots, u_s$ be the rows of M interpreted as vectors. Let u be an arbitrary row-vector consisting of n components which are either 0 or 1. Let U denote the set consisting of all 2^n such vectors u. To any u there corresponds a vector W_u consisting of the numbers $c(u, u_1), \ldots, c(u, u_s)$. The matrix M will be called a B-matrix if the 2^n vectors W_u corresponding to different elements u of U are all different from each other. Thus if M is a B-matrix, then each vector $u \in U$ is uniquely determined by the s numbers $c(u, u_1), \ldots, c(u, u_s)$ (and thus also by the distances $\| u - u_j \|$, $j = 1, 2, \ldots, s$). Let $P_{s,n}(B)$ denote the probability that the random matrix M of order $s \times n$ (whose elements are independent random variables each taking on the values 0 and 1 with probability $\frac{1}{2}$ should be a B-matrix, and put $\mathbf{Q}_{s,n}(B) = 1 - \mathbf{P}_{s,n}(B)$.

Let $u = (\varepsilon_1, \ldots, \varepsilon_n)$ and $u' = (\varepsilon_1', \ldots, \varepsilon_n')$ be two arbitrary different row-vectors consisting of n components each of which is either 0 or 1. Let H and $\bar{H}$ denote the set of those indices k $(1 \leqq k \leqq n)$ for which $\varepsilon_k = 1$ and $\varepsilon_k = 0$, respectively and similarly let H' and $\bar{H}'$ denote the set of those indices k $(1 \leqq k \leqq n)$ for which $\varepsilon_k' = 1$ and $\varepsilon_k' = 0$ respectively. Let k_1, k_2, k_3 and k_4 denote the number of elements of the sets HH', $H\bar{H}'$, $\bar{H}H'$ and $\bar{H} \cdot \bar{H}'$ respectively. Let $u_j = (\vartheta_{j1}, \ldots, \vartheta_{jn})$ be the j-th row of the random matrix M and let l_{j1}, l_{j2}, l_{j3} and l_{j4} denote the number of those indices k which belong to the sets HH', $H\bar{H}'$, $\bar{H}H'$ and $\bar{H}\bar{H}'$ respectively and for which $\vartheta_{jk} = 1$. Clearly we have $c(u, u_j) = c(u', u_j)$ if and only if

$$l_{j1} + l_{j2} + k_3 - l_{j3} + k_4 - l_{j4} = l_{j1} + l_{j3} + k_2 - l_{j2} + k_4 - l_{j4}$$

that is if

$$2(l_{j2} - l_{j3}) = k_2 - k_3 . \tag{3.2}$$

It follows that a necessary condition for $c(u, u_j) = c(u', u_j)$ is that $k_2 - k_3$ should be even, and further that

$$\mathbf{Q}_{s,n}(B) \leqq \sum_{\substack{k_2 + k_3 \equiv 0 \bmod 2 \\ 1 \leqq k_2 + k_3 \leqq n}} \frac{n!}{k_2!\, k_3!\, (n - k_2 - k_3)!} \left(\frac{\sum_{l=0}^{\frac{k_2 + k_3}{2}} \binom{k_2}{l} \binom{k_3}{l - \frac{k_2 - k_3}{2}}}{2^{k_2 + k_3}} \right)^s . \tag{3.3}$$

Now

$$\sum_{l=0}^{\frac{k_2+k_3}{2}} \binom{k_2}{l}\binom{k_3}{l-\frac{k_2-k_3}{2}} = \binom{k_2+k_3}{\frac{k_2+k_3}{2}}$$

and thus

$$\mathbf{Q}_{s,n}(B) \leqq \sum_{r=1}^{\left[\frac{n}{2}\right]} \binom{n}{2r} 2^{2r} \left(\frac{\binom{2r}{r}}{2^{2r}}\right)^s . \tag{3.4}$$

It follows similarly as in § 2 that if $s = s(n) \sim \alpha \dfrac{n}{\log_2 n}$ where $\alpha > \log_2 9$ then

$$\lim_{n\to+\infty} \mathbf{Q}_{s(n),n}(B) = 0 . \tag{3.5}$$

Clearly if $Q_{s(n),n}(B) < 1$ then $\mathbf{P}_{s(n),n}(B) > 0$ and thus there exists a B-matrix of order $s(n)\times n$ and therefore $B(n) \leqq s(n)$. Thus we have proved the following

Theorem 2. *For any $\delta > 0$ and $n \geqq n_1(\delta)$ one has*

$$B(n) \leqq (1+\delta)\frac{n\log_2 9}{\log_2 n} . \tag{3.6}$$

§ 4. Lower bounds for $A(n)$ and $B(n)$

In this § we prove the following results

Theorem 3. *One has*

$$\liminf_{n\to+\infty} \frac{A(n)\log_2 n}{n} \geqq 2 . \tag{4.1}$$

Theorem 4. *One has*

$$\liminf_{n\to+\infty} \frac{B(n)\log_2 n}{n} \geqq 2 . \tag{4.2}$$

Proof of Theorem 3. Let M be now an arbitrary A-matrix of order $s\times n$. Let us divide the row-vectors of M in two classes. A row-vector u of M belongs to the first class if it contains less than h elements equal to 1, where $h = \sqrt{n\log n}$; otherwise it belongs to the second class. We shall give first an upper estimate for the number of different column-vectors v_e consisting of the row-sums of the submatrix $M(e)$ of M consisting of the columns of M belonging to the set e; here e is an arbitrary subset of the set E of columns of M. Clearly any component of v_e corresponding to a row belonging to the first class may take on at most h different values. On the other hand if a row u_j of M belongs to the second class, and contains m ones ($m \geqq h$) then the number of possible choices of the subset e of the columns for which the sum of the elements of the row u_j standing in the selected columns does not lie between the bounds $\frac{m}{2} \pm \lambda\sqrt{m\log m}$ (where the positive constant λ will be chosen later) is equal to

$$2^{n-m} \sum_{\left|k-\frac{m}{2}\right| > \lambda\sqrt{m\log m}} \binom{m}{k} . \tag{4.3}$$

According to the Moivre—Laplace theorem we have

$$\sum_{\left|k-\frac{m}{2}\right|>\lambda\sqrt{m\log m}}\binom{m}{k}=O\left(\frac{2^m}{m^{2\lambda^2}}\right). \tag{4.4}$$

Let us call a subset e of the set E of columns a ,,bad'' subset, if there exists a row u_j belonging to the second class and containing m ones, for which the sum of the elements of u_j standing in the columns belonging to e lies outside the bounds $\frac{m}{2}\pm\lambda\sqrt{m\log m}$. Otherwise we call e a ,,good'' subset. Clearly by (4.4) if N denotes the number of bad subsets we have

$$N=O\left(\frac{n\,2^n}{h^{2\lambda^2}}\right)=O\left(\frac{2^n}{n^{(\lambda^2-1)}(\log n)^{\lambda^2}}\right). \tag{4.5}$$

Thus if $\lambda^2\geqq 1$ we have

$$N=O\left(\frac{2^n}{\log n}\right). \tag{4.6}$$

On the other hand, denoting by V the number of different values of the vector v_e if e runs over the good subsets, we have

$$V\leqq h^x[2\lambda\sqrt{n\log n}]^{s-x}\leqq(2\lambda\sqrt{n\log n})^s. \tag{4.7}$$

As M is by supposition an A-matrix, the inequality

$$V\geqq 2^n-N \tag{4.8}$$

has to be valid, which implies by (4.6) and (4.7)

$$(2\lambda\sqrt{n\log n})^s\geqq 2^n\left(1-O\left(\frac{1}{\log n}\right)\right). \tag{4.9}$$

Thus we obtain that the inequality

$$s\geqq\frac{2n}{\log_2 n+O(\log\log n)} \tag{4.10}$$

holds, from which Theorem 3 immediately follows.

Proof of Theorem 4. Theorem 4 can be proved in a similar way as we proved Theorem 3. The only difference is that the distinction between rows of the first and second class is now unnecessary. Let M be a B-matrix of order $s\times n$. Let U denote again the set of all possible rows of n elements each of which is equal either to 0 or to 1. Let $u_1, u_2, \ldots, u_s$ denote the rows of the matrix M. An element u of U will be called ,,bad'' if there is a row u_j of M such that the number of coincidences $c(u, u_j)$ of u and u_j, does not lie in the interval $\frac{n}{2}\pm\lambda\sqrt{n\log n}$; otherwise u will be called ,,good''. If N denotes the number of ,,bad'' elements u of U we have by Chebyshev's inequality

$$N=O\left(\frac{2^n}{\log n}\right). \tag{4.11}$$

On the other hand if W denotes the number of possible values of the vector $w_u = (c(u, u_1), \ldots, c(u, u_s))$ where u runs over the „good" elements of U, we have

$$W \leqq (2\sqrt{n \log n})^s . \tag{4.12}$$

As M is a B-matrix, we have

$$W \geqq 2^n - N. \tag{4.13}$$

Thus it follows from (4.11) and (4.12) that

$$s \geqq \frac{2n}{\log_2 n + O(\log\log n)} \tag{4.14}$$

which proves Theorem 4.

§ 5. Discussion of a modified form of both problems

Let U denote again the set of all possible sequences of length n consisting of zeros and ones. Let M denote again a matrix of order $s \times n$ consisting of zeros and ones; let $u_1, \ldots, u_s$ denote the rows of M. Let (u, u') where $u \in U$, $u' \in U$ denote the inner product of the vectors u and u', i.e. the number of places in which 1 stands both in u and u'. Let $c(u, u') = n - \|u - u'\|^2$ denote the number of coincidences of the vectors u and u', i.e. the number of places in which the same number stands both in u and u'. A matrix M will be called a p-A matrix (resp. a p-B matrix) where $0 < p < 1$ if by choosing at random an element u of U (so that each of the 2^n elements of U has the same probability to be chosen) the probability that u is uniquely determined by the sequence of numbers $(u, u_1), (u, u_2), \ldots, (u, u_s)$ (resp.. by the sequence $c(u, u_1)$, $c(u, u_2), \ldots, c(u, u_s)$) exceeds p. Let $s_A(n, p)$ and $s_B(n, p)$ respectively denote the minimal value of s for which a p-A matrix resp. a p-B matrix M of order $s \times n$ exists. Then the following results hold:

Theorem 5. *For any fixed p with $0 < p < 1$ one has*

$$\lim_{n \to +\infty} \frac{s_A(n, p)}{\left(\frac{2n}{\log_2 n}\right)} = 1 . \tag{5.1}$$

Theorem 6. *For any fixed p with $0 < p < 1$ one has*

$$\lim_{n \to +\infty} \frac{s_B(n, p)}{\left(\frac{2n}{\log_2 n}\right)} = 1 . \tag{5.2}$$

Proof of Theorems 5 and 6. Let M denote the set of all $s \times n$ matrices the elements of which are zeros and ones. Let $\mathbf{P}_A(M)$ and $\mathbf{P}_B(M)$ resp. denote the probability that by choosing at random an element u of U this element should be uniquely determined by the sequence $(u, u_1), (u, u_2), \ldots, (u, u_s)$ resp. by the sequence $c(u, u_1), c(u, u_2), \ldots, c(u, u_s)$ where $u_1, \ldots, u_s$ denote the rows of the

matrix M. Clearly the assertions that $s_A(n, p) \leqq s$ and $s_B(n, p) \leqq s$ resp. are equivalent to the assertions that

$$\max_{M \in \mathsf{M}} \mathbf{P}_A(M) \geqq p \tag{5.3}$$

and

$$\max_{M \in \mathsf{M}} \mathbf{P}_B(M) \geqq p\,. \tag{5.4}$$

Evidently if $\overline{\mathbf{P}_A(M)}$ and $\overline{\mathbf{P}_B(M)}$ denote the mean value of $\mathbf{P}_A(M)$ and $\mathbf{P}_B(M)$ when M is chosen at random so that M may be equal to any element of M with the same probability $\frac{1}{2^{sn}}$, then

$$\max_{M \in \mathsf{M}} \mathbf{P}_A(M) \geqq \overline{P_A(M)} \tag{5.5}$$

and

$$\max_{M \in \mathsf{M}} \mathbf{P}_B(M) \geqq \overline{P_B(M)}\,. \tag{5.6}$$

Thus if we prove that for a certain value of s we have

$$\overline{\mathbf{P}_A(M)} \geqq p$$

and

$$\overline{\mathbf{P}_B(M)} \geqq p\,,$$

it follows that the inequalities $s_A(n, p) \leqq s$ and $s_B(n, p) \leqq s$ hold.

Let $A(u, M)$ denote the event that the row vector $u \in U$ is uniquely determined by the sequence $(u, u_1), \ldots, (u, u_s)$ and $B(u, M)$ the event that the row vector $u \in U$ is uniquely determined by the sequence $c(u, u_1), \ldots, c(u, u_s)$ where $u_1, \ldots, u_s$ denote the rows of M. Then evidently

$$\overline{\mathbf{P}_A(M)} = \mathbf{P}(A(u, M)) \tag{5.7}$$

and

$$\overline{\mathbf{P}_B(M)} = \mathbf{P}(B(u, M)) \tag{5.8}$$

where on the right hand side of (5.7) and (5.8) u is a randomly chosen element of U and M a randomly chosen element of M. Let us put

$$1 - \mathbf{P}(A(u, M)) = \mathbf{Q}_A(s, n) \tag{5.9}$$

and

$$1 - \mathbf{P}(B(u, M)) = \mathbf{Q}_B(s, n). \tag{5.10}$$

We obtain by a similar argument as that used in § 2 and § 3 resp.

$$\mathbf{Q}_A(s, n) \leqq \sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^n} \sum_{i+j>0} \binom{k}{i} \binom{n-k}{j} \left[\frac{\binom{i+j}{i}}{2^{i+j}} \right]^s \tag{5.11}$$

and

$$\mathbf{Q}_B(s,n) \leqq \sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^n} \sum_{\substack{i \equiv j \bmod 2 \\ i+j>0}} \binom{k}{i} \binom{n-k}{j} \left[\frac{\binom{i+j}{\frac{i+j}{2}}}{2^{i+j}} \right]^s. \tag{5.12}$$

and therefore

$$\mathbf{Q}_A(s,n) \leqq \left(\sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^n} \right) \sum_{l=1}^{n} \binom{n}{l} \sum_{i=0}^{l} \left[\frac{\binom{l}{i}}{2^l} \right]^s$$

and

$$\mathbf{Q}_B(s,n) \leqq \left(\sum_{k=0}^{n} \binom{n}{k} \frac{1}{2^n} \right) \sum_{l=1}^{\left[\frac{n}{2}\right]} \binom{n}{2l} \left[\frac{\binom{2l}{l}}{2^{2l}} \right]^s.$$

Using again the inequalities $\binom{l}{i} \leqq \binom{l}{\left[\frac{l}{2}\right]} \leqq \frac{2^l}{\sqrt{l+1}}$

it follows that

$$\mathbf{Q}_A(s,n) \leqq \sum_{l=1}^{n} \frac{\binom{n}{l}}{(l+1)^{s/2-1}} \tag{5.13}$$

and

$$\mathbf{Q}_B(s,n) \leqq \sum_{l=1}^{\left[\frac{n}{2}\right]} \frac{\binom{n}{2l}}{(2l+1)^{s/2}}. \tag{5.14}$$

Thus if $s \sim \frac{\alpha n}{\log_2 n}$ we obtain

$$\mathbf{Q}_A(s,n) \leqq 2^{n\left(1-\frac{\alpha}{2}\right)+O\left(\frac{n \log\log n}{\log n}\right)} \tag{5.15}$$

and similarly

$$\mathbf{Q}_B(s,n) \leqq 2^{n\left(1-\frac{\alpha}{2}\right)+O\left(\frac{n \log\log n}{\log n}\right)}. \tag{5.16}$$

Thus if $\alpha > 2$ we have

$$\lim_{n\to+\infty} \mathbf{Q}_A(s,n) = \lim_{n\to+\infty} \mathbf{Q}_B(s,n) = 0. \tag{5.17}$$

By (5.9) and (5.10) this implies

$$\lim_{n\to+\infty} \mathbf{P}(A(u,M)) = \lim_{n\to+\infty} \mathbf{P}(B(u,M)) = 1 \tag{5.18}$$

and thus by (5.5)—(5.8) if follows

$$\lim_{n\to+\infty} \max_{M\in\mathsf{M}} \mathbf{P}_A(M) = \lim_{n\to+\infty} \max_{M\in\mathsf{M}} \mathbf{P}_B(M) = 1 . \tag{5.19}$$

As mentioned above this proves Theorems 5 and 6.

(Received July 28, 1963.)

REFERENCES

[1] SHAPIRO, H. S.: „Problem E 1399." *American Mathematical Monthly* **67** (1960) p. 82.
[2] FINE, N. I.: „Solution of problem E 1399." *American Mathematical Monthly* **67** (1960) p. 697.

Remark, added on september 24, 1963

Since the present paper was given to print, we have been informed that quite a number of mathematicians worked on the first problem of the present paper, and obtained results which are closely related to our results. None of these results are published but some of them are in print. As W. MOSER informed us, D. G. CANTOR has proved in a paper in print in the Canadian Journal of Mathematics the relation (1.5); in fact he obtained the estimate $A(n) = O\left(\frac{n \operatorname{loglog} n}{\log n}\right)$. L. MOSER (University of Alberta, Edmonton) informed us that, he obtained together with ABBOT, that

$$\limsup_{n\to+\infty} \frac{A(n)\log_2 n}{n} \leqq \log_2 27 . \tag{*}$$

While this upper bound is greater by the factor $^3/_2$ than our bound $\log_2 9$, the method of proof applied by ABBOTT and L. MOSER has the advantage that it is constructive; they exhibit effectively A-matrices of size $s \times n$ where $s \sim \frac{n \log_2 27}{\log_2 n}$.

The same result has been obtained by H. S. SHAPIRO and S. SÖDERBERG. Their paper is in print in the *American Mathematical Monthly*. E. R. BERLEKAMP (Bell Telephone Laboratories) has obtained by a method, essentially the same as our method, that

$$A(n) \leqq \frac{n \log_2 9}{\log_2 n} .$$

This result is slightly better than our result (1.6) (by the factor $1 + \delta$). To get rid of the unnecessary factor $(1 + \delta)$ one has to use instead of the rough estimate (2.5) a sharper estimate following from Stirling's formula.

BERLEKAMP conjectured also that (1.8) holds, and gave a heuristic argument for his conjecture.

Other proofs of (1.8) have been given by B. GORDON (University of California, Los Angeles) and L. MOSER. E. MILLS has also proved that $A(n) = O\left(\frac{n}{\log n}\right)$. Quite recently B. LINDSTRÖM (University of Stockholm) has proved the conjecture (1.7) with $\alpha = 2$. His paper will be printed in the next issue of this journal.

О ДВУХ ПРОБЛЕМАХ ТЕОРИИ ИНФОРМАЦИИ

P. ERDŐS и A. RÉNYI

Резюме

Пусть U множество всех 2^n последовательностей $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$ где $\varepsilon_k = 0$ или $\varepsilon_k = 1$ $(k = 1, 2, \ldots, n)$. Пусть M некоторая матрица с размерами $s \times n$, элементы которой все равны или 0 или 1. Пусть $u_1, \ldots, u_s$ строки матрицы M. Положим для $u = (\varepsilon_1, \ldots, \varepsilon_n) \in U$ и $u' = (\varepsilon_1' \ldots, \varepsilon_n') \in U$

$(u, u') = \sum_{k=1}^{n} \varepsilon_k \varepsilon_k'$ и $c(u, u') = n - \sum_{k=1}^{n} (\varepsilon_k - \varepsilon_k')^2 = n - \|u - u'\|^2$. Матрица M

называется A-матрицой (соотв. B-матрицой) если все элементы u от U однозначно определены заданием чисел $(u, u_1), \ldots, (u, u_s)$ (соотв. чисел $c(u, u_1), \ldots, c(u, u_s)$). Пусть $A(n)$ (соотв. $B(n)$) означает минимальное значение s для которого существует A-матрица (соотв. B-матрица) с размерами $s \times n$.

В работе доказано, что

$$2 \leqq \liminf_{n \to +\infty} \frac{A(n) \log_2 n}{n} \leqq \limsup_{n \to +\infty} \frac{A(n) \log_2 n}{n} \leqq \log_2 9$$

и

$$2 \leqq \liminf_{n \to +\infty} \frac{B(n) \log_2 n}{n} \leqq \limsup_{n \to +\infty} \frac{B(n) \log_2 n}{n} \leqq \log_2 9 .$$