COMBINATORICA 3 (3—4) (1983) 325—329

MASTERMIND

V. CHVÁTAL

Dedicated to Paul Erdős on his seventieth birthday

Received 2 February 1983

Let $V(n, k)$ denote the set of vectors of length n whose components are integers j with $1 \leqq j \leqq k$. For every two vectors x, y in $V(n, k)$, let $a(x, y)$ stand for the number of subscripts i with $x_i = y_i$. We prove that for every positive ε there is an $n(\varepsilon)$ with the following property: if $n > n(\varepsilon)$ and $k < n^{1-\varepsilon}$ then there is a set Q of at most $(6+\varepsilon)(n \log k)/(\log n - \log k)$ vectors in $V(n, k)$ such that for every two distinct vectors x, y in $V(n, k)$ some q in Q has $a(q, x) \neq a(q, y)$.

Mastermind is a game for two players, called *S.F.* and the *P.G.O.M.* In the beginning, S.F. creates a "mystery vector" $m = [m_1, m_2, \ldots, m_n]$ such that each m_i is one of the "colors" $1, 2, \ldots, k$. The P.G.O.M. (who knows both n and k) then proceeds to determine m by asking a number of questions, which are answered by S.F. Each question q is a vector $[q_1, q_2, \ldots, q_n]$ such that each q_i is one of the k colors; each answer consists of a pair of numbers $a(q, m)$, $b(q, m)$ such that $a(q, m)$ is the number of subscripts i with $q_i = m_i$ and $b(q, m)$ is the largest $a(q, \tilde{m})$ with $\tilde{m}$ running through all the permutations of m.

In the commercial version that became popular a few years ago, $n=4$ and $k=6$ (with each answer represented by $a(q, m)$ black pins and $b(q, m) - a(q, m)$ white pins); Knuth [1] has shown that four questions suffice to determine m in this case. The generalization to arbitrary n and k was suggested by Pierre Duchet, who asked for

(i) the smallest number $f(n, k)$ such that the P.G.O.M. can determine any m by asking $f(n, k)$ questions (waiting, as usual, for each answer before asking the next question), and

(ii) the smallest number $g(n, k)$ such that the P.G.O.M. can determine any m by asking $g(n, k)$ questions at once (without waiting for the answers).

Trivially, $f(n, k) \leqq g(n, k)$; Duchet also observed that

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

AMS subject classification (1980): 05 B 99; 94 A 50, 90 D 99.

(The proof is routine: there are no more than $\binom{n+2}{2}$ possible answers to each question, and the sequence of $f(n, k)$ answers has to distinguish between every two of the k^n possible mystery vectors.) The purpose of this paper is to establish upper bounds on $f(n, k)$; in particular, we shall show that the lower bound (1) is best possible (up to a constant factor) whenever k is small relative to n. Throughout, we shall let ln and log stand for the natural and the binary logarithms, respectively.

Theorem 1. *For every positive ε there is an $n(\varepsilon)$ with the following property: if $n>n(\varepsilon)$ and if $k<n^{1-\varepsilon}$* then

$$g(n, k) \leqq (2+\varepsilon) n \frac{1+2\log k}{\log n-\log k}. \tag{2}$$

Proof. By a *difference pattern*, we shall mean a nonempty set I of subscripts along with two distinct colors x_i, y_i for each $i\in I$; we shall say that this difference pattern is *split* by a question q if the number of subscripts $i\in I$ with $q_i=x_i$ differs from the number of subscripts $i\in I$ with $q_i=y_i$. Note that every two distinct candidates x, y for the mystery vector define a unique difference pattern by $i\in I$ iff $x_i\neq y_i$, and that this difference pattern is split by a question q if and only if $a(q, x)\neq a(q, y)$. Thus we only need establish the existence of a set Q of questions such that every difference pattern is split by some question in Q, and such that $|Q|=N$ with N standing for the right-hand side of (2) rounded down to the nearest integer.

We claim that such a set may be obtained by taking N questions at random: the probability that the result will fail to have the property required of Q is less than $1/n$. To justify this claim, let $p(d, k)$ stand for the probability that an arbitrary but fixed difference pattern with $|I|=d$ is *not* split by a randomly chosen question, and observe that

$$p(d, k) = \frac{1}{k^d}\sum_i \binom{d}{2i}\binom{2i}{i}(k-2)^{d-2i} = \sum_i \binom{d}{2i}\left(\frac{2}{k}\right)^{2i}\left(1-\frac{2}{k}\right)^{d-2i}\cdot\frac{\binom{2i}{i}}{2^{2i}},$$

Since the probability that at least one difference pattern is split by none of the N questions does not exceed

$$\sum_{d=1}^{n}\binom{n}{d}(k(k-1))^d(p(d, k))^N,$$

we only need prove that

$$\binom{n}{d}(k(k-1))^d(p(d, k))^N < n^{-2}. \tag{3}$$

For this purpose, we divide the range of d into two parts.

In case $d\leqq n^{1-\delta}$ with $\delta=\varepsilon^3$, we shall establish the inequality

$$n^{5d}(p(d, k))^N < 1$$

which is stronger than (3). First, observe that $\binom{2i}{i}2^{-2i}\leqq\frac{1}{2}$ whenever $i\geqq 1$, and so

$$p(d, k) \leqq \left(1-\frac{2}{k}\right)^d + \frac{1}{2}\sum_{j=1}^{d}\binom{d}{j}\left(\frac{2}{k}\right)^j\left(1-\frac{2}{k}\right)^{d-j} = 1-\frac{1}{2}\left(1-\left(1-\frac{2}{k}\right)^d\right).$$

It follows that

$$\ln p(d, k) \leqq -\frac{1}{2}\left(1-\left(1-\frac{2}{k}\right)^{d}\right) \leqq -\frac{1}{2}(1-e^{-2d/k}),$$

and so

$$\frac{N}{5d}\ln\frac{1}{p(d, k)} \geqq \frac{\left(2+\frac{1}{2}\varepsilon\right)}{5d}\, n\,\frac{1+2\log k}{\log n-\log k}\cdot\frac{1-e^{-2d/k}}{2}.$$

Observing that $(1-e^{-2d/k})/d$ is a decreasing function of d, and that $2n^{1-\delta}/k \geqq 2n^{\varepsilon-\delta} \geqq 1$ whenever $n > n(\varepsilon)$, we conclude that

$$\frac{N}{5d}\ln\frac{1}{p(d, k)} \geqq \frac{\left(2+\frac{1}{2}\varepsilon\right)}{20}\, n^{\delta}\,\frac{1+2\log k}{\log n-\log k} \geqq \frac{n^{\delta}}{10\log n} > \ln n,$$

whenever $n > n(\varepsilon)$.

In case $d \geqq n^{1-\delta}$ with $\delta = \varepsilon^3$, we shall establish the inequality

$$2^n k^{2n}(p(d, k))^N < n^{-2}$$

which is stronger than (3). First, observe that $\binom{2i}{i}2^{-2i} \leqq (\pi i)^{-1/2}$ whenever $i \geqq 1$, and so

$$\begin{aligned} p(d, k) &\leqq \sum_{j \leqq d/k}\binom{d}{j}\left(\frac{2}{k}\right)^{j}\left(1-\frac{2}{k}\right)^{d-j} + \left(\frac{d}{k}\right)^{-1/2}\cdot\sum_{j \geqq d/k}\binom{d}{j}\left(\frac{2}{k}\right)^{j}\left(1-\frac{2}{k}\right)^{d-j} \\ &\leqq \left(\frac{2}{e}\right)^{d/k} + \left(\frac{d}{k}\right)^{-1/2}. \end{aligned}$$

Since $d/k \geqq 2n^{\varepsilon-\delta}$, it follows that

$$p(d, k) \leqq \left(\frac{d}{2k}\right)^{-1/2}$$

whenever $n > n(\varepsilon)$, and so

$$\begin{aligned} N\log\frac{1}{p(d, k)} &\geqq \left(2+\frac{1}{2}\varepsilon\right) n\,\frac{1+2\log k}{\log n-\log k}\cdot\frac{(1-\delta)\log n-\log k-1}{2} \\ &= \left(1+\frac{1}{4}\varepsilon\right) n(1+2\log k)\,\frac{(1-\delta)\log n-\log k-1}{\log n-\log k} \\ &\geqq \left(1+\frac{1}{4}\varepsilon\right)\left(1-\frac{\delta}{2\varepsilon}\right) n(1+2\log k) \\ &\geqq \left(1+\frac{1}{8}\varepsilon\right) n(1+2\log k) > n+2n\log k+2\log n \end{aligned}$$

whenever $n > n(\varepsilon)$. ∎

When $k=n$, the lower bound (1) is linear in n; the best upper-bound we can offer goes as follows.

Theorem 2. *If* $n \leqq k \leqq n^2$ *then* $f(n, k) \leqq 2n \log k + 4n$.

Proof. First, let $A(n)$ denote the smallest number of questions that suffice to determine the mystery vector m if $k=n$ (assuming that each question q is answered only by $a(q, m)$). Observe that

$$A(r+s) \leqq 2(r+s-1)+A(r)+A(s): \tag{4}$$

the mystery vector may be determined by

(i) asking $r+s$ questions (with $q_i=j$ if $1 \leqq i \leqq r$, $q_i=1$ if $r<i \leqq r+s$, and with j ranging through $1, 2, \ldots, r+s$) to find out which colors appear in the first r components of m,

(ii) asking $r+s-2$ questions (with $q_i=1$ if $1 \leqq i \leqq r$, $q_i=j$ if $r<i \leqq r+s$, and with j ranging through $2, 3, \ldots, r+s-1$) to find out which colors appear in the last s components of m,

(iii) asking $A(r)$ questions (with $q_i=1$ if $r<i \leqq r+s$) to determine the first r components of m,

(iv) asking $A(s)$ questions (with $q_i=1$ if $1 \leqq i \leqq r$) to determine the last s components of m.

Since $A(1)=0$, repeated applications of (4) with $r=s$ and $r=s+1$ show that

$$A(n) \leqq 2(n\lceil \log n \rceil - 2^{\lceil \log n \rceil}+1),$$

and so $A(n) \leqq 2n\lceil \log n \rceil$.

Next, let $B(n, k)$ denote the smallest number of questions that suffice to find a set C of n colors such that $m_i \in C$ for all i (assuming that each question q is answered only by $b(q, m)$). Observe that

$$B(n, 2sn) \leqq 2n+B(n, sn) \quad \text{for} \quad s=1, 2, \ldots, n: \tag{5}$$

at least sn absent colors may be identified by splitting the set of $2sn$ colors into disjoint sets $C_1, C_2, \ldots, C_{2n}$ of size s and asking $2n$ questions, the j-th of which involves all the colors in C_j (and no other colors). Repeated applications of (5) show that

$$B(n, 2^t n) \leqq 2tn \quad \text{for all} \quad t=0, 1, \ldots, \lceil \log n \rceil,$$

and so $B(n, k) \leqq 2n\lceil \log k/n \rceil$ whenever $n \leqq k \leqq n^2$.

Now the theorem follows by observing that $f(n, k) \leqq B(n, k)+A(n)$. ∎

In closing, let us note that $f(n, k) \sim k/n$ as soon as $k/n^2 \log n \to \infty$: more precisely,

$$(k-1)/n \leqq f(n, k) \leqq \lceil k/n \rceil + f(n, n^2)$$

for all n and k. To justify the upper bound, note that $\lceil k/n \rceil$ questions suffice to confine the range of colors to at most n^2; the lower bound is justified by the following trivial argument. If the P.G.O.M. is allowed fewer than $(k-1)/n$ questions then some two colors r, s must be missing from all of his questions; now S.F. can answer all the questions by $a(q, m)=b(q, m)=0$, leaving the P.G.O.M. in a painful doubt as to which of the 2^n vectors composed of r and s is the mystery vector.

Note added in proof. I had thought it appropriate to dedicate this particular paper to E.P. for his birthday, since I learned the kind of methods used here from him. Unfortunately, I was too right: over four months after the manuscript was submitted for publication, V. Rödl informed me that the problem of determining $g(n, 2)$ had been known as the "coin-weighing problem" and, in particular, my proof of Theorem 1 turns out to be an extension of an argument used by Erdős and Rényi in "On two problems in information theory", Magyar Tud. Akad. Mat. Kut. Int. Közl. 8 (1963), 229—242.

Reference

[1] D. E. Knuth, The computer as a Master Mind, *Journal of Recreational Mathematics* **9** (1976—77), 1—6.

V. CHVÁTAL

School of Computer Science
McGill University
Montreal, PQ, H3A 2K6 Canada