Sets of properly separated permutations

R. C. Mullin[1]
Department of Combinatorics and Optimization
University of Waterloo
Waterloo Ontario N2L 3G1

D. R. Stinson[2]
Computer Science and Engineering
University of Nebraska
Lincoln NE 68588

W. D. Wallis[3]
Department of Mathematics
Southern Illinois University
Carbondale IL 62901

August 29, 1990

Abstract

Let n and k be positive integers, where $k \leq n$. Two $k-$permutations of an $n-$set, say $\mathbf{a} = (a_1 a_2 \dots a_k)$ and $\mathbf{b} = (b_1 b_2 \dots b_k)$, are said to be *properly separated* if there exist indices i and j, where $i \neq j$, such that $a_i = b_j$. Let $PS(k,n,b)$ denote a set of b $k-$permutations of an $n-$set such that any two of the $k-$permutations are properly separated. Then, define $P(k,n)$ to be the maximum value of b such that a $PS(k,n,b)$ exists. In this paper, we study the numbers $P(k,n)$.

[1]research supported by NSERC grant A3071

[2]research supported by NSERC grant A9287 and by the Center for Communication and Information Science at the University of Nebraska

[3]this author's research was supported in part by the National Security Agency under grant no. MDA904-89-H-2048. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon

CONGRESSUS NUMERANTIUM **80**(1991), pp.185-191

1 Introduction

Let n and k be positive integers, where $k \leq n$. A *k-permutation* of an n-set is an ordered list of k distinct elements of the n-set. Two k-permutations of an n-set, say $\mathbf{a} = (a_1 a_2 \dots a_k)$ and $\mathbf{b} = (b_1 b_2 \dots b_k)$, are said to be *properly separated* if there exist indices i and j, where $i \neq j$, such that $a_i = b_j$. Let $PS(k,n,b)$ denote a set of b k-permutations of an n-set such that any two of the k-permutations are properly separated. Then, define $P(k,n)$ to be the maximum value of b such that a $PS(k,n,b)$ exists.

It is clear than $P(n,n) = n!$ and $P(1,n) = 1$, for any $n \geq 1$. It is almost immediate that $P(2,n) = 3$ if $n \geq 3$.

Theorem 1.1 $P(k,n) \leq n \times P(k-1, n-1)$.

Proof: Let S be any $PS(k,n,P(k,n))$ on an n-set S. For a symbol $x \in S$, let S_x denote the k-permutations in S in which x occurs in ths first position. Clearly, there are at most $P(k-1,n-1)$ k-permutations in S_x. Letting x range over S, we see that $P(k,n) \leq n \times P(k-1,n-1)$. □

If we iterate the above inequality, we get the following corollary.

Corollary 1.1 $P(k,n) \leq 3 \times n!/(n-k+2)!$.

In the case $k = n-1$, the bound of Theorem 1.1 is exact, as we demonstrate in the following theorem.

Theorem 1.2 $P(n-1,n) = n!/2$.

Proof: $P(n-1,n) \leq n!/2$ follows from Corollary 1.1. It remains to construct a $PS(n-1,n,n!/2)$. This is done as follows. Let $S = \{1,2,\dots,n\}$, and let $\mathbf{a} = (12\dots n-1)$. For any *even* permutation π of S, let $\mathbf{a}^\pi$ be the $(n-1)$-permutation $(1^\pi 2^\pi \dots (n-1)^\pi)$. It is easy to see that any two of the resulting $(n-1)$-permutations are properly separated. □

2 The numbers P(k, n) for fixed k

In this section, we discuss the behaviour of the sequence of numbers $P(k,n)$ for fixed k. Our main result is that any such sequence is bounded above. That is, if we fix k and let n grow, eventually we reach a point where $P(k,n)$ does not change. In particular, for $k = 3$, we can show that $P(k,n) = 12$ for all $n \geq 4$.

Let S be any $PS(k,n+1,b)$ on an $(n+1)$-set S. Suppose some symbol $x \in S$ occurs in r of the k-permutations in S, where $r \leq (n-1)/(k-1)$. Then there must be some symbol y such that x and y never occur in the same k-permutation, since $1 + r(k-1) \leq n-1$. If we then replace every occurrence of y by x, we obtain a $PS(k,n,b)$. Hence, we have the following result.

Lemma 2.1 *Suppose S is a $PS(k, n+1, b)$ in which there is some symbol that occurs in at most $(n-1)/(k-1)$ of the k-permutations. Then $P(k,n) \geq b$.*

Now, we can establish our main result.

Theorem 2.1 *For any $k \geq 2$, there exist positive integers $n_0 = n_0(k)$ and p_k, such that $P(k,n) = P(k,n_0) = p_k$ for all integers $n \geq n_0$.*

Proof: The proof is by induction on k. It is clearly true for $k = 2$, so assume $k \geq 3$. Let S be any $PS(k, n+1, b)$ on an $(n+1)$-set S. For any symbol $x \in S$ and for any position j, $1 \leq j \leq k$, there can be at most $P(k-1, n)$ k-permutations $\mathbf{a} \in S$ such that $a_j = x$. So, the total number of occurrences of x is at most $k \times P(k-1,n) \leq kp_{k-1}$. Let $n = 1 + k(k-1)p_{k-1}$. Apply Lemma 2.1, to obtain $P(k,n) \geq b$. If we take $b = P(k, n+1)$, then we have that $P(k,n) = P(k, n+1)$. The argument can be repeated, replacing n by $n+1, n+2, \ldots$, yielding the desired conclusion. □

From the proof of Theorem 2.1, we have the following corollary.

Corollary 2.1 *$n_0(k) \leq 1 + k(k-1)p_{k-1}$ and $p_k \leq n_0(k)p_{k-1}$.*

It the case $k = 2$, it is easy to see that $n_0(2) = 3$ and $p_2 = 3$. In the next case, $k = 3$, matters are already considerably more difficult. Corollary 2.1 yields $n_0(3) \leq 19$ and $p_3 \leq 57$, but these bounds are not very good.

We now look more carefully at the numbers $P(3,n)$, $n \geq 3$. Of course, $P(3,3) = 6$ and $P(3,4) = 12$. It happens that there is a unique example (up to isomorphism) of a $PS(3,4,12)$. It has the alternating group A_4 as its automorphism group, so there are precisely $4!/12 = 2$ distinct examples on a specified symbol set. One of the two examples is

$$123, 134, 142, 214, 231, 243, 312, 324, 341, 413, 421, 432 \tag{1}$$

and the other example consists of the twelve 3-permutations not in (1).

Computer searches for $n = 5$, 6, and 7 yield the following results.

There are precisely two non-isomorphic examples of $PS(3,5,12)$, one using four symbols (i.e. a $PS(3,4,12)$ on four of the five symbols), and one using five symbols. A $PS(3,5,12)$ using five symbols is as follows:

$$123, 135, 152, 214, 231, 243, 312, 324, 341, 413, 421, 532 \tag{2}$$

The automorphism group of (2) is trivial, so there are 120 distinct isomorphic copies of (2) on a fixed symbol set. Hence, the total number of distinct $PS(3,5,12)$ is $120 + 2 \times \binom{5}{4} = 130$.

When we enumerate the non-isomorphic $PS(3,6,12)$, we find precisely three examples. These are (1) and (2), and the following example that uses all six symbols:

$$123, 135, 152, 214, 231, 243, 312, 326, 361, 413, 621, 532 \tag{3}$$

It can be shown that (3) has an automorphism group of order 3. Hence, we can count the distinct examples of $PS(3,6,12)$ on a specified symbol set. There are $2 \times \binom{6}{4} = 30$ copies of (1), $120 \times \binom{6}{5} = 720$ copies of (2), and $6!/3 = 240$ copies of (3), for a total of 990.

It is also interesting to observe that (2) can be obtained from (1) by "splitting" points. For example, if all occurrences of the symbol 5 in (2) are changed to 4, then (1) is produced. (3) can also be constructed from (2) in this fashion.

There are only three non-isomorphic examples of $PS(3,7,12)$, as well. The number of distinct examples on a specified symbol set can be computed to be 4270.

At this point, we might begin to suspect that $n_0(3) = 4$ and $p_3 = 12$. Proving this will be made easier by the following lemma.

Lemma 2.2 *Suppose* $P(k,n) \leq (n^2-1)/(k^2-k)$. *Then* $P(k,n_1) = P(k,n)$ *for all integers* $n_1 \geq n$.

Proof: Suppose $P(k,n) < P(k,n+1)$, and let $\mathcal{S}$ be any $PS(k,n+1,P(k,n)+1)$ on an $(n+1)-$set S. Then, there must be some symbol $x \in S$ that occurs in at most $k(P(k,n)+1)/(n+1)$ of the $k-$permutations in $\mathcal{S}$. But, we have

$$\frac{k(P(k,n)+1)}{n+1} \leq \frac{n-1}{k-1}$$

so Lemma 2.1 can be applied. This contradiction implies that $P(k,n) = P(k,n+1)$. The argument can be repeated for $n+1, n+2, \ldots$, and so the result follows. □

Suppose we can prove that $P(3,9) = 12$. Then Lemma 2.2 would tell us that $P(3,n_1) = 12$ for all integers $n_1 \geq 9$. First, we show that $P(3,9) > 12$ implies $P(3,8) > 12$, by refining the argument of Lemma 2.2.

Suppose $\mathcal{S}$ is a $PS(3,9,13)$ on a $9-$set S. Then, there must be some symbol $x \in S$ that occurs in at most four of the $3-$permutations in $\mathcal{S}$ (since $3 \times 13 < 9 \times 5$). If x occurs in at most three of the 3-permutations, then Lemma 2.1 would yield $P(3,8) > 12$. Hence, assume x occurs in exactly four 3-permutations. Since there are only three positions in which x can occur, there must be two 3-permutations in $\mathcal{S}$ in which x occurs in the same position, say **a** and **b**. Since **a** and **b** are properly separated, they must contain a common symbol other than x. It follows that x occurs with at most seven other symbols, and hence there is a symbol y with which x does not occur. Then we can replace all occurrences of y by x, thereby producing a $PS(3,8,13)$.

Next, we show that $P(3,8) > 12$ implies $P(3,7) > 12$. Suppose that $\mathcal{S}$ is a $PS(3,8,13)$ on an $8-$set S. If there exist distinct symbols $x, y \in S$ such that x and y never occur in the same 3-permutation, then we could replace all occurrences of y by x, as before, and obtain $P(3,7) > 12$. Hence, we can assume that for every pair of distinct symbols, there is a 3-permutation in which they both occur.

There must be some element x appearing in at most four 3-permutations, since $3 \times 13 < 8 \times 5$. If x appears in fewer than four 3-permutations, then there is an element y with which it does not occur. Hence, x must appear in exactly four 3-permutations. Without loss of generality, we can assume that $x = 1$, and that the 3-permutations containing 1 are permutations of the sets {1, 2, 3}, {1, 4, 5}, {1, 6, 7} and {1, 7, 8}. Now, there must be some 3-permutation **a** containing the symbols 6 and 8. But then **a** must contain at least one symbol from {1, 2, 3} and at least one symbol from {1, 4, 5}, in order that it be properly separated from the corresponding 3-permutations. It follows that **a** must be a permutation of {1, 6, 8}. But this is impossible, as we have already accounted for the four occurrences of the symbol 1.

Since we have already established that $P(3,7) = 12$, we get the following result.

Theorem 2.2 $P(3,n) = 12$ *for all integers* $n \geq 4$.

When we turn to the next case, $k = 4$, we know almost nothing. From Theorems 1.1 and 1.2, we have $P(4,5) = 60$, and $60 \leq P(4,6) \leq 72$. From Corollary 2.1, we have $n_0(4) \leq 145$ and $p_4 \leq 1740$, but these bounds are undoubtedly very poor.

3 Regular sets of permutations

A $PS(k,n,b)$ is said to be *regular* if every one of the n symbols occurs in exactly bk/n of the k-permutations. A regular $PS(k,n,b)$ is denoted $RPS(k,v,b)$, and the maximum value of b such that an $RPS(k,n,b)$ exists is denoted by $RP(k,n)$.

Certainly $RP(n,n) = n!$, and the construction of Theorem 1.2 yields a regular example, so $RP(n-1,n) = n!/2$. Up until now, we have presented no examples of $RPS(k,n,b)$ when $k < n-1$. Hence, we present a construction that gives a lower bound on the numbers $RP(k,2k-1)$.

Theorem 3.1 $RP(k,2k-1) \geq (2k-1)(k-1)!$.

Proof: Define $\mathbf{A} = \{1,2,\ldots k-1\}$. For any $j \in \mathbf{Z}_{2k-1}$, let $\mathbf{A}_j = \{i+j : i \in \mathbf{A}\}$. It is not difficult to see that $i \neq j$ implies that $i \in \mathbf{A}_j$ or $j \in \mathbf{A}_i$. Now, for any $j \in \mathbf{Z}_{2k-1}$, define the k-permutation $\mathbf{a}_j = (j, j+1, \ldots, j+k-1)$, where all entries are reduced modulo $2k-1$. Next, for any permutation ϕ of $\{2,3,\ldots,k\}$, let $\mathbf{a}_j^\phi$ denote the k-permutation $(a_1 a_{\phi(2)} \ldots a_{\phi(k)})$, where $\mathbf{a}_j = (a_1 a_2 \ldots a_k)$. The resulting set of $(2k-1)(k-1)!$ k-permutations are properly separated, and are easily seen to be regular. □

The regularity condition is a very strong one to impose, and we obtain the following necessary condition for existence.

Theorem 3.2 $RP(k,n) = 0$ *if* $n \geq k^2 - k + 2$.

Proof: Let $\mathcal{S}$ be any $RPS(k,n,b)$ on an n-set S, where $b \geq 1$. For every k-permutation $\mathbf{a} \in \mathcal{S}$, Let $A_\mathbf{a}$ denote the k-subset whose members are the symbols in **a**. Define $\mathcal{A}$ to be the family of k-subsets $\{A_\mathbf{a} : \mathbf{a} \in \mathcal{S}\}$. Then $\mathcal{A}$ is a

1–design (every point ocurs in the same number of k–subsets). Also, any two of the k–subsets in $\mathcal{A}$ intersect in at least one element. Applying a theorem of Frankl and Füredi (see [1] for a short proof), we obtain $n \leq k^2 - k + 1$. □

In the case $n = k^2 - k + 1$, we have the following.

Theorem 3.3 *$RP(k, k^2 - k + 1) = k^2 - k + 1$ if and only if there exists a projective plane of order $k - 1$.*

Proof: Let $\mathcal{S}$ be any $RPS(k, n, b)$ on an n–set S, where $b \geq 1$. Define $\mathcal{A}$ as in the proof of Theorem 3.2. The proof of the theorem of Frankl and Füredi shows that $\mathcal{A}$ must be a projective plane of order $k-1$; hence $b = k^2 - k + 1$. Conversely, suppose a projective plane of order $k - 1$ exists. Then every pair of k–subsets contain exactly one common element, and every element occurs in exactly k of the k–subsets. Clearly, what we desire is an ordering of the blocks, so that every element occurs exactly once in each position. Such a structure is called a *Youden square* and can be obtained by using well-known results on systems of distinct representatives (see, for example, [2, pp. 104-105]). □

4 Spanning sets of permutations

A $PS(k, n, b)$ is said to be *spanning* if every one of the n symbols occurs in at least one of the k–permutations. A spanning $PS(k, n, b)$ is denoted $SPS(k, n, b)$, and the maximum value of b such that an $SPS(k, n, b)$ exists is denoted by $SP(k, n)$.

From the results of Section 2, the following theorem is immediate.

Theorem 4.1 *For any $k \geq 2$, there exists a positive integer $n_1 = n_1(k)$ such that $SP(k, n) = 0$ for all integers $n \geq n_1$.*

From Section 2, we can obtain the (weak) bound $n_1(k) \leq n_0(k)p_k + 1$. Conversely, it is clear that $n_0(k) \leq n_1(k)$ and $p_k \leq P(k, n_1(k) - 1)$. Hence, it would be of interest to obtain direct proofs of good upper bounds on $n_1(k)$.

We give a construction that provides a lower bound on $n_1(k)$.

Theorem 4.2 *For any $k \geq 2$, there exists an $SPS(k, k^3 - 3k^2 + 3k + 1, k^2 - k)$.*

Proof: Place the symbol 1 in the first position of the first $k - 1$ k–permutations; in the second position of the next $k - 1$ k–permutations; etc. Next, insert symbol 2 into $k - 1$ distinct positions in the first $k - 1$ k–permutations; insert symbol 3 into $k - 1$ distinct positions in the next $k - 1$ k–permutations; etc. Finally, fill out all remaining positions with distinct symbols. The total number of symbols used is $1 + k + k(k-1)(k-2) = k^3 - 3k^2 + 3k + 1$, and the resulting set of k–permutations is easily seen to be properly separated. □

Example 4.1 *An* $SPS(4,27,12)$

1	2	6	7
1	8	2	9
1	10	11	2
12	1	3	13
14	1	15	3
3	1	16	17
18	19	1	4
4	20	1	21
22	4	1	23
5	24	25	1
26	5	27	1
28	29	5	1

5 Summary

The problem of constructing properly separated sets of $k-$permutations seems to be a very difficult one. We mention several open questions.

1. Compute $P(4,6)$.
2. Determine $n_0(4)$ and p_4.
3. Determine the asymptotic behaviour of p_k. Is it true that p_k is $O(k^k)$?
4. Find *any* example of a $PS(k,n,b)$ with $k < n$ and $b > (k+1)!/2$.
5. Find improved bounds on the numbers $P(n-2,n)$.
6. Prove good bounds on $n_1(k)$. In particular, determine if $n_1(k) \leq k^3$.

References

[1] A. R. Calderbank. Symmetric designs as the solution of an extremal problem in combinatorial set theory. *European Journal of Combinatorics*, 8:171–173, 1987.

[2] D. Raghavarao. *Constructions and Combinatorial Problems in Design of Experiments.* John Wiley & Sons, New York, 1971.