ON A COMBINATORY DETECTION PROBLEM I

by

BERNT LINDSTRÖM[1]

1. Introduction

The present investigation was inspired by the work of H. S. SHAPIRO and S. SÖDERBERG [4] on a weighing problem:

"Counterfeit coins weigh 9 grams and genuine coins weigh 10 grams. Given a scale that weighs all real numbers exactly, what is the minimum number of weighings required to extract all the counterfeits from a sample of n coins"?.

The schemes for finding the counterfeits are of two kinds; (1) either one determines in advance which coins are to be weighed together in each weighing or (2) the choice of coins for a weighing is made to depend on the results of all previous weighings. I shall only consider schemes of the first kind. Then the problem can be given a formulation in terms of sets.

Detection Problem. Let S be a given set of $|S| = n$ elements. A family $\mathcal{F}$ of subsets $T_1, T_2, \ldots, T_m$ of S is a *detecting family* for S if each subset M of S is uniquely determined by the m numbers $|M \cap T_i|$, $i = 1, 2, \ldots, m$. Then the problem is to find $f(n) = \min m$ is the class of all detecting families for S.

It is easy to prove that $f(4) = 3$ and $f(5) = 4$, but for larger n the determination of $f(n)$ is difficult. Therefore one must in the first instance search for good estimates.

Since there are at most $(n+1)^m$ combinations of values for the numbers $|M \cap T_i|$, $(i = 1, \ldots, m)$ and different combinations correspond to the 2^n different subsets of S, we find that $2^n \leqq (n+1)^m$ and

$$f(n) \geqq \frac{n \log 2}{\log (n+1)}. \tag{1.1}$$

The main achievement of H. S. SHAPIRO and S. SÖDERBERG was the proof of

$$f(n) = O\left(\frac{n}{\log n}\right). \tag{1.2}$$

P. ERDŐS and A. RÉNYI have given a proof [1] of the inequality

$$\liminf_{n\to\infty} \frac{f(n) \log n}{n} \geqq \log 4. \tag{1.3}$$

[1] Stockholm.

This inequality has also been proved by B. GORDON, L. MOSER and myself (see [1] Remark). Although my proof is not the shortest it may have some interest as an application of information theory.

But my main result is

$$\limsup_{n\to\infty} \frac{f(n)\log n}{n} \leqq \log 4\,, \tag{1.4}$$

thus confirming a conjecture in [1] that the limit exists.

I am grateful to Professor H. S. Shapiro for stimulating discussions during his stay in Stockholm. I also express my thanks to Prof. O. Frostman, who suggested many simplifications in my proofs.

2.

The following two inequalities are easy consequences of the definition.

$$f(n) \leqq f(n+1)\,, \qquad n = 1,2\,,\ldots \tag{2.1}$$

$$f(n_1+n_2) \leqq f(n_1)+f(n_2)\,, \qquad n_1, n_2 = 1,2\,,\ldots\,. \tag{2.2}$$

In order to prove (2.1) we note that if $T_1, \ldots, T_m$ is a detecting family for S and T is any subset of S then $T \cap T_1, \ldots, T \cap T_m$ is a detecting family for $T \cap S$. Take $|S| = n+1$, $|T| = n$, $m = f(n+1)$ and (2.1) follows.

Now, let S_1 and S_2 be two disjoint sets and $\mathcal{F}_i$: $T_{i_1}, \ldots, T_{im_i}$ a detecting family for S_i $(i = 1, 2)$. Then $\mathcal{F}$: $T_{11}, \ldots, T_{1m}, T_{21}, \ldots, T_{2m_2}$ is a detecting family for $S_1 \cup S_2$. With $|S_i| = n_i$, $m_i = f(n_i)$, $(i = 1, 2)$ we get (2.2).

It is suitable to use vectors representing sets, and matrices representing families of sets. Define $S_n = \{1, 2, \ldots, n\}$. A subset T of S_n can be represented by an n-dimensional column vector x with „1" in the i-th position if $i \in T$ and „0" if $i \notin T$. A family $\mathcal{F}$: $T_1, \ldots, T_m$ of subsets in S_n can be represented by an $m \times n$ matrix $A = (a_{ij})$ with $a_{ij} = 1$ *if* $j \in T_i$ and $a_{ij} = 0$ if $j \notin T_i$. With this mode of representing sets we find that Ax is an m-dimensional column vector with $|T \cap T_i|$ in its i-th position $(i = 1, \ldots, m)$. If $\mathcal{F}$ is detecting family for S_n we say that the corresponding matrix A is a *detecting matrix*.

Suppose A is a matrix, all of whose entries are 0 or 1, which has the property that $Ax = Ay$ implies $x = y$ for x, y columnvectors with entries 0 or 1. Then A evidently is a detecting matrix.

For convenience we introduce vectors ξ with entries from the set $\{-1, 0, 1\}$. Then the above statement can be expressed in the form:

A is a detecting matrix if $A\xi = 0$ implies $\xi = 0$.

Example. To the family $\{1, 3, 4\}$, $\{1, 2\}$, $\{2, 3\}$ of subsets of S_4 corresponds the matrix

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

which is easily proved to be a detecting matrix. ([4] p. 1069).

3.

In this section we prove the following result

Theorem 1. $f(k\,2^{k-1}) \leqq 2^k - 1\,, \qquad k = 2,3\,, \ldots .$

In order to prove this theorem we shall prove the existence of a $(2^k - 1) \times$ $\times k2^{k-1}$ detecting matrix A_k for every integer $k \geqq 2$. The matrix A_k will be of the form

$$A_k = B_k \,|\, C_k^{L_1} \,|\, C_k^{L_2} \,|\, \ldots \,|\, C_k^{L_t}\,,$$

where B_k, $C_k^{L_1}$ etc. are certain matrices to be defined later, and the bars indicate that they must be put together side by side. Before we define them we shall prove three lemmas.

From now on, the set $S_k = \{1, 2, \ldots, k\}$ and its subsets will only be used as indices for numbers and matrices. Suppose that a number a_M is given for every subset $M \subset S_k$. For any $N \subset S_k$ and $i \in N$ we put $N^- = N - \{i\}$ and get

$$\sum_{M \subset N} a_M = \sum_{M \subset N^-} (a_M + a_{M \cup (i)})\,, \tag{3.1}$$

where summations are taken over all subsets, the null set $\emptyset$ included.

In the following three lemmas the numbers a_i, b_i, a_M, b_M take only the values 0 or 1. The number of elements in a set $N \subset S_k$ is denoted by $|N|$.

Lemma 1. Choose numbers $a_1, a_2, \ldots, a_k$. *Put* $a_\emptyset = 0$ *and define* a_M *for every other subset* $M \subset S_k$ *by the aid of the congruence*

$$a_M \equiv \sum_{i \in M} a_i \pmod 2 \tag{3.2}$$

The for every $N \subset S_k$

$$\sum_{M \subset N} a_M = 0 \quad \text{or} \quad 2^{|N|-1}\,. \tag{3.3}$$

Lemma 2. Choose numbers $a_1, a_2, \ldots, a_k$ *(not all 0) and* $b_1, b_2, \ldots, b_k$ *(not all 0). Put* $a_\emptyset = b_\emptyset = 0$ *and define* a_M *and* b_M *as above by the aid of* (3.2). *Then*

$$\begin{aligned} \sum_{M \subset S_k} a_M b_M &= 2^{k-1} \quad \text{if} \quad a_i = b_i \quad \text{for} \quad i = 1,2\,, \ldots, k \\ &= 2^{k-2} \quad \text{if} \quad a_i \neq b_i \quad \text{for some } i\,. \end{aligned} \tag{3.4}$$

Lemma 3. *Let* L *be any subset of* S_k. *Choose a number* a_M *for every non-void* $M \subset L$. *Put* $a_\emptyset = 0$ *and define* a_M *for every* $M \not\subset L$ *by the aid of the congruence*

$$a_M \equiv a_{M \cap L} + |M - M \cap L| \pmod 2\,. \tag{3.5}$$

Then for every $N \subset S_k$ *for which* $N \not\subset L$

$$\sum_{M \subset N} a_M = 2^{|N|-1}\,. \tag{3.6}$$

Proof of lemma 1. Either $a_i = 0$ for every i $\in N$, or $a_i = 1$ for at least one $i \in N$. In the former case $a_M = 0$ for $M \subset N$ and the sum in (3.3) is 0.

In the latter case we put $N^- = N - \{i\}$ and find by (3.2) that if $M \subset N^-$ then $a_{M\cup\{i\}} \equiv a_M + 1 \pmod 2$ and $a_M + a_{M\cup\{i\}} = 1$. Now (3.3) follows by (3.1).

Proof of lemma 2. If $a_i = b_i$ for $i = 1, 2, \ldots, k$ then $a_M = b_M$ and $a_M b_M = a_M$ for $M \subset S_k$. In this case (3.4) follows by (3.3) since at least one $a_M \neq 0$. Now suppose $a_i \neq b_i$ for some i. Then either $a_i = 0$, $b_i = 1$ (a) or $a_i = 1$, $b_i = 0$ (b). We see that if $M \subset N^-$ then

$$a_M b_M + a_{M\cup\{i\}} b_{M\cup\{i\}} = a_M \text{ (a)} \quad \text{or} \quad b_M \text{ (b)}.$$

By the aid of (3.1) and lemma 1 we now get (3.4) in the 2nd instance.

Proof of lemma 3. First we observe that (3.5) is valid for every $M \subset S_k$. Since $N \not\subset L$ there is an $i \in N$ which $i \notin L$. For $M \subset N^-$ we now find by (3.5)

$$a_{M\cup\{i\}} \equiv a_{M\cap L} + |M \cup \{i\} - M \cap L| \equiv a_M + 1 \pmod 2.$$

Thus $a_M + a_{M\cup\{i\}} = 1$ and (3.6) follows by (3.1).

Structure of $\mathbf{B}_k$. Let $M_1, M_2, \ldots, M_r$ $(r = 2^k - 1)$ be enumeration of the nonvoid subsets of S_k. There are $(2^k - 1)$ different combinations of values for the numbers $a_1, \ldots, a_k$ in lemma 1 if at least one $a_i = 1$. For each such combination we define a_M by (3.2) and then arrange them (excepting $a_\varnothing$) in a column in the order determined by $M_1, M_2, \ldots, M_r$. These columns make a square matrix B_k of order $2^k - 1$.

Now we define an r-dimensional rowvector D_k^N for each non-void $N \subset S_k$. D_k^N shall have „1" in the i-th position if $M_i \subset N$ and „0" if $M_i \not\subset N$. By (3.3) we find that

$$D_k^N B_k \equiv (0, \ldots, 0) \pmod{2^{|N|-1}} \tag{3.7}$$

According to lemma 2 is $B_k^* B_k$ an $r \times r$ matrix with 2^{k-1} in the main-diagonal and 2^{k-2} in all other places („*" denotes transposition). By an easy calculation we find the determinant

$$\det(B_k^* B_k) = (\det B_k)^2 = 2^{2+(k-2)2^k}. \tag{3.8}$$

Structure of $\mathbf{C}_k^L$. Suppose $L \subset S_k$ with $|L| \geqq 2$. For each $\nu = 0, 1, \ldots, (|L| - 2)$ we can find numbers a_M (0 or 1) for $M \subset L$ such that $a_\varnothing = 0$ and

$$\sum_{M\subset L} a_M = 2^\nu.$$

By the aid of (3.5) we then define a_M for $M \subset S_k$. The a_M with $M \neq \emptyset$ are arranged in a column in the order determined by $M_1, M_2, \ldots, M_r$. For each ν we get a column and these colums form the matrix C_k^L when they are put in the order of increasing ν.

We find by lemma 3 and the definition of C_k^L that

$$\begin{aligned} D_k^N C_k^L &= (2^{|N|-1}, \ldots, 2^{|N|-1}) \quad \text{if} \quad N \not\subset L \\ &= (2^0, 2^1, \ldots, 2^{|N|-2}) \quad \text{if} \quad N = L. \end{aligned} \tag{3.9}$$

Proof of Theorem 1. Let $L_1, L_2, \ldots, L_t$ $(t = 2^k - k - 1)$ be an enumeration of the subsets $L \subset S_k$ for which $|L| \geqq 2$. Form the matrix

$$A_k = B_k | C_k^{L_1} | C_k^{L_2} | \ldots | C_k^{L_t}.$$

We shall prove that A_k is a detecting matrix, i.e. that $A_k\,\xi = 0$ implies $\xi = 0$. Let ξ_0 be an r-dimensional column-vector and $\xi_{L_i}\,(i = 1, 2, \ldots, t)$ be $(|\,L_i\,| - 1)$ dimensional column-vectors with their entries from $\{-1, 0, 1\}$. Put

$$\xi = \begin{pmatrix} \xi_0 \\ \xi_{L_1} \\ \vdots \\ \xi_{L_t} \end{pmatrix}.$$

Then $A_k\xi = 0$ is equivalent to

$$B_k\,\xi_0 + \sum_{2 \leqq |L| \leqq k} C_k^L\,\xi_L = 0\,. \tag{3.10}$$

We assert that if (3.10) holds then $\xi = 0$. If $\xi_L = 0$ for $|\,L\,| \geqq 2$ then $\xi_0 = 0$. This follows since B_k is non-singular by (3.8). Now suppose $\xi_N \neq 0$ for some N, $|\,N\,| \geqq 2$, and $\xi_L = 0$ for $|\,L\,| > |\,N\,|$. Multiply (3.10) from the left by D_k^N. Then we find using (3.7) and (3.9)

$$(2^0, 2^1, \ldots, {}^{|N|-2})\,\xi_N \equiv 0 \qquad (\mathrm{mod}\ 2^{|N|-1})\,.$$

But evidently

$$-(2^{|N|-1} - 1) \leqq (2^0, 2^1, \ldots, 2^{|N|-2})\,\xi_N \leqq 2^{|N|-1} - 1$$

and so

$$(2^0, 2^1, \ldots, 2^{|N|-2})\,\xi_N = 0\,.$$

We conclude that $\xi_N = 0$. This follows from the uniqueness of the binary representation of non-negative integers. We have arrived at a contradiction which proves that $\xi_L = 0$ for $|\,L\,| \geqq 2$ and so that $\xi = 0$.

Now Theorem 1 follows if we observe that A_k is an $m \times n$ matrix, where $m = 2^k - 1$ and

$$n = 2^k - 1 + \sum_{i=2}^{k} (i-1)\binom{k}{i} = k\,2^{k-1}\,.$$

Example.

$$A_3 = \left(\begin{array}{ccccccc|cccc|c} & & & & & & & L_i\colon & \{1,2\} & \{1,3\} & \{2,3\} & \{1,2,3\} & M_j\colon \\ \hline 1 & 0 & 1 & 0 & 1 & 0 & 1 & & 1 & 1 & 1 & 1\ 1 & \{1\} \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & & 0 & 1 & 1 & 0\ 1 & \{2\} \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & & 1 & 0 & 0 & 0\ 0 & \{3\} \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & & 0 & 0 & 0 & 0\ 0 & \{1,2\} \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & & 0 & 0 & 1 & 0\ 0 & \{1,3\} \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & & 1 & 1 & 0 & 0\ 0 & \{2,3\} \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & & 1 & 1 & 1 & 0\ 0 & \{1,2,3\} \end{array}\right)$$

4.

Now we shall prove the main result in this paper

Theorem 2. $$\limsup_{n \to \infty} \frac{f(n) \log n}{n} \leqq \log 4\,.$$

When this theorem is combined with the result (1.3) we obtain the

Corollary. $$\lim_{n\to\infty} \frac{f(n)\log n}{n} = \log 4\,.$$

Proof of Theorem 2. Suppose $n \geqq 4$ and define k by $k2^{k-1} \leqq n < (k+1)2^k$. By repeated divisions we define non-negative integers $a_k, \ldots, a_1$ such that

$$\begin{aligned} n &= k\,2^{k-1}a_k + r_k\,; && 0 \leqq r_k < k\,2^{k-1} \\ &\cdots\cdots\cdots\cdots && \\ r_\nu &= (\nu-1)\,2^{\nu-2}a_{\nu-1} + r_{\nu-1}\,; && 0 \leqq r_{\nu-1} < (\nu-1)\,2^{\nu-1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots && \\ r_3 &= 4\,a_2 + a_1 && 0 \leqq a_1 < 4\,. \end{aligned} \tag{4.1}$$

Observing that $\nu 2^{\nu-1}a_\nu \leqq r_{\nu+1} < (\nu+1)2^\nu$ for $\nu \geqq 2$, we find that $a_\nu < 2\left(1+\frac{1}{\nu}\right)$ and so $a_\nu \leqq 2$ for $\nu \geqq 2$. Now we have

$$n = \sum_{\nu=2}^{k} \nu\,2^{\nu-1}a_\nu + a_1$$

By induction on (2.2) and Theorem 1 we get

$$f(n) \leqq \sum_{\nu=2}^{k} (2^\nu - 1)\,a_\nu + f(a_1) \leqq \sum_{\nu=2}^{k} 2^\nu a_\nu + a_1\,. \tag{4.2}$$

An easy calculation shows that

$$kf(n) - 2n \leqq \sum_{\nu=2}^{k} (k-\nu)\,2^\nu a_\nu + (k-2)\,a_1 < \sum_{\nu=1}^{k} (k-\nu)\,2^{\nu+1} < 2^{k+2}\,.$$

Multiply this inequality by

$$\frac{\log n}{kn} < \frac{k\log 2 + \log(k+1)}{k^2\,2^{k-1}}$$

and we obtain

$$\frac{f(n)\log n}{n} < \frac{2}{k}\left(1+\frac{4}{k}\right)\left(k\log 2 + \log(k+1)\right).$$

As n and k tend to infinity simultaneously we conclude

$$\limsup_{u\to\infty} \frac{f(n)\log n}{n} \leqq \log 4\,.$$

5.

In this section I shall give a proof of (1.3) based on information theory. We state this as a theorem

Theorem 3. $\liminf_{n\to\infty} \frac{f(n)\log n}{n} \geqq \log 4$.

We shall need some elementary results from information theory. For proofs of them the reader may consult e.g. [2].

Let X be a finite set of n elements x. Let p be a probability distribution over X with probabilities $p(x) \geqq 0$. The entropy of the probability space (X, p) is defined (let $0 \log 0 = 0$) by

$$H(X) = -\sum_{x\in X} p(x) \log p(x) .$$

It is well known that

$$0 \leqq H(X) \leqq \log n , \tag{5.1}$$

with equality on the right-hand side if and only if $p(x) = 1/n$ for every $x \in X$.

If X and Y are finite sets let $X \times Y$ denote the set of all ordered pairs (x, y) where $x \in X$ and $y \in Y$. A probability distribution over $X \times Y$ gives rise to probability distributions

$$p(x) = \sum_{y\in Y} p(x, y) \text{ and } p(y) = \sum_{x\in X} p(x, y) \text{ over } X \text{ and } Y \text{ respectively.}$$

Let $H(X)$ and $H(Y)$ be the corresponding entropies. Define a conditional probability $p(x \mid y)$ such that $p(x \mid y)\, p(y) = p(x, y)$ and the conditional entropy $H(X \mid Y)$ by

$$H(X \mid Y) = -\sum_{y\in Y} p(y) \sum_{x\in X} p(x \mid y) \log p(x \mid y) .$$

Then it is known that

$$H(X \mid Y) \leqq H(X) , \tag{5.2}$$

with equality if and only if $p(x, y) = p(x)\, p(y)$ for $x \in X$, $y \in Y$.

From the definitions given above follows

$$H(X \times Y) = H(X \mid Y) + H(Y) . \tag{5.3}$$

As a consequence of (5.2) and (5.3) we get

$$H(X \times Y) \leqq H(X) + H(Y) , \tag{5.4}$$

with equality if and only if X and Y are independent (i.e. $p(x, y) = p(x)\, p(y)$).

A stochastic variable is a vector-valued function $u(x)$ defined over a probability space X. Its range U is a probability space with the distribution

$$p(u) = \sum_{x:u(x)=u} p(x) .$$

If u, v and $u + v$ are stochastic variables and U, V, $U + V$ their ranges, and if U, V are independent, then[2]

$$H(U) \leqq H(U + V) . \tag{5.5}$$

In order to prove (5.5) we note that there is an one-one correspondence between the probability spaces $(U + V) \times V$ and $U \times V$. Thus $H((U + V) \times V) = H(U \times V)$. Subtract $H(V)$ in both members, and we get $H(U + V \mid V) = H(U \mid V) = H(U)$. Then use (5.2) once again and we get the desired result.

As an application we consider the set $X = \{(x_1, \ldots, x_n); x_i = 0 \text{ or } 1\}$. A probability distribution can be defined over X in such a manner that $x_1, \ldots, x_n$ are independent and $P(x_i = 1) = p$, $P(x_i = 0) = q$, where $p > 0$ and $q > 0$ are fixed numbers with the sum 1. Now $u_\nu(x) = x_1 + x_2 + \ldots + x_\nu$ and $v_\nu(x) = x_{\nu+1} + \ldots + x_n$ are two independent stochastic variables and $H(U_\nu)$, the entropy of the first. But now $u_\nu + v_\nu = u_n$ and so we get by (5.5)

$$H(U_\nu) \leqq H(U_n), \qquad \nu = 1, \ldots, n. \tag{5.6}$$

$U_n = \{0,1, \ldots, n\}$, the range of u_n, has the binomial probability distribution

$$\mathbf{P}(u_n = i) = \binom{n}{i} p^i q^{n-i} = p_n(i) .$$

The following assymptotic formula will be important in our proof of (1.3)

$$H(U_n) \sim \frac{1}{2} \log n . \tag{5.7}$$

But we shall prove a little more, namely

Lemma 4. $$\lim_{n\to\infty} \left[H(U_n) - \frac{1}{2} \log 2\pi enpq \right] = 0 .$$

For the proof of this lemma I need a theorem in FELLER [3] on p. 135.

Theorem. *If n and k vary in such a way that $(k - np)^3/n^2 \to 0$, then*

$$p_n(k) \sim (2\pi npq)^{-1/2} e^{-x_k^2/2} \tag{5.8}$$

asymptotically, with $x_k = (k - np)\,(npq)^{-1/2}$.

Proof of lemma 4. Choose α in the interval $0 < \alpha < \frac{1}{6}$. Then we obtain by Chebyshev's inequality

$$S_0 = \sum_{k:|x_k| \leq n^\alpha} p_n(k) < n^{-2\alpha} . \tag{5.9}$$

[2] *I* am indebted to B. AJNE for this inequality.

Put $p(x_k) = p_n(k)/S_0$ for $|x_k| > n^\alpha$ and use (5.1). Then we find that $0 < S_1 = -\sum_{k:|x_k|>n^\alpha} p_n(k) \log p_n(k) \leqq S_0 \log(n+1) - S_0 \log S_0 \to 0$ when $n \to \infty$.

Now we put

$$S_2 = -\sum_{k:|x_k|\leqq n^\alpha} p_n(k) \log\left(p_n(k)\, e^{x_k^2/2}\right),$$

For $|x_k| \leqq n^\alpha$ and $\alpha < \frac{1}{6}$ we get $(k - np)^3/n^2 \to 0$ if $n \to \infty$. Then we find by (5.8) and (5.9)

$$(1 - n^{-2\alpha}) \log \frac{(2\pi npq)^{1/2}}{1+\varepsilon} < S_2 < \log \frac{(2\pi npq)^{1/2}}{1-\varepsilon} \quad \text{for } n > n_\varepsilon .$$

Further, put

$$S_3 = \sum_{k:|x_k|\leqq n^\alpha} p_n(k) \log e^{x_k^2/2} \quad \text{and} \quad S_4 = \sum_{k:|x_k|\leqq n^\alpha} \frac{1}{2} x_k^2\, e^{-x_k^2/2} (2\pi npq)^{-1/2} .$$

Then we get by (5.8)

$$(1-\varepsilon)\, S_4 \log e < S_3 < (1+\varepsilon)\, S_4 \log e \quad \text{for} \quad n > n_\varepsilon .$$

Now $S_4 \to \frac{1}{2}$ when $n \to \infty$, and so $S_3 \to \frac{1}{2} \log e$. Thus $S_1 + S_2 + S_3 - \frac{1}{2} \log 2\pi enpq$ tends to 0 when n tends to ∞.

Proof of Theorem 3. Let A be an $m \times n$ detecting matrix. Let X be the set of n-dimensional column-vectors x with components 0 or 1. Put $p(x) = 2^{-n}$. Then the components of x become independent stochastic variables. Also the j-th component of Ax is a stochastic variable. Its entropy H_j is $\leqq H(U_n)$ according to (5.6), and if its range is denoted by V_j, $(j = 1, :\ldots, m)$, Ax has the range $U \subset V_1 \times V_2 \times \ldots \times V_m = V$. Ax is a stochastic variable with the range V if we define $p(y) = 0$ for $y \in V - U$. By (5.4) we now find that

$$H(U) = H(V) \leqq \sum_{j=1}^{m} H(V_j) \leqq m\, H(U_n) . \tag{5.10}$$

Since A is detecting there is an one-one correspondence between the probability spaces X and U, and so

$$H(U) = H(X) = n \log 2 \tag{5.11}$$

From (5.10) and (5.11) we get

$$f(n) \geqq \frac{n \log 2}{H(U_n)} . \tag{5.12}$$

Take (5.7) into account and the theorem is proved.

6. Another detection problem

The following problem was posed by P. Erdös and A. Rényi in [1].

Detection Problem. Let A be an $m \times n$ matrix with entries 0 and 1. If x is a sequence of n digits (=0 or 1) we are told the number of places (c_i)

in which x and the i-th row in A coincide, $i = 1, \ldots, m$. Suppose A has the property that the x's are uniquely determined by $c_1, \ldots, c_m$. For n given let $B(n)$ be the minimum of m for such matrices A. Then the problem is to determine the asymptotic behaviour of $B(n)$.

It has been proved by P. ERDŐS and A. RÉNYI that

$$\liminf_{n\to\infty} \frac{B(n)\log n}{n} \geqq \log 4 . \tag{6.1}$$

By the methods in this paper I can prove

Theorem 4. $$\limsup_{n\to\infty} \frac{B(n)\log n}{n} \leqq \log 4 .$$

This confirms a conjecture in [1] as to the existence of the limit.

We saw in section 2 that a matrix A is detecting if $A\,\xi = 0$ implies $\xi = 0$. Now we take this as *definition* of a detecting matrix when the entries of A are not necessarily restricted to be 0 or 1.

I now claim that the detection problem above has the following equivalent form:

Detection Problem. For n given, let $B(n)$ be the minimum of m in the class of all $m \times n$ detecting matrices B with all entries from the set $\{+1, -1\}$. Determine the asymptotic behaviour of $B(n)$.

In order to see the equivalence of the two problems let E be the m $\times$ n matrix all of whose entries are 1, and let F be the n-dimensional column-vector of merely 1's. Let x and y be column-vectors of 0's and 1's. Then the matrices A of the first problem have the property that

$$Ax + (E - A)(F - x) = Ay + (E - A)(F - y) \text{ implies } x = y . \tag{6.2}$$

The matrices B of the second problem have the property that

$$Bx = By \text{ implies } x = y . \tag{6.3}$$

Subtract $(E - A)F$ in both members of (6.2) and put $2A - E = B$. Then (6.2) and (6.3) become identical. A is a (0,1)-matrix if and only if B is a $(-1, +1)$-matrix and so we have proved the equivalence of the problems.

By the methods of section 3 we can prove the result

Theorem 5. $$B(k\,2^{k-1} + 1) \leqq 2^k, \qquad k = 2, 3, \ldots$$

I think it is not necessary to give all details of the proof, which is analogous to the proof of Theorem 1, but I shall describe those parts where the two proofs differ.

We shall keep the notations of section 3. Thus matrices denoted A_k are from now on detecting matrices with entries $+1$ and -1.

Instead of Lemmas 1—3 we need the three following lemmas, whose proofs are left to the reader. a_i, b_i, a_M, b_M are 0 or 1.

Lemma 5. *Choose numbers $a_1, a_2, \ldots, a_k$. Put $a_\varnothing = 0$ and define a_M for every non-void $M \subset S_k$ by the aid of the congruence*

$$a_M \equiv \sum_{i\in M} a_i \pmod 2. \tag{6.4}$$

Then we get for every $N \subset S_k$

$$\sum_{M \subset N} (-1)^{a_M} = 0 \text{ or } 2^{|N|}. \tag{6.5}$$

Lemma 6. *Choose numbers* $a_1, a_2, \ldots, a_k$ *and* $b_1, b_2, \ldots, b_k$. *Put* $a_\varnothing = b_\varnothing = 0$ *and define* a_M *and* b_M *as above. Then we get*

$$\begin{aligned} \sum_{M \subset S_k} (-1)^{a_M + b_M} &= 2^k \quad \text{if} \quad a_i = b_i \quad \text{for} \quad i = 1, \ldots, k \\ &= 0 \quad \text{if} \quad a_i \neq b_i \quad \text{for some } i. \end{aligned} \tag{6.6}$$

Lemma 7. *Let* L *be any subset of* S_k. *Choose a number* a_M *for every non-void* $M \subset L$. *Put* $a_\varnothing = 0$ *and define* a_M *for every* $M \not\subset L$ *by the aid of*

$$a_M \equiv a_{M \cap L} + |M - M \cap L| \pmod 2 . \tag{6.7}$$

Then we get

$$\sum_{M \subset N} (-1)^{a_M} = 0 \quad \text{if} \quad N \not\subset L . \tag{6.8}$$

Observe that the role played by ø is more important than before. The matrix A_k shall have the form

$$A_k = B_k | C_k^{L_1} | C_k^{L_2} | \ldots | C_k^{L_t}, \qquad t = 2^k - k - 1 ,$$

where B_k, $C_k^{L_1}$ etc. are certain matrices now to be defined.

Structure of $\mathbf{B}_k$. Let $M_1, M_2, \ldots, M_r$ $(r = 2^k)$ be an enumeration of all subsets of S_k. There are 2^k different combinations of values for $a_1, \ldots, a_k$. For each such combination we define a_M by (6.4) and arrange the numbers $(-1)^{a_M}$ in the order defined by $M_1, M_2, \ldots, M_r$ in a column of the matrix B_k.

Define the r-dimensional row-vector D_k^N for each $N \subset S_k$ with $|N| \geqq 2$. D_k^N shall have „1" in the i-th position if $M_i \subset N$ and „0" if $M_i \not\subset N$.

We now find by (6.5) and (6.6) respectively

$$D_k^N B_k \equiv (0, \ldots, 0) \pmod{2^{|N|}}, \tag{6.9}$$

$$(\det B_k)^2 = 2^{k 2^\kappa} . \tag{6.10}$$

Structure of $\mathbf{C}_k^L$. Suppose $L \subset S_k$ and $|L| \geqq 2$. We can find a_M for $M \subset L$ such that $a_\varnothing = 0$ and

$$\sum_{M \subset L} (-1)^{a_M} = 2^\nu , \qquad \nu = 1, 2, \ldots, (|L| - 1) . \tag{6.11}$$

By the aid of (6.7) we then define a_M for $M \not\subset L$. The numbers $(-1)^{a_M}$ are arranged in a column in the order determined by $M_1, M_2, \ldots, M_r$. For each ν we get such a column and the $|L| - 1$ columns form the matrix C_k^L when they are put in the order of increasing ν.

By Lemma 7 and (6.11) we find that

$$\begin{aligned} D_k^N C_k^L &= (0, \ldots\ldots\ldots, 0) \quad \text{if} \quad N \not\subset L \\ &= (2^1, 2^2, \ldots, 2^{|N|-1}) \quad \text{if} \quad N = L . \end{aligned} \tag{6.12}$$

Proof of Theorem 5. Take an enumeration of the sets $L \subset S_k$ with $|L| \geqq 2$. Form the matrix A_k. The previous proof that A_k is detecting holds with only small changes. A_k is an $m \times n$ matrix, with $m = 2^k$ and $n = k 2^{k-1} + 1$.

Proof of Theorem 4. First I prove that

$$B(n_1 + n_2) \leqq B(n_1) + B(n_2), \qquad n_1, n_2 = 1, 2, \ldots \tag{6.13}$$

Let B_i $(i = 1, 2)$ be $m_i \times n_i$ detecting matrices. We may assume that the first row in B_i contains merely $1's$, for in other case we can multiply by -1 in a column without altering the property of being a detecting matrix. Introduce E_1 as the $m_2 \times n_1$ matrix of merely $1's$ and E_2 as the $m_1 \times n_2$ matrix of $1's$, and let F_i $(i = 1, 2)$ be the n_i-dimensional row-vector of $1's$.

We shall prove that the matrix

$$B = \begin{pmatrix} B_1 & E_2 \\ E_1 & B_2 \\ F_1 & -F_2 \end{pmatrix}$$

is a detecting matrix. Let ξ_i $(i = 1, 2)$ be n_i-dimensional column-vectors and suppose that

$$B \begin{pmatrix} \xi_1 \\ \xi_2 \end{pmatrix} = 0 .$$

Then we get the equations

$$\begin{aligned} B_1 \xi_1 + E_2 \xi_2 &= 0 \\ E_1 \xi_1 + B_2 \xi_2 &= 0 \\ F_1 \xi_1 - F_2 \xi_2 &= 0 \\ F_1 \xi_1 + F_2 \xi_2 &= 0. \end{aligned} \tag{6.14}$$

The last one follows since the first row in B contains merely $1's$. By (6.14) we now find that $B_1 \xi_1 = 0$ and $B_2 \xi_2 = 0$. But B_1 and B_2 are detecting, and so $\xi_1 = 0$ and $\xi_2 = 0$, if ξ_1 and ξ_2 have all components equal to -1, 0 or $+1$. Thus we have proved that B is detecting.

Now we note that the $(m_1 + 1)$-st row in B is identical with the 1-st. When it is removed we get an $(m_1 + m_2) \times (n_1 + n_2)$ detecting matrix.

If we take $m_i = B(n_i)$ for $i = 1, 2$ (6.13) follows.

From Theorem 5 we find $B(k2^{k-1}) \leqq 2^k$, since $B(n)$ is non-decreasing. Now we can take over the proof of Theorem 2 with 2^ν instead of $2^\nu - 1$ in (4.2).

(Received December 28, 1963)

REFERENCES

[1] Erdős, P.—Rényi, A.: "On two problems of information theory", *This journal*, **8** (1963) p. 241.

[2] Feinstein, A.: *Foundations of information theory*, New York 1958.

[3] Feller, W.: *An introduction to probability theory and its applications*, *Vol* 1, New York 1950.

[4] Shapiro, H. S.—Söderberg, S.: "A combinatory detection problem", *American Math. Monthly*, **70** (1963) pp. 1066–1070.

ОБ ОДНОЙ КОМБИНАТОРНОЙ ПРОБЛЕМЕ ДЕТЕКТИРОВАНИЯ

B. LINDSTRÖM

Резюме

Автор решает две комбинаторные проблемы, изучаемые P. Erdős и A. Rényi [1]. Проблемы в терминах теории матриц формулируются следующим образом. Пусть (C) — класс матриц с элементами, равными 0 и 1 (случай (1)) или -1 и $+1$ (случай (2)). Матрицы, для которых из равенства $A\xi = 0$ следует, что $\xi = 0$, если ξ — вектор с компонентами -1, 0 и 1, называются *детектированными матрицами*.

Пусть $f(n)$ — минимальное число строк детектированных матриц с n столбцами. Проблема заключается в определении асимптотического поведения функции $f(n)$ при $n \to \infty$.

P. Erdős и A. Rényi доказали для обоих классов (C), что

$$\liminf_{n\to\infty} \frac{f(n)\log n}{n} \geqq \log 4 .$$

Посредством конструирования детектированных матриц автор доказывает следующие соотношения:

$$f(k\cdot 2^{k-1}) \leqq 2^k - 1 \qquad k = 2, 3, \ldots \text{ (в случае (1))}$$

$$f(k\cdot 2^{k-1} + 1) \leqq 2^k \qquad k = 2, 3, \ldots \text{ (в случае (2))}$$

и из них, используя соотношение $f(n_1 + n_2 + \ldots + n_i) \leqq f(n_1) + f(n_2) + \ldots + f(n_i)$, выводит, что $\limsup_{n\to\infty} \frac{f(n)\log n}{n} \leqq \log 4$ (в обоих случаях).

Этим доказана гипотеза P. Erdős и A. Rényi о существовании предела.