JOURNAL OF COMBINATORIAL THEORY (A) 22, 352–360 (1977)

Note

On the Maximum Number of Permutations with Given Maximal or Minimal Distance

PETER FRANKL

Eötvös L. University, Budapest, Hungary, and Université de Paris VII, France

AND

MIKHAIL DEZA

CNRS, 15, Quai Anatole-France, 75007 Paris, France

Communicated by the Managing Editors

Received February 19, 1976

Let us denote by $R(k, \geqslant\lambda)[R(k, \leqslant\lambda)]$ the maximal number $\mathscr{M}$ such that there exist $\mathscr{M}$ different permutations of the set $\{1,..., k\}$ such that any two of them have at least λ (at most λ, respectively) common positions. We prove the inequalities $R(k, \leqslant\lambda) \leqslant kR(k-1, \leqslant\lambda-1)$, $R(k, \geqslant\lambda) \geqslant R(k, \leqslant\lambda-1) \leqslant k!$, $R(k, \geqslant\lambda) \leqslant kR(k-1, \geqslant\lambda-1)$. We show: $R(k, \geqslant k-2) = 2$, $R(k, \geqslant 1) = (k-1)!$, $R(p^m, \geqslant 2) = (p^m-2)!$, $R(p^m+1, \geqslant 3) = (p^m-2)!$, $R(k, \leqslant k-3) = k!/2$, $R(k, \leqslant 0) = k$, $R(p^m, \leqslant 1) = p^m(p^m-1)$, $R(p^m+1, \leqslant 2) = (p^m+1)p^m(p^m-1)$. The exact value of $R(k, \geqslant\lambda)$ is determined whenever $k \geqslant k_0(k-\lambda)$; we conjecture that $R(k, \geqslant\lambda) = (k-\lambda)!$ for $k \geqslant k_0(\lambda)$. Bounds for the general case are given and are used to determine that the minimum of $| R(k, \geqslant\lambda) - R(k, \leqslant\lambda)|$ is attained for $\lambda = (k/2) + O(k/\log k)$.

In this paper we consider extremal problems for permutations which were raised in [2].

Let k be a positive integer and let K denote the set $\{1,..., k\}$. Let us denote by $F(P)$ the set of elements of K which are left fixed by the permutation P, acting on K. Let the cardinality of $F(P)$ be $f(P)$. We say that the permutations Q and R acting on K coincide in m positions if $f(Q^{-1}R) = m$ (Q^{-1} is the permutation inverse to Q, obviously $f(Q^{-1}R) = f(R^{-1}Q)$).

The distance of two permutations Q, R is $k - f(Q^{-1}R)$. With this distance the set of permutations of K becomes a metric space, which is easily verified.

Let $\mathscr{P} = \{P_1, ..., P_s\}$ be a set of permutations of K. We are concerned with the following problem: What is the maximum possible value of s if, for $1 \leqslant i < j \leqslant s$, $f(P_i^{-1}P_j) \geqslant \lambda$ ($f(P_i^{-1}P_j) \leqslant \lambda$, respectively) ($\lambda$ is an integer).

Using the terminology of [2] let us denote these maximum values of s by $R(k, \geqslant\lambda)$ ($R(k, \leqslant\lambda)$, respectively). It is evident that $R(k, \geqslant k-1) = 1$, $R(k, \geqslant 0) = k!$, $R(k, \leqslant k-1) = k!$ and that $R(k, \geqslant\lambda)(R(k, \leqslant\lambda))$ is a monotonically decreasing (increasing, resp.) function of λ.

Now we prove two inequalities ($k \geqslant 2; \lambda \geqslant 1$)

$$R(k, \leqslant\lambda) \leqslant kR(k-1, \geqslant\lambda - 1), \tag{1}$$

$$R(k, \geqslant\lambda) \leqslant kR(k-1, \leqslant\lambda - 1). \tag{2}$$

Proof. For $i = 1,..., k$ let P_i be any permutation of K such that $P(i) = 1$. Let $\{Q_1,..., Q_m\}$ be any collection of permutations of K such that any two different permutations belonging to it coincide in at least (at most, resp.) λ positions. Let us choose j in such a way that there are at least m/k permutations among the Q_i's which satisfy $Q_i(1) = j$. As there are k possibilities for $Q_i(1)$, this choice of j is always possible. Hence we may assume that for some $t \geqslant m/k$, the permutations $Q_1,..., Q_t$ satisfy $Q_i(1) = j$ for $i = 1,..., t$. As the distance of two permutations P, Q is the same as the distance of the permutations RP, RQ, where R is an arbitrary permutation of K, so by the assumption that any two different permutations among $P_jQ_t,..., P_jQ_t$ coincide in at least (at most) λ positions. As for $i = 1,..., t$, $P_jQ_i(1) = P_j(Q_i(1)) = 1$, so P_jQ_i can be regarded as a permutation of $K - \{1\}$ as well ($i = 1,..., t$). Hence, regarded as permutations of $K - \{1\}$, any two different ones must coincide in at least (at most) $\lambda - 1$ positions, which entails $t \leqslant R(k-1, \geqslant\lambda - 1)(t \leqslant R(k-1, \leqslant\lambda - 1))$. As $m \leqslant kt$, inequalities (1) and (2) follow.

1

At first we prove a lemma which will be a fundamental tool in establishing the main results of this paragraph.

LEMMA.

$$R(k, \geqslant\lambda)\, R(k, \leqslant\lambda - 1) \leqslant k! \qquad (\lambda \geqslant 1). \tag{3}$$

Proof. Let $\mathscr{P}$ and $\mathscr{Q}$ be sets of permutations of K such that any two different elements of $\mathscr{P}$ ($\mathscr{Q}$) coincide in at least λ (in at most $\lambda - 1$) positions, respectively. Let us suppose that the cardinalities of $\mathscr{P}$ and $\mathscr{Q}$ are $R(k, \geqslant\lambda)$ and $R(k, \leqslant\lambda - 1)$, respectively. Let us form all the possible products of the form PQ, $P \in \mathscr{P}$, $Q \in \mathscr{Q}$. We claim that they are all different permutations of K. Let us suppose that $P_1, P_2 \in \mathscr{P}$, $Q_1, Q_2 \in \mathscr{Q}$, and $P_1Q_1 = P_2Q_2$, or equivalently $P_1^{-1}P_2 = Q_1Q_2^{-1}$. As $f(P_1^{-1}P_2) \geqslant \lambda$ so $f(Q_2^{-1}Q_1) = f(Q_1Q_2^{-1}) \geqslant \lambda$.

By the definition of $\mathscr{Q}$ it is possible only for $Q_1 = Q_2$, and consequently $P_1 = P_2$.

So we have proved the existence of $R(k, \geqslant\lambda)\, R(k, \leqslant\lambda - 1)$ different permutations of the k-element set K, which proves the lemma.

THEOREM 1.

(i) $R(k, \geqslant 1) = (k-1)!$, $R(k, \leqslant 0) = k$;

(ii) $R(p^m, \geqslant 2) = (p^m - 2)!$, $R(p^m, \leqslant 1) = p^m(p^m - 1)$ (*p is a prime*, $m \geqslant 1$ *is an integer*);

(iii) $R(p^m + 1, \geqslant 3) = (p^m - 2)!$, $R(p^m + 1, \leqslant 2) = (p^m + 1) \times p^m(p^m - 1)$ ($m \geqslant 1$ *is an integer*);

(iv) $R(k, \geqslant k-2) = 2!$, $R(k, \leqslant k-3) = k!/2$ ($k \geqslant 2$).

Proof. In view of the lemma, in order to prove the theorem it is sufficient to show that the left-hand sides of the above equalities are greater than or equal to the corresponding right-hand sides. There are exactly $(k - \lambda)!$ permutations of K which leave all the numbers $1,..., \lambda$ unchanged, whence $R(k, \geqslant\lambda) \geqslant (k-\lambda)!$

Let C be the permutation which takes i into $i + 1$ for $i = 1,..., k-1$ and $C(k) = 1$. Then the permutations $C, C^2,..., C^k$ coincide nowhere, which proves $R(k, \leqslant 0) \geqslant k$. Hence (i) is proved.

Let $k = p^m$ (p a prime, m an integer, $m \geqslant 1$). Let $x_1,..., x_{p^m}$ be the elements of $GF(p^m)$. Let us denote by L the group of affine transformations of $GF(p^m)$ of the form $ax + b$, $a \neq 0$, $a, b \in GF(p^m)$.

There corresponds to every transformation of the set $\{x_1,..., x_{p^m}\}$ a permutation of the set $\{1,..., p^m\}$. Let $\mathscr{P}$ be the group of permutations corresponding to the transformations L. It can be easily verified that $\mathscr{P}$ is sharply doubly transitive, and consequently any two different permutations belonging to $\mathscr{P}$ coincide in at most one position. It proves $R(p^m, \leqslant 1) \geqslant p^m(p^m - 1)$. Hence assertion (ii) follows. To prove (iii) let us consider the group $PGL(2, p^m)$, the group of all the projective transformations of the projective line over the finite field of p^m elements. $PGL(2, p^m)$ can be regarded as a group of permutations on the set $\{1,..., p^m + 1\}$, and it is sharply triply transitive (see [4]). Hence any two permutations belonging to $PGL(2, p^m)$ coincide in at most two positions, which entails $R(k, \leqslant 2) \geqslant |PGL(2, p^m)| = (2^m + 1)\, p^m(p^m - 1)$. Hence (iii) is proved. To prove (iv) let us consider the alternating group A_k. It is sharply $(k-2)$-ply transitive of order $\frac{1}{2}k!$, and the assertion of (iv) follows as in the other cases. The proof of the theorem is complete.

In connection with the above results, the authors make the following conjecture.

Conjecture. For $k \geqslant k_0(\lambda)$,

$$R(k, \geqslant\lambda) = (k-\lambda)!.$$

2

In this section the value of $R(k, \geqslant\lambda)$ is determined for $k \geqslant k_0(k-\lambda)$. Let us denote $k - \lambda$ by r.

If P is a permutation of the set K, then let $E(P)$ denote $K - F(P)$, i.e., the set of numbers which are effectively moved by P. If Q is another permutation of K then it is obvious that P and Q cannot coincide on any element of the set $E(P) * E(Q)$ ($*$ denotes the symmetric difference). On the other hand, they coincide on the set $K - (E(P) \cup E(Q))$. Let $\mathscr{F}_r$ denote the set of all permutations P of K such that $|E(P)| \leqslant t$ if $r = 2t$, and the set of all permutations Q of K such that $|E(P) \cap (K - \{1\})| \leqslant t$ if $r = 2t + 1$. It can be easily verified that any two permutations in $\mathscr{F}_r$ coincide in at least λ positions. Hence, $R(k, \geqslant\lambda) \geqslant |\mathscr{F}_r|$.

THEOREM 2. *For $r \geqslant 3$, $k \geqslant k_0(r)$,*

$$R(k, \geqslant k - r) = |\mathscr{F}_r|.$$

Remark. As we have seen for $r = 2$, $R(k, \geqslant k - 2) = 2 \neq 1 = |\mathscr{F}_2|$. For the cardinality of $\mathscr{F}_r$ the following expressions can be given:

$$\begin{aligned} |\mathscr{F}_r| &= \sum_{i=0}^{t} D_i \binom{k}{i}, && \text{for} \quad r = 2t, \\ &= \sum_{i=0}^{t} D_i \binom{k}{i} + \binom{k-1}{t} D_{t+1}, && \text{for} \quad r = 2t+1. \end{aligned} \tag{4}$$

(D_i is the number of permutations of order i not fixing any letter, i.e., $D_i = i!(\sum_{j=0}^{i}(-1)^j(1/j!))$.)

Proof. Let $\mathscr{P}$ be a set of permutations of K such that any members of $\mathscr{P}$ coincide in at least $k - r$ positions and $|\mathscr{P}| = R(k, \geqslant k - r)$. Let Q be an arbitrary permutation of K. Then the set of permutations $\{QP \mid P \in \mathscr{P}\}$ has the desired properties too. Hence we may assume that the identity permutation belongs to $\mathscr{P}$. As a consequence we have $|E(P)| \leqslant r$ for any $P \in \mathscr{P}$. Let P_0 be an element of $\mathscr{P}$ such that $|E(P_0)|$ is maximal.

We assert that for any $P \in \mathscr{P}$ $|E(P) - E(P_0)| \leqslant r/2$. Suppose that for some $P \in \mathscr{P}$ $|E(P) - E(P_0)| > r/2$. Then by the maximality of $|E(P_0)|$ $|E(P_0) - E(P)| > r/2$, implying $|E(P) * E(P_0)| > r$, a contradiction.

Let us choose $P_1 \in \mathscr{P}$ in such a way that $|E(P_1) - E(P)| = [r/2]$, and if we have already chosen P_i then choose a $P_{i+1} \in \mathscr{P}$ satisfying $|E(P_{i+1}) - \bigcup_{j=0}^{i} E(P_j)| = [r/2]$. Suppose that for some $i < 3r$ we cannot find any $P \in \mathscr{P}$ satisfying this condition. It means that for any $P \in \mathscr{P}$, $|E(P) \cap$

$(K - \bigcup_{j=0}^{i} E(P_j))| \leqslant [r/2]$, entailing that the number of different $E(P)$'s is less than $2^{3r^2} \sum_{j=0}^{[r/2]-1} \binom{k}{j}$. As to a given set $E(P)$, there correspond at most $(| E(P)|)! \leqslant r!$ permutations of $\mathscr{P}$, so we obtain

$$| \mathscr{P} | \leqslant \sum_{j=0}^{[r/2]-1} \binom{k}{j} 2^{3r^2} r! < | \mathscr{F}_r |, \qquad \text{for} \quad k > k_0(r), \text{ a contradiction.}$$

Let us separate two cases:

(a) $r = 2t$. Let $| E(P_0)| = t + s, 0 \leqslant s \leqslant t$. If for some i, $1 \leqslant i \leqslant 3t + 1$, $| E(P_i)| < t + s$, then as $| E(P_i) - E(P_0)| \geqslant t$ so $| E(P_0) - E(P)| > t$, implying $| E(P) * E(P_0)| > 2t$, a contradiction. Hence for $i = 1,..., 3t + 1$, $| E(P_i)| = t + s$. Then $| E(P_i) * E(P_0)| = 2t$, implying that the two permutations coincide in every position of $E(P) \cap E(P_0)$. We assert that for $i = 2,..., 3t + 1$ $E(P_i) \cap E(P_0) = E(P_1) \cap E(P_0)$. Indeed, if it is not the case, then $| E(P_i) \cap E(P_1)| < s$, implying $| E(P_i) * E(P_1)| \geqslant 2(t + 1) > 2t$, a contradiction. Hence any of the permutations $P_0 ,..., P_{3t+1}$ act in the same way on $E(P_0) \cap E(P_1)$. It follows that this set is invariant under P_i $i = 1,..., 3t + 1$. Let Q be the permutation which coincides with P_0 on $E(P_1) \cap E(P_0)$ and with the identity on the rest of K. Let us set

$$\mathscr{P}_Q = \{PQ^{-1} \mid P \in \mathscr{P}\}.$$

Then for $0 \leqslant i \leqslant j \leqslant 3t + 1$, $| E(P_iQ^{-1})| = t$, and for $i \neq j$, $E(P_i) \cap E(P_j) = \varnothing$. As $| E(Q)| \leqslant S \leqslant t$ so for $P \in \mathscr{P}$ $| E(PQ^{-1})| \leqslant 3t$. Let us suppose that for some $P \in \mathscr{P}_Q$ $| E(P)| > t$. As any two permutations belonging to P_Q coincide in at least $k - r$ positions, so for $i = 1,..., 3t + 1$ $| E(P) * E(P_iQ^{-1})| \leqslant 2t$, implying that $E(P)$ intersects each of the mutually disjoint sets $E(P_iQ^{-1})$, contradicting $| E(P)| \leqslant 3t$. Hence, for any $P \in \mathscr{P}_Q$, $| E(P)| \leqslant t$, i.e., $\mathscr{P}_Q \subseteq \mathscr{F}_r$, and we are done.

(b) $r = 2t + 1$. Let $| E(P_0)| = t + s$, $0 \leqslant s \leqslant t + 1$. If for some $1 \leqslant i < 3r$, $| E(P_i)| \leqslant | E(P_0)| - 2$, then $| E(P_0) - E(P_i)| \geqslant | E(P_i) - E(P_0)| + 2 \geqslant t + 2$, implying $| E(P_i) * E(P_0)| \geqslant 2t + 2 > r$, a contradiction. Hence for $| E(P_i)|$ there are only two possibilities, namely, $t + s$ and $t + s - 1$. Let us first consider the case when there are at least $3t + 1$ among the P_i's such that $| E(P_i)| = t + s - 1$. Then we may assume that for $i = 1,..., 3t + 1$, $| E(P_i)| = t + s - 1$. It follows that $| E(P_0) - E(P_i)| = t + 1$, whence $| E(P_0) * E(P_i)| = r$. Consequently, P_0 and P_i coincide on $E(P_0) \cap E(P_i)$ for $i = 1,..., 3t + 1$. If for some i, $2 \leqslant i \leqslant 3t + 1$, $E(P_0) \cap E(P_1) \neq E(P_0) \cap E(P_i)$, then it follows that $| E(P_1) * E(P_i)| > r$, a contradiction.

Now we can choose Q, and define $\mathscr{P}_Q$ as in case (a). For $i = 0,..., 3t + 1$, $E(P_iQ^{-1})$ are pairwise disjoint subsets of K. $|E(P_iQ^{-1})| = t$ for $i \neq 0$ and $|E(P_0Q^{-1})| = t + 1$. $|E(Q)| \leqslant s - 1 \leqslant t$, implying $|E(PQ^{-1})| \leqslant 3t + 1$ for $P \in \mathscr{P}$.

If, for some $R \in \mathscr{P}_Q$, $|E(R)| \geqslant t + 2$, then we come to a contradiction, as in case (a). If $R_1, R_2 \in \mathscr{P}_Q$ and $|E(R_1)| = t + 1 = |E(R_2)|$, then $E(R_1) \cap E(R_2) \neq \varnothing$, implying by the Erdös–Ko–Rado theorem (see [3]) that there are at most $\binom{k-1}{t}$ different $(t + 1)$-element sets among the $E(PQ^{-1})$'s. As to a given j-element subset L of K there are at most D_j different permutations P belonging to $\mathscr{P}_Q$ such that $E(P) = L$, so the statement of the theorem follows.

Let us suppose now that at most $3t$ permutations among the P_i's have cardinality $t + s - 1$. Then there are at least $3t + 2$ of cardinality $t + s$. Hence it can be assumed that for $i = 1,..., 3t + 2$, $|E(P_i)| = t + s$. It follows in exactly the same way as before that for $i = 2,..., 3t + 2$, $E(P_i) \cap E(P_0) = E(P_1) \cap E(P_0)$. Let us set $E(P_1) \cap E(P_0) = A$. Then A is an s-element subset of K. Any two of the permutations P_i can differ in at most one position of A. If for some i_1, i_2, i_3, P_{i_1} and P_{i_j} differ on A in the position a_j $(j = 2, 3)$ then P_{i_2} and P_{i_3} differ in both positions, implying $a_2 = a_3$. Hence we can find an $a \in A$ such that all the permutations $P_0,..., P_{3t+2}$ coincide on the set $A_1 = A - \{A\}$. Let us set $P_0(A_1) = A_2$. Then $A_2 \subset A$, $|A - A_2| = 1$. Let $A - A_2$ consist of the single element b. Let us define the permutation Q in the following way: $Q(d) = d$ for $d \in K - A$, $Q(d) = P_0(d)$ for $d \in A_1$, and $Q(a) = b$. $|E(Q)| \leqslant s \leqslant t + 1$, implying that $|E(PQ^{-1})| \leqslant 3t + 2$ for any $P \in \mathscr{P}$. For $i = 0,..., 3t + 2$, $E(P_iQ^{-1}) \subseteq E(P_iQ^{-1}) - A_2$, implying $|E(P_iQ^{-1})| \leqslant t + 1$ and that the sets $E(P_iQ^{-1})$ have pairwise at most the element b in common. Now the proof can be finished, as in the other subcase of case (b).

Remark. This theorem can be regarded as the analog of a theorem of Katona [5].

3

Here we give estimations of the functions $R(k, \geqslant\lambda)$, $R(k, \leqslant\lambda)$ for the general case.

The set of permutations of $K = \{1,..., k\}$ is a metric space where the distance $d(P_1, P_2)$ is the number of different positions, i.e., $d(P_1, P_2) = k - f(P_1, P_2)$. Let S_r denote the volume of the sphere of radius r in this space (it is obviously independent of the center). Let D_i denote the number of derangements of i elements. It is well known that $D_i \sim i!/e$. Therefore, $S_r = 1 + \sum_{i=2}^{r} D_i\binom{k}{i} \sim e^{-1}k! \sum_{i=k-1}^{k-2} (1/i!)$.

Let us consider $R(k, \geqslant\lambda)$ at first. Let us set

$$T_1(k,\lambda) = \begin{cases} \sum_{i=0}^{(k-\lambda)/2} \binom{k}{i} D_i, & \text{if } k-\lambda \text{ is even,} \\ \sum_{i=0}^{(k-\lambda-1)/2} \binom{k}{i} D_i + \binom{k-1}{(k-\lambda-1)/2} D_{(k-\lambda+1)/2}, & \text{if } k-\lambda \text{ is odd;} \end{cases}$$

$$T_2(k,\lambda) = \begin{cases} \sum_{i=0}^{(k-\lambda)/2} \binom{k}{i}, & \text{if } k-\lambda \text{ is even,} \\ \sum_{i=0}^{(k-\lambda-1)/2} \binom{k}{i} + \binom{k}{(k-\lambda-1)/2}, & \text{if } k-\lambda \text{ is odd.} \end{cases}$$

THEOREM 3.

$$\max((k-\lambda)!, T_1(k,\lambda)) \leqslant R(k, \geqslant\lambda) \leqslant D_{k-\lambda} T_2(k,\lambda).$$

Proof. We have already proved the lower estimation in Sections 1 and 2. In order to prove the upper estimation make use of the following inequality for the distance of two permutations P_1, P_2 of K:

$$d(P_1, P_2) \geqslant |E(P_1) * E(P_2)|.$$

Let $\mathscr{P} = \{P_1, ..., P_m\}$ be a set of permutations of K satisfying $d(P_i, P_j) \geqslant k - \lambda$ (for $1 \leqslant i < j \leqslant m$) and suppose $m = R(k, \geqslant\lambda)$. Let us define $\mathscr{B} = \{E(P_1), ..., E(P_m)\}$. Then for $1 \leqslant i \subset j \leqslant m$ we have $|E(P_i) * E(P_j)| \leqslant d(P_i, P_j) \leqslant k - \lambda$. Kleitman [6] proved that under these conditions $|\mathscr{B}| \leqslant T_2(k,\lambda)$. We may assume that P_1 is the identity permutation of K. Then for any $P \in \mathscr{P}$ $|E(P)| \leqslant k - \lambda$. If $E(P) = B$ then P fixes the elements of $K - B$ and acts as a disorder on the set B. If $P_{i_1}, ..., P_{i_u}$ are the different permutations belonging to $\mathscr{P}$ such that $E(P_{i_j}) = B$ for $j = 1, ..., u$, then $u \leqslant D_{|B|} \leqslant D_{k-\lambda}$. So $R(k, \geqslant\lambda) \leqslant D_{k-\lambda} |B| \leqslant D_{k-\lambda} T_2(k,\lambda)$. Q.E.D.

Remark. It follows from Theorem 2 that the upper estimation is far from being best possible. In general, the lower bound is not best possible either, as the following example shows. Let us set $\lambda = k - [k^{1/q}]$ $(1 < q < 2)$, $k > k_0(q)$. In this case, $(k-\lambda)! > T_1(k,\lambda)$ (it can be easily verified using $D_i \sim i!/e$ and the Stirling formula). Let us set $L = \{1, ..., [k^{1/q}] - 2\}$ and $\mathscr{L} = \{P \mid |E(P) \cap (K - L)| \leqslant 1$, then for $P_1, P_2 \in \mathscr{L}$ $d(P_1, P_2) \leqslant k - \lambda$. $|\mathscr{L}| \geqslant |K - L| D_{|L|+1} \geqslant (k - k^{1/q})([k^{1/q}] - 1)!/e > [k^{1/q}]! = (k-\lambda)!$
In connection with the above example we have the following

Conjecture. Let $\mathscr{F}$ be a family of subsets of K such that $|F_1 \cup F_2| \leqslant$

$k - \lambda$ for $F_1, F_2 \in \mathscr{F}$ and let us define $\mathscr{P}_{\mathscr{F}} = \{P \mid P$ is a permutation of K, $E(P) \in \mathscr{F}\}$. Then $R(k, \geqslant\lambda) = \max_{\mathscr{F}} |\mathscr{P}_{\mathscr{F}}|$.

Let us consider now the function $R(k, \leqslant\lambda)$ which is analogous to the cardinality of maximum codes with minimal distance $k - \lambda$ from coding theory [1].

THEOREM 4.

$$k!/S_{k-\lambda-1} \leqslant R(k, \leqslant\lambda) \leqslant k!/\max((k - \lambda - 1)!, T_1(k, \lambda + 1)).$$

Proof. The upper bound follows directly from $R(k, \leqslant\lambda)R(k, \geqslant\lambda + 1) \leqslant k!$ (lemma of Section 1) and the lower bound of Theorem 3. Suppose that $k!/S_{k-\lambda-1} > R(k, \leqslant\lambda)$. Let $\mathscr{P} = \{P_1, ..., P_m\}$ be a set of permutations of K such that for $1 \leqslant i < j \leqslant m$, $d(P_i, P_j) \geqslant k - \lambda$ and $m = R(k, \leqslant\lambda)$. $mS_{k-\lambda-1} < k!$, therefore there exists a permutation P' of K such that P' does not belong to any of the spheres of radius $k - \lambda - 1$ with center P_i, $i = 1, ..., m$. Consequently, $d(P', P) \geqslant k - \lambda$ for any $P \in \mathscr{P}$, i.e., $d(P, Q) \geqslant k - \lambda$ for $P, Q \in \mathscr{P} \cup \{P'\}$, which contradicts the maximal choice of $\mathscr{P}$ and proves the lower estimation.

Remark. The lower estimation is analogous to the estimation of Gilbert in coding theory (cf. [1]).

Remark. From the upper estimation it follows that $R(k, \leqslant\lambda) \leqslant k!/T_1(k, \lambda + 1)$. For $k - \lambda$ odd we have $T_1(k, \lambda + 1) = S_{(k-\lambda-1)/2}$. The upper estimation $R(k, \leqslant\lambda) \leqslant k!/S_{(k-\lambda-1)/2}$ is analogous to the Hamming–Rao estimation in coding theory (cf. [1]), and can be proved directly in essentially the same way. Equality in this estimation corresponds to the case of perfect codes in coding theory.

Let $\lambda^*(k)$ be any value of λ for which $|R(k, \geqslant\lambda) - R(k, \leqslant\lambda)|$ assumes its minimum.

THEOREM 5.

(i) $\lambda^*(k)/k \to \frac{1}{2}$ *for* $k \to \infty$,

(ii) $((\ln 2/2) + \epsilon(k))(k/\ln k) \geqslant |k/2 - \lambda^*(k)|$, *where* $\epsilon(k) \to 0$ *for* $k \to \infty$.

Proof. The first assertion of the theorem is an immediate consequence of the second one. The second assertion follows by easy computation using the Stirling formula and the following consequences of Theorems 3 and 4:

$$(k - \lambda)! \leqslant R(k, \geqslant\lambda) \geqslant k!/R(k, \leqslant\lambda - 1) \lesssim 2k!/e\lambda!,$$

$$\frac{(\lambda + 1)!\, e}{2} \lesssim \frac{k'}{S_{k-\lambda-1}} \leqslant R(k, \leqslant\lambda) \leqslant \frac{k!}{R(k \geqslant \lambda + 1)} \leqslant \frac{k!}{(k - \lambda - 1)!}.$$

References

1. E. R. Berlekamp, "Algebraic Coding Theory," McGraw–Hill, New York, 1968.
2. M. Deza, Matrices dont deux lignes quelconques coincident dans un nombre donné de positions communes, *J. Combinatorial Theory A* **20** (1976), 306–318.
3. P. Erdös, C. Ko, and R. Rado, Intersection theorems for sytems of finite sets, *Quart. J. Math. Oxford* **12** (1961), 313-318.
4. B. Huppert, "Endliche Gruppen," Springer–Verlag, Berlin 1967.
5. G. Katona, Intersection theorems for systems of finite sets, *Acta Math. Acad. Sci. Hungar.* **15** (1964), 329–337.
6. D. J. Kleitman, On a combinatorial conjecture of Erdös, *J. Combinatorial Theory* **1** (1966), 209–214.