Reprinted from JOURNAL OF COMBINATORIAL THEORY Vol. 1, No. 2, September 1966

Printed in Italy

On Separating Systems of a Finite Set

G. KATONA

Mathematical Institute of the Hungarian Academy of Sciences,

Budapest, Hungary

Communicated by Alfred Rényi

ABSTRACT

Let H be a finite set, and $A_1, A_2, \ldots, A_m$ subsets of H. We call a system $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ separating system, if for any two distinct elements x and y of H there exists an A_i $(1 \leq i \leq m)$ such that either

$$x \in A_i \qquad \text{and} \qquad y \notin A_i$$

or

$$x \notin A_i \qquad \text{and} \qquad y \in A_i .$$

This paper deals with the problem of finding the minimum of m, if additionally $|A_i| \leq k$ $(1 \leq i \leq m)$, where $1 \leq k \leq n$, and $|A_i|$ is the cardinal number of A_i. We reduce this combinatorial problem to an analytical one, and give a lower and an upper estimation:

$$\frac{\log n}{\log en/k} \frac{n}{k} \leq \min m \leq \left\{ \frac{\log 2n}{\log n/k} \right\} \frac{n}{k} .$$

1. INTRODUCTION

We call a system $\mathscr{A}$ of subsets of a set H a separating system, if the system separates any two elements of the set H, that is, to any two elements of the set H there exists an element of the system $\mathscr{A}$ containing exactly one of them. It is easy to see [1] that the minimal separating system of a set of n elements has exactly $\{\log_2 n\}$ elements (where $\{x\}$ denotes the least integer $\geq x$). Rényi raised the problem of finding minimal separating systems, if in addition it is required that each subset

in the separating system should consist of exactly k elements. The present paper investigates this question. We reduce this combinatorial problem to an analytical one, and give a lower and an upper estimation. The lower estimation will be given by simple information-theoretic considerations.

2. Origin of the problem

Seeking an unknown element of a set H_n of n elements, we can proceed in the following way: let us perform experiments to decide whether the unknown element in question is in a particular subset or not for each subset of a system $\mathscr{A}$ of subsets of H_n. It is easy to see that this procedure is always effective only for a separating system $\mathscr{A}$. The concept of a separating system was introduced by Rényi in his papers concerning certain information-theoretic problems [1–5].

In practice we often have an additional condition, that the cardinal numbers of the subsets are less than or equal to a number k. As we will see, seeking for the minimal system one can replace this condition with the exact equality.

3. Reduction of the problem

Let H_n be a set having the elements

$$x_1, x_2, \ldots, x_n \ (n > 1),$$

and $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ a system of subsets of H_n. We call this system a separating system if for any x_j and x_l $(j \neq l)$ there exists an A_i $(1 \leq i \leq m)$, such that

$$x_j \in A_i \quad \text{and} \quad x_l \notin A_i$$

or

$$x_j \notin A_i \quad \text{and} \quad x_l \in A_i .$$

Let S denote the set of all separating systems, that is,

$$\mathscr{A} = \{A_1, A_2, \ldots, A_m\} \in S$$

if and only if $\mathscr{A}$ is a separating system of subsets of H_n. Let k be a positive

integer, and let S_k denote the set of systems $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ for which $\mathscr{A} \in S$, and $|A_i| = k$ $(1 \leq i \leq m)$, where $|A_i|$ denotes the cardinal number of the subset A_i. We want to determine the minimal value of m for which there exists a system $\mathscr{A} = \{A_1, A_2, \ldots, A_m\} \in S_k$.

Obviously, it is sufficient to examine the case $k \leq n/2$; otherwise $\{\bar{A}_1, \bar{A}_2, \ldots, \bar{A}_m\} \in S_{n-k}$ (where $\bar{A}$ is the set complementary to A in H_n) and $n - k \leq n/2$.

To any set $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ of subsets of the set H_n let us define a corresponding m by n matrix M_{mn} of the elements ε_{ij}, where $\varepsilon_{ij} = 1$ if $x_j \in A_i$ and $\varepsilon_{ij} = 0$ otherwise $(1 \leq i \leq m;\ 1 \leq j \leq n)$. If $\{A_1, A_2, \ldots, A_m\} \in S$, then, because of the definition of S, for any two columns there exists a row in which the two columns differ, that is, there are no two identical columns in M_{mn}. Conversely, if all columns are different, then to any two columns there exists a row in which they differ; thus the corresponding system of sets is separating. Similarly, the condition $|A_i| = k$ in the term of matrices is the following. In each row of M_{mn} stand exactly k ones, and the others are zeros.

Thus we have to determine the smallest integer m for which there exists a matrix M_{mn}: (*a*) with elements 0, 1; (*b*) in each row containing k ones; and (*c*) no two columns are identical. Denote this integer by $U = U(n, k)$.

For the matrices having the above-mentioned three properties the following interesting theorem is valid:

THEOREM 1. *Let m, n, $1 \leq k \leq n/2$, $s_0, s_1, \ldots, s_m$ be fixed non-negative integers. We can find a matrix M_{mn} of m rows and n columns having the properties (a), (b), and (c) and in which the number of the columns containing i ones is s_i if and only if*

$$mk = \sum_{i=0}^{m} i\, s_i, \tag{1}$$

$$n = \sum_{i=0}^{m} s_i, \tag{2}$$

$$s_i \leq \binom{m}{i} \quad (i = 0, 1, \ldots, m). \tag{3}$$

COROLLARY. *The number $U = U(n, k)$ is equal to the least number m for which there exists a system of non-negative integers $m, s_0, s_1, \ldots, s_m$ satisfying conditions* (1), (2) *and* (3).

The necessity of the conditions is trivial. We may obtain (1) by counting the number of ones in M_{mn} in two different ways; (2) means that the number of columns is n. Finally there can be at most $\binom{m}{i}$ different columns containing i ones; thus (3) is also necessary. The point of the theorem lies just in the sufficiency of these three evidently necessary conditions.

The proof consists of four steps.

First we introduce some notations and definitions. If $Q_1, Q_2, \ldots, Q_q$ are matrices with the same number of rows, $[Q_1, Q_2, \ldots, Q_q]$ denotes the matrix obtained by writing side by side (in the given order) the matrices $Q_1, Q_2, \ldots, Q_q$. $M[i]$ denotes the matrix consisting of the first i columns of M.

We shall call a zero-one matrix *admissible* if each row contains the same number of ones, and *quasi-admissible* if the numbers of ones in the rows differ at most by one. Finally, we say that a matrix M is *perfect*, if it is admissible and the matrices $M[i]$ are quasi-admissible for each i.

REMARK 1.1. Obviously, if we write side by side two admissible matrices, the new matrix is also admissible.

REMARK 1.2. Similarly, writing side by side an admissible and a perfect matrix, the new matrix has the property that the matrix consisting of its first i columns is quasi-admissible if i is greater or equal to the number of columns of the first matrix.

REMARK 1.3. Finally, writing side by side perfect matrices, the new matrix will be perfect, too.

REMARK 1.4. By interchanging the rows of a matrix, the properties "admissible", "quasi-admissible", and "perfect" remain valid. However by interchanging the columns of a matrix only the properties "admissible" and "quasi-admissible" remain valid, and the property of perfectness may be destroyed.

STEP A. Considering a fixed column C of elements 0, 1, and writing all its distinct cyclic permutations side by side, the matrix M_C obtained in this way is admissible.

PROOF. Let us put the last row of M_C before the first. The obtained matrix M_C' differs from M_C only in the order of the columns; the columns of M_C' are, namely, cyclic permutations of C; moreover the number of columns is the same and the columns of M_C are evidently different.

Thus the number of ones in the i-th row of M_C and the i-th row of M_C' are equal; as, however, the i-th row of M_C' is identical with the $(i-1)$-st row of M_C for $i = 2, 3, \ldots, m$, M_C is admissible.

STEP B. If D is a column of length m which has 1 in its first t places, and 0 elsewhere, there exists a perfect matrix M^* consisting of all cyclic permutation of D.

PROOF. We construct the desired matrix. Let $D(j)$ denote the cyclic shift of D by j downward. Thus $D(0) = D$. Determine M^0 as the matrix consisting of the columns

$$D(0), D(t), D(2t), \ldots, D\left(\left(\frac{[m,t]}{t} - 1\right)t\right)$$

($[m, t]$ denotes the least common multiple of m and t). We may characterize each column by $r(D(j))$, the position of the 0 preceding a 1. Such a 0 always exists unless the column is identical with D. In the latter case we put $r(D(0)) = 0$. Obviously $r(D(j))$ is the remainder of the division of j by m:

$$j = qm + r(D(j)) \qquad 0 \leq r(D(j)) < m. \tag{4}$$

It is easy to see, by induction, that the number of ones in each of the first r rows in the matrix $M^0[i]$ is greater by one than that in any of the other rows, where

$$r \equiv r(D(it)) + t \pmod{m} \quad \text{and} \quad 0 \leq r < m.$$

Thus the matrix M^0 is perfect, because M^0 is admissible, since for the case $i = [m, t]/t - 1$:

$$it = \left(\frac{[m,t]}{t} - 1\right)t = \left(\frac{[m,t]}{m} - 1\right)m + (m - t),$$

and, further, $r = 0$ follows from $r(D(it)) = m - t$.

If $(m, t) = 1$ where (m, t) denotes the greatest common divisor of m and t) then $[m, t]/t = m$ and the construction is completed. If however, $(m, t) = d > 1$ we construct the matrices $M^1, M^2, \ldots, M^{d-1}$ in the following way: M^i $(1 \leq i \leq d-1)$ consists of the columns

$$D(i), D(t+i), D(2t+i), \ldots, D\left(\left(\frac{[m,t]}{t} - 1\right)t + i\right).$$

We may say that M^i results from M^0 by an i-fold cyclic shift of the rows. Thus, by Remark 1.4, M^i is also perfect ($1 \leq i \leq d-1$). If $M^* = [M, M^1, \ldots, M^{d-1}]$, then by Remark 1.3 M^* is perfect, indeed.

It remains only to prove that the columns of M^* are all different. This follows from the remark that if a runs over the numbers $0, 1, \ldots, [m, t]/t - 1$ and b over the numbers $0, 1, \ldots, (m, t) - 1$, the numbers $at + b$ are all different mod m and thus represent each residue class mod m exactly once, in view of $[m, t]\,(m, t) = m\,t$.

STEP C. Let s_t be an integer satisfying $s_t \leq \binom{m}{t}$; then there exists a quasi-admissible matrix N_t of m rows and s_t columns containing in each column exactly t ones.

PROOF. Let us consider all cyclically distinct columns of length m containing exactly t ones and form to each column the matrix M_C described in Step A, except for the column in which the first t elements are ones, to which we form the matrix M^* described in Step B. Denote this set of matrices by $\mathfrak{M}$. Obviously each element M of $\mathfrak{M}$ is admissible and $M^* \in \mathfrak{M}$ is perfect. In addition, denoting by $l(M)$ the number of columns of M

$$\sum_{M \in \mathfrak{M}} l(M) = \binom{m}{t} \tag{5}$$

holds, because in the matrices each column containing t ones occurs exactly once. Finally

$$l(M) \leq m \qquad M \in \mathfrak{M} \tag{6}$$

and

$$l(M^*) = m. \tag{7}$$

Number the elements of $\mathfrak{M}$ in some manner, the only condition being, that M^* must be the last: $M_1, M_2, \ldots$. If $s_t \leq \binom{m}{t}$, then because of (5), there exists an index i such that

$$\sum_{j=1}^{i} l(M_j) \leq s_t < \sum_{j=1}^{i+1} l(M_j)$$

holds, Obviously by (6) and (7)

$$s_t - \sum_{j=1}^{i} l(M_j) > l(M^*).$$

We obtained the desired matrix N_t in the form

$$N_t = \left[M_1, M_2, \ldots, M_i, M^* \left[s_t - \sum_{j=1}^{i} l(M_j)\right]\right].$$

Indeed, N_t has s_t columns, and by Remarks 1.1 and 1.2 is quasi-admissible.

STEP D. On the basis of Steps A, B, and C we construct the matrix M_{mn} occurring in Theorem 1 as follows:

It is easy to see that, if Q_1 and Q_2 are quasi-admissible matrices, the rows of Q_2 can be interchanged so that for the new Q_2' the matrix $[Q_1, Q_2']$ is quasi-admissible.

Thus, we construct for each t the matrices N_t and interchange the rows of N_1 so that, for the N_1' obtained the matrix $[N_0, N_1']$ should be admissible. If we have already constructed N_t', we determine N_{t+1}' by the condition of admissibility of $[N_0, N_1', \ldots, N_t', N_{t+1}']$. Finally, in this way we obtain the desired matrix

$$M_{mn} = [N_0, N_1', N_2', \ldots, N_m'].$$

We have still to see that M_{mn} satisfies the conditions of Theorem 1. It follows from the construction that the columns of M_{mn} are different, and the number of columns containing t ones is s_t. It remains only to show that each row contains exactly k ones. We know that the number of the ones in M_{mn} is equal to $\sum_{i=0}^{m} is_i$. Applying (1), the number of the ones in M_{mn} is divisible by m. But this is possible only if M_{mn} is admissible. Thus, because of (1) each row contains exactly k ones, which completes our proof.

Now we deal with a question mentioned in § 2. Denote by S_k' the set of systems satisfying the conditions

$$\{A_1, A_2, \ldots, A_m\} \in S \quad \text{and} \quad |A_i| \leq k \quad i = 1, 2, \ldots, m.$$

The problem is to find the minimal value of m for which there exists a system

$$\{A_1, A_2, \ldots, A_m\} \in S_k'.$$

The following theorem shows how this question is related to that discussed above.

THEOREM 2. *If* $k < n/2$, *and the system* $\{A_1', A_2', \ldots, A_m'\} \in S_k'$ *then there esists a system* $\{A_1, A_2, \ldots, A_m\} \in S_k$.

COROLLARY. *The minimum of the numbers of the elements of a system in* S_k' *is* $U(n, k)$. (*Obviously* $S_k \subset S_k'$).

REMARK 2.1. For $k \geq n/2$ the condition $|A_i| \leq k$ is not essential, because either $|A_i| \leq k$ or $|\bar{A}_i| \leq k$ always holds. Thus for any system $\{A_1, A_2, \ldots, A_m\} \in S$ there exists a system $\{B_1, B_2, \ldots, B_m\} \in S_k'$ where

$$B_i = A_i \quad \text{or} \quad B_i = \bar{A}_i.$$

PROOF. Let us consider the matrix M_{mn}' of elements ε_{ij} where $\varepsilon_{ij} = 1$ if $x_j \in A_i'$ and $\varepsilon_{ij} = 0$ otherwise. If s_t' denotes the number of columns containing exactly t ones, obviously

$$mk \geq \sum_{i=0}^{m} i s_i', \tag{8}$$

$$n = \sum_{i=0}^{m} s_i', \tag{9}$$

$$s_i' \leq \binom{m}{i}, \tag{10}$$

hold similarly to (1), (2), and (3).

Let $m, s_0, s_1, \ldots, s_m$ be a system of non-negative integers satisfying (8), (9), and (10), and in addition $\sum_{i=0}^{m} i s_i$ is maximal if m is fixed. If $mk > \sum_{i=0}^{m} i s_i$ and for any $l \geq 1$ the inequalities $s_l < \binom{m}{l}$ and $s_{l-1} > 0$ hold, then the integers $m, s_0, s_1, \ldots, s_{l-1} - 1, s_l + 1, \ldots, s_m$ satisfy the conditions (8), (9), and (10) and

$$\sum_{i=0}^{m} i s_i < \sum_{\substack{i=0 \\ i \neq l-1,\, l}}^{m} i s_i + (l-1)(s_{l-1} - 1) + l(s_l + 1),$$

which contradicts our supposition that, for $m, s_0, s_1, \ldots, s_m$, the expression $\sum_{i=0}^{m} i s_i$ is maximal. Thus, either

$$mk = \sum_{i=0}^{m} i s_i \tag{11}$$

or for some j

$$s_i = 0 \quad i = 0, 1, \ldots, j-1 \quad \text{and} \quad s_i = \binom{m}{i} \quad i = j, j+1, \ldots, m. \tag{12}$$

However, from (12) follows

$$n = \sum_{i=j}^{m} \binom{m}{i}$$

and

$$mk \geq \sum_{i=j}^{m} i \binom{m}{i}.$$

Hence

$$k \geq \sum_{i=j}^{m} \frac{i}{m} \binom{m}{i} = \sum_{i=j-1}^{m-1} \binom{m-1}{i} \geq \frac{\sum_{i=j}^{m} \binom{m}{i}}{2} = \frac{n}{2},$$

which contradicts the supposition $k < n/2$.

Therefore (11) holds for $m, s_0, s_1, \ldots, s_m$, and applying Theorem 1 we can construct a matrix M_{mn}, that is, a system $\{A_1, A_2, \ldots, A_m\} \in S_k$. This completes our proof.

Using (1), (2), (3) or (8), (9), (10) to determine $U(n, k)$ the assumption of $m, s_0, s_1, \ldots, s_m$ being integer will cause difficulties. Thus we will try to eliminate this requirement.

LEMMA 1. *There exists a minimum of numbers m for which a system of non-negative numbers $m, s_0, s_1, \ldots, s_{\{m\}}$ satisfies the conditions*

$$mk \geq \sum_{i=0}^{\{m\}} s_i, \tag{13}$$

$$n = \sum_{i=0}^{\{m\}} s_i, \tag{14}$$

$$0 \leq s_i \leq \binom{m}{i} = \frac{m(m-1)\cdots(m-i+1)}{i!} \quad (0 \leq i \leq \{m\}). \tag{15}$$

PROOF. Obviously there exists an infimum of numbers m. Denote it by U'. Let $m^j (j = 1, 2, \ldots)$ be a sequence converging to U', and $U' < m^j < [U'] + 1 (j = 1, 2, \ldots)$. The systems $m^j, s_0^j, s_1^j, \ldots, s^j_{[U']+1}$ satisfy conditions (13), (14), and (15) for all $j \geq 1$. For fixed i the sequence $s_i^j (j = 1, 2, \ldots)$ is bounded because of

$$0 \leq s_i^j \leq \binom{m^j}{i} \leq \binom{[U'] + 1}{i}.$$

Therefore there exists a convergent subsequence of the numbers s_i^j which converges to some s_i. Performing this choice for all the i, we get a subsequence of the sequence of the vectors $m^j, s_0^j, \ldots, s^j_{[U']+1}$ which converges to $U', s_0, s_1, \ldots, s_{[U']+1}$. Since for each j (13), (14), and (15) hold, $U', s_0, s_1, \ldots, s_{[U']+1}$ also satisfies these conditions. If U' is not an integer, we have finished the proof; if it is one, then we have still to show $s_{[U']+1} = 0$. But this is a trivial consequence of

$$0 \leq s^j_{[U']+1} \leq \binom{m^j}{[U'] + 1},$$

because the right side converges to zero if $m^j \to U'$. This completes our proof.

LEMMA 2.

$$\{U'\} = U.$$

PROOF. Let $U', s_0, s_1, \ldots, s_{\{U'\}}$ be a system of non-negative real numbers satisfying (13), (14), and (15). We have to construct a system of non-negative integers $\{U'\}, s_0', \ldots, s'_{\{U'\}}$, which satisfies (8), (9), and (10).

Let us choose the integer r according to

$$\sum_{i=0}^{r} \{s_i\} + \sum_{i=r+1}^{\{U'\}} [s_i] = n. \tag{16}$$

Such an r exists because

$$\left(\sum_{i=0}^{j+1} \{s_i\} + \sum_{i=j+2}^{\{U'\}} [s_i] \right) - \left(\sum_{i=0}^{j} \{s_i\} + \sum_{i=j+1}^{\{U'\}} [s_i] \right) = 0 \text{ or } 1,$$

and

$$\sum_{i=0}^{\{U'\}} [s_i] \leq n \leq \sum_{i=0}^{\{U'\}} \{s_i\}.$$

Determine the s_i' in the following manner:

$$s_i' = \begin{cases} \{s_i\} & i = 0, 1, \ldots, r, \\ [s_i] & i = r+1, \ldots, \{U'\}. \end{cases}$$

Then because of (16) condition (9) holds.

Obviously, by (16) and (14)

$$\sum_{i=0}^{\{U'\}} is_i = \sum_{i=0}^{r} i\{s_i\} + \sum_{i=r+1}^{\{U'\}} i[s_i] + \sum_{i=0}^{r} i(s_i - \{s_i\}) + \sum_{i=r+1}^{\{U'\}} i(s_i - [s_i])$$

$$\geq \sum_{i=0}^{r} i\{s_i\} + \sum_{i=r+1}^{\{U'\}} i[s_i] + r\sum_{i=0}^{r} (s_i - \{s_i\}) + r\sum_{i=r+1}^{\{U'\}} (s_i - [s_i])$$

$$= \sum_{i=0}^{r} i\{s_i\} + \sum_{i=r+1}^{\{U'\}} i\,[s_i] + r\left(\sum_{i=0}^{\{U'\}} s_i - \sum_{i=0}^{r} \{s_i\} - \sum_{i=r+1}^{\{U'\}} [s_i]\right)$$

$$= \sum_{i=0}^{r} i\{s_i\} + \sum_{i=r+1}^{\{U'\}} i[s_i]\,; \tag{17}$$

further because of (13) and (17)

$$\{U'\}k \geq U'k \geq \sum_{i=0}^{\{U'\}} is_i \geq \sum_{i=0}^{r} i\{s_i\} + \sum_{i=r+1}^{\{U'\}} i[s_i] = \sum_{i=0}^{\{U'\}} is_i',$$

that is, (8) hold also. Finally we deduce (10) from (15):

$$s_i' \leq \{s_i'\} \leq \left\{\binom{U'}{i}\right\} \leq \binom{\{U'\}}{i} \quad (0 \leq i \leq \{U'\}).$$

Thus we have proved the inequality

$$\{U'\} \geq U, \tag{18}$$

but (8), (9), (10) is a special case of (13), (14), (15); thus

$$U' \leq U, \tag{19}$$

and

$$\{U'\} = U$$

from (18) and (19).

LEMMA 3. *If* $U', s_0, s_1, \ldots, s_{\{U'\}}$ *is a system of non-negative numbers satisfying* (13), (14), *and* (15), *and* U' *is minimal, then equality must hold in* (13).

PROOF. Instead of the above statement we will prove that if $m, s_0, s_1, \ldots, s_{\{m\}}$ is a system of non-negative numbers satisfying (13), (14), and (15), with strict inequality in (13), then m can be decreased, that is, $m \neq U'$.

Put

$$\varepsilon_1 = mk - \sum_{i=0}^{\{m\}} is_i > 0. \tag{20}$$

For some r

$$s_r < \binom{m}{r};$$

otherwise

$$k > \sum_{i=0}^{\{m\}} \frac{i}{m}\binom{m}{i} = \sum_{i=0}^{\{m\}-1} \binom{m-1}{i} \geq \frac{1}{2}\sum_{i=0}^{\{m\}} \binom{m}{i} \geq \frac{n}{2}$$

contradicts the supposition $k \leq n/2$.

Denote by ε_2 the difference $\binom{m}{r} - S_r$:

$$\varepsilon_2 = \binom{m}{r} - s_r. \tag{21}$$

Determine first the number δ_r in the following way

$$\delta_r = \min\left(\frac{\varepsilon_2}{2}, \frac{\varepsilon_1}{2r}, \sum_{\substack{i=0 \\ i\neq r}}^{\{m\}} s_i\right), \tag{22}$$

then $\delta_i\ (i = 0, 1, \ldots, r-1, r+1, \ldots, \{m\})$ is determined by

$$0 < \delta_i \leq s_i \qquad \text{if} \quad s_i \neq 0$$

$$i = 0, \ldots, r-1, r+1, \ldots, \{m\}. \tag{23}$$

$$\delta_i = 0 \qquad \text{if} \quad s_i = 0$$

$$\sum_{\substack{i=0 \\ i\neq r}}^{\{m\}} \delta_i = \delta_r \tag{24}$$

Further, let $\varrho_i\ (i = 0, 1, \ldots r-1, r+1, \ldots \{m\}$ be a positive number, such that

$$s_i - \delta_i \leq \binom{m-\varrho_i}{i}. \tag{25}$$

Obviously, by (23)

$$s_i - \delta_i < \binom{m}{i}$$

always holds; thus by continuity there exists such a ϱ_i. Similarly we

determine $\varrho_r > 0$ by the inequality

$$s_r + \delta_r \leq \binom{m - \varrho_r}{r} \tag{25'}$$

Such a ϱ_r also exists, because by (22)

$$\delta_r \leq \frac{\binom{m}{r} - s_r}{2}.$$

Finally put

$$\delta^* = \min\left(\frac{\varepsilon_1}{2k}, \varrho_i\,(i = 0, 1, \ldots, \{m\})\right) > 0\,. \tag{26}$$

The new system

$$m - \delta^*,\ s_0 - \delta_0,\ s_1 - \delta_1, \ldots, s_{r-1} - \delta_{r-1},\ s_r + \delta_r, s_{r+1} - \delta_{r+1}, \ldots, s_{\{m\}} - \delta_{\{m\}}$$

also satisfies (13), (14), and (15). Indeed by (26), (20), and (22)

$$(m - \delta^*)\,k \geq \left(m - \frac{\varepsilon_1}{2k}\right)k = mk - \frac{\varepsilon_1}{2} = \sum_{i=0}^{\{m\}} i s_i + \frac{\varepsilon_1}{2} \geq$$

$$\sum_{\substack{i=0\\ i\neq r}}^{\{m\}} i s_i + r(s_r + \delta_r) - r\frac{\varepsilon_1}{2r} + \frac{\varepsilon_1}{2} \geq \sum_{\substack{i=0\\ i\neq r}}^{\{m\}} i(s_i - \delta_i) + r(s_r + \delta_r),$$

that is, (13) holds. (14) is a trivial consequence of (24); finally, (15) results from (26), (25), and (25'). Thus the proof is finished.

LEMMA 4. *If* $U', s_0, \ldots, s_{\{U'\}}$ *is a system of non-negative numbers satisfying* (13), (14), *and* (15), *and* U' *is minimal, then for some* $r > 0$

$$\begin{aligned} s_i &= \binom{U'}{i} && i = 0, 1, \ldots, r-1, \\ s_i &= 0 && i = r+1, \ldots, \{U'\}. \end{aligned} \tag{27}$$

PROOF. Instead of the above statement we will prove the following one: If $m, s_0, s_1, \ldots, s_{\{m\}}$ is a system of non-negative numbers satisfying (13), (14), and (15), for which (27) does not hold, then it is possible to construct a system $m, s_0', s_1', \ldots, s_{\{m\}}'$ satisfying (13), (14), and (15) with strict inequality in (13). Thus by Lemma 3 m is not minimal.

If (27) does not hold, then for some j

$$s_j < \binom{m}{j}$$

and

$$s_{j+1} > 0$$

Put

$$\varepsilon = \min\left(\binom{m}{j} - s_j,\ s_{j+1}\right),$$

and

$$\begin{aligned} s_i' &= s_i \qquad i = 0, 1, \ldots, j-1,\ j+2, \ldots, \{m\} \\ s_j' &= s_j + \varepsilon \\ s_{j+1}' &= s_{j+1} - \varepsilon. \end{aligned}$$

Thus (14) and (15) obviously hold; further

$$mk \geq \sum_{i=0}^{\{m\}} i s_i = \sum_{\substack{i=0 \\ i \neq j+1, j}}^{\{m\}} i s_i + j(s_j + \varepsilon) + (j+1)(s_{j+1} - \varepsilon) + \varepsilon > \sum_{i=0}^{\{m\}} i s_i',$$

that is, (13) holds also, with strict inequality, and the proof of Lemma 4 is completed.

On the basis of Lemmas 1, 3, and 4 it follows that for some r

$$U'k = \sum_{i=0}^{r-1} i\binom{U'}{i} + r s_r,$$

$$n = \sum_{i=0}^{r-1} \binom{U'}{i} + s_r,$$

and

$$0 \leq s_r < \binom{U'}{r+1}.$$

In other words, eliminating s_r

$$U'k = \sum_{i=0}^{r-1} i\binom{U'}{i} + r\left[n - \sum_{i=0}^{r-1} \binom{U'}{i}\right] \tag{28}$$

and

$$\sum_{i=0}^{r-1} \binom{U'}{i} \leq n < \sum_{i=0}^{r} \binom{U'}{i}. \tag{29}$$

For a fixed r, (28) is an equation in U'. (29) means an additional limitation for the solution of the equation.

LEMMA 5. (a) *For any r,* (28) *has only non-negative solution.* (b) *There exists one and only one r for which the above solution of* (28) *satisfies* (29).

PROOF. (a) The statement follows from the fact that the left side of (28) has the value 0 for $U' = 0$ and is monotonically decreasing.

(b) By Lemma 1 there exists the minimal U', and it must satisfy (28) and (29); thus we have at least one such r. Assume that for r the solution of (28) satisfies (29). We will show, then for $q < r$ that this is not possible. Indeed, in the case of q we may write (28) in the following form:

$$xk = \sum_{i=0}^{q-1} i \binom{x}{i} + q\left[n - \sum_{i=0}^{q-1} \binom{x}{i}\right] = \sum_{i=0}^{r-1} i \binom{x}{i} + r\left[n - \sum_{i=0}^{r-1} \binom{x}{i}\right]$$
$$- \left[(r-q)\, n - (r-q) \sum_{i=0}^{q-1} \binom{x}{i} - \sum_{i=q}^{r-1} (r-i) \binom{x}{i}\right]. \tag{30}$$

For U' in (28) equality holds. The left side of equation (30) for U' has the same value as in (28). However, as we will show, the right side has a less or equal value; thus the root of (30) is less than or equal to U'.

We have to prove that

$$(r-q)\, n - (r-q) \sum_{i=0}^{q-1} \binom{U'}{i} - \sum_{i=q}^{r-1} (r-i) \binom{U'}{i} \geq 0 .$$

Diminishing the last term we obtain

$$(r-q)\left[n - \sum_{i=0}^{r-1} \binom{U'}{i}\right] \geq 0 .$$

But this follows from (29). Thus the root of (30) is $\leq U'$, but the condition

$$\sum_{i=0}^{q-1} \binom{x}{i} \leq n < \sum_{i=0}^{q} \binom{x}{i} \tag{31}$$

means that x must be in an interval lying disjointly in the right of the interval determined by (29). This is a contradiction, which finishes the proof.

THEOREM 3. *If U is the minimal integer for which there exists a system* $\{A_1, A_2, \ldots, A_U\} \in S_K$ *and* U' *is a root of the equation*

$$xk = \sum_{i=0}^{r-1} i \binom{x}{i} + r\left[n - \sum_{i=0}^{r-1} \binom{x}{i}\right], \tag{32}$$

for some r, and satisfies the condition

$$\sum_{i=0}^{r-1} \binom{U'}{i} \leq n < \sum_{i=0}^{r} \binom{U'}{i} \tag{33}$$

then

$$U = \{U'\}.$$

This theorem is a trivial consequence of our lemmas.

THEOREM 4. *If* $k \geq 1$,

$$n \geq \frac{k(k+1)}{2} + 1$$

then

$$U = \left\{2\frac{n-1}{k+1}\right\}.$$

PROOF. We will use Theorem 3. If $r = 2$, we can write (32) in the form

$$xk = x[n - 1 - x].$$

Hence

$$U' = 2\frac{n-1}{k+1}.$$

The left side inequality of (33) holds, because by supposition

$$1 + 2\frac{n-1}{k+1} \leq U,$$

if $k \geq 1$. Similarly, the right side of (33) results from the inequality

$$n \geq \frac{k(k+1)}{2} + 1.$$

REMARK 4.1. Of course this theorem can be proved directly too without our Theorem 3. Different simple unpublished proofs have been given independently of the author by B. Bollobás, J. Galambos, T. Nemetz, and D. Szász.

REMARK 4.2. We may obtain further similar results if we perform for $r = 3$ the same construction as in the proof of Theorem 4.

4. Lower Estimations

THEOREM 5. *If* $\{A_1, A_2, \ldots, A_m\} \in S_K$ *then*

$$\frac{\log n}{\frac{k}{n}\log\frac{n}{k} + \frac{n-k}{n}\log\frac{n}{n-k}} \leq m \tag{34}$$

(log *denotes logarithm with base* 2).

COROLLARY, *Using the inequality* $ln(1 + x) < x$, *we can obtain from* (34) *a weaker but simpler estimation*

$$\frac{n \log n}{k \log \frac{en}{k}} \leq m\,. \tag{35}$$

PROOF. Let $\mathfrak{P}$ be the uniform probability space over the set $H_n = \{x_1, x_2, \ldots, x_n\}$. Denote by α_i the indicator function of A_i, which is now a random variable taking on the value 1 with probability k/n, and the value 0 with the probability $(n-k)/n$, in view of $|A_i| = k$ $(1 \leq i \leq m)$. Denoting by $H(\alpha_i)$ the entropy of the random variable α_i,

$$H(\alpha_i) = \frac{k}{n}\log\frac{n}{k} + \frac{n-k}{n}\log\frac{n}{n-k}\,. \tag{36}$$

Investigate the joint distribution of the random variables $\alpha_1, \alpha_2, \ldots, \alpha_m$. There exist exactly 2^m 0,1 sequences of lenght m, but from these at most n have positive probability, because there are n elementary events in H_n. If for two elementary events x_j and x_l the random sequences $\alpha_1, \alpha_2, \ldots, \alpha_m$ are identical, then x_j and x_l are simultaneously elements of $A_i (1 \leq i \leq m)$ or not; that is, $j = l$ since $\{A_1, A_2, \ldots, A_m\} \in S_K$ is a separating system. Thus the sequence $\alpha_1, \alpha_2, \ldots, \alpha_m$ has n distinct values with probability $1/n$. The entropy of the joint distribution of the α_i is therefore

$$H((\alpha_1, \alpha_2, \ldots, \alpha_m)) = \log n \tag{37}$$

Applying (36), (37) and the well-known inequality (see e.g. [6])

$$H(\alpha_1) + \cdots + H(\alpha_m) \geq H((\alpha_1, \ldots, \alpha_m)),$$

we get the desired inequality (34).

5. Upper Estimation

THEOREM 6. *There exists for arbitrary* $n \geq$ *and* $1 \leq k \leq n/2$ *a system* $\{A_1, A_2, \ldots, A_m\} \in S_K$ *such that*

$$m = \left[\left\{\frac{\log 2n}{\log n/k}\right\} \frac{n}{k}\right]$$

($[x]$ *denotes the greatest integer* $\leq x$).

PROOF. We use Theorem 1, and so we have to find only a system of non-negative integers $m, s_0, s_1, \ldots, s_m$ satisfying the conditions (1), (2), and (3).

Let i be for the moment an arbitrary positive integer, and let r be defined by

$$in \equiv r \pmod{k} \qquad 0 \leq r < k.$$

Determine the integers $s_{i-1} = r$, $s_i = n - r$, $s_t = 0$ ($t = 0, 1, \ldots i - 2, i + 1, \ldots, m$), $m = (in - r)/k$. Thus the properties (1) and (2) obviously hold. We will determine the integer i corresponding to condition (3).

$$n - r \leq \binom{\frac{in - r}{k}}{i} \quad \text{and} \quad r \leq \binom{\frac{in - r}{k}}{i - 1}.$$

These follow from

$$n \leq \binom{\frac{in}{k} - 1}{i} \quad \text{and} \quad r \leq \binom{\frac{in}{k} - 1}{i}. \tag{38}$$

Therefore it is sufficient to investigate (38). Now we need a simple lemma

LEMMA 6. *If* $i > 0$ *is an integer, further* $x \geq 2i$ *and* $x \geq 2$, *then*

$$\frac{1}{2}\left(\frac{x}{i}\right)^i \leq \binom{x - 1}{i} \tag{39}$$

PROOF. If $i \geq j \geq 2$, then $j \leq 2(j - 1)$ and because of $x \geq 2i$

$$ij \leq 2i(j - 1) \leq x(j - 1).$$

That is, $ix - ij \geq ix - x(j-1)$, and finally

$$\frac{x-j}{i-j+1} \geq \frac{x}{i}.$$

If $j = 1$,

$$\frac{x-1}{i} \geq \frac{x}{2i}$$

trivially holds because of $x \geq 2$. Thus we have

$$\frac{1}{2}\left(\frac{x}{i}\right)^i \leq \frac{x-1}{i}\,\frac{x-2}{i-1}\cdots\frac{x-i}{1} = \binom{x-1}{i},$$

and the lemma is proved.

Applying (39), it is sufficient to show that

$$n \leq \frac{1}{2}\,\frac{1}{i^i}\left(\frac{in}{k}\right)^i \quad \text{and} \quad k \leq \frac{1}{2}\,\frac{1}{(i-1)^{i-1}}\left(\frac{in}{k}\right)^{i-1}$$

instead of (38). Both inequalities follow from

$$i \geq \frac{\log 2n}{\log n/k}.$$

Thus set

$$i = \left\{\frac{\log 2n}{\log n/k}\right\};$$

that is,

$$m = \left[\left\{\frac{\log 2n}{\log n/k}\right\}\frac{n}{k}\right],$$

indeed.

6. Further Remarks and Problems

(i) Theorem 6 and the corollary of Theorem 5 give for U the estimation

$$\frac{\log n}{\log en/k}\,\frac{n}{k} \leq U \leq \left\{\frac{\log 2n}{\log n/k}\right\}\frac{n}{k}.$$

The lower and the upper estimations are formally very similar. Moreover the ratio of the two bounds converges to 1 in the case $n \to \infty$ only if $k = o(n)$ and $(\log n)/(\log k) \to 1$.

However, it is easy to see, that the ratio of the estimations is bounded:

$$\frac{\left\{\frac{\log 2n}{\log n/k}\right\}\frac{n}{k}}{\frac{\log n}{\log en/k}\cdot\frac{n}{k}} \leq \frac{\frac{1+\log n}{\log n/k}+1}{\frac{\log n}{\log e+\log n/k}} \leq \frac{2\,\frac{2\log n}{\log n/k}}{\frac{\log n}{(1+\log e)\log n/k}} = 4(1+\log e)$$

If $n \to \infty$, this bound tends to $2(1+\log e)$; if in addition $k = o(n)$ then it tends to 2; finally if $k = cn$ then the limit is $\log(e/c)/\log(1/c)$.

(ii) The most important case is $k = cn$. For this case we have the estimation

$$\frac{\log n}{H(c)} \leq U \leq \left\{\frac{\log 2n}{\log 1/c}\right\}\frac{1}{c},$$

where

$$H(c) = c\log\frac{1}{c} + (1-c)\log\frac{1}{1-c}.$$

On the basis of Theorem 3 it is not difficult to show that the lower estimation is not even asymptotically the best (except for $c = 1/2$). It is well known that

$$\sum_{i=0}^{d\cdot x}\binom{x}{i} \sim \frac{1}{2}\cdot 2^{xH(d)} \qquad \text{for} \qquad 0 < d \leq 1/2.$$

In our case $x = (\log n)/H(c)$. Because of (33) we have

$$r \sim c\,\frac{\log n}{H(c)}.$$

Applying

$$\sum_{i=0}^{r-1} i\binom{x}{i} = x\sum_{i=0}^{r-2}\binom{x-1}{i} = \frac{x}{2}\sum_{i=0}^{r-1}\binom{x}{i} - \frac{r}{2}\binom{x}{r}$$

it is easy to see that (32) cannot hold for $x = (\log n)/H(c)$ and $r = c[(\log n)/H(c)]$, only if $c = 1/2$.

(iii) Our problem admits the following generalization. Let $k_1, k_2, \ldots, k_p$ be non-negative integers satisfying $\sum_{i=1}^{p} k_i = n$, where n is the cardinal number of the set H_n. Further let $A_i (1 \leq i \leq m)$ be a partition of H_n into p parts having cardinal numbers $k_1, k_2, \ldots, k_p$. We call a system $\{A_1, A_2, \ldots, A_m\}$ separating if to any two elements of H_n there

exists a partition A_i which separates these two elements. What is the minimum of m?

Similarly to (1), (2), and (3) we can give necessary conditions for the number of certain columns, but we do not know whether these conditions are sufficient.

References

1. A. Rènyi, On Random Generating Elements of a Finite Boolean Algebra, *Acta Sci. Math. (Szeged)* **22** (1961), 75–81.

2. A. Rènyi, Statistical Laws of Accumulation of Information, *Bull. Inst. Internat. Stat.* **39**, No. 2 (1962) 311–316.

3. A. Rènyi, Az Információ-akkumulació Statisztikus Törvènyszerüsègèröl, *Magyar Tud. Akad. III. Oszt. Közl.* **12** (1962), 15–33.

4. A. Rènyi, On Measures of Entropy and Information, *Proceedings of the Fourth Berkeley Symposium*, Univ. of California Press, Berkeley, Vol. I, 1961, pp. 547–561.

5. A. Rènyi, On a Problem of Information Theory, *Publ. Math. Inst. Hungar. Acad. Sci.* **6** (1961), 505–516.

6. A. Feinstein, *Foundations of Information Theory*, Mc Graw-Hill, New York, 1958.

Printed in Italy by I.T.E.C. - Milan