INFORMATION AND CONTROL 43, 1–19 (1979)

Coding with Permutations

IAN F. BLAKE

Department of Electrical Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

GÉRARD COHEN

ENST, 46 rue Barrault, 75013, Paris, France

AND

MIKHAIL DEZA

3 rue Duras, 75008, Paris, France

I. INTRODUCTION

Much interest has recently been shown in permutation arrays in both their mathematical and engineering settings. They have the following definition:

DEFINITION. A permutation array (PA) of degree r and size v is a set of v permutations on a set Ω, $|\Omega| = r$ (thought of as v orderings of the r elements), with the property that any two distinct permutations agree in at most λ positions. It will be denoted by $A(r, \leqslant\lambda; v)$. As an example a Latin square, or any cyclic set of permutations, is an $A(r, \leqslant 0; r)$.

Other types of PAs have also been considered; those with the property that any two distinct permutations agree in exactly λ positions, called equidistant PAs and denoted by $A(r, \lambda; v)$ and those with the property that any two distinct permutations agree in at least λ positions denoted by $A(r, \geqslant \lambda; v)$. These two types will not be considered here.

A considerable amount of information is now known about such arrays and they have received the attention of combinatorial theorists, group theorists, and engineers, among others. Because of the diversity of the background of those interested in these structures, the research results on PAs have appeared widely scattered in the literature. This has tended to hamper further progress in the area and has led to some overlap of work. The main purpose of this paper is to briefly present the most important of these results in a unified setting to assess their significance and to lay a basis for further work. In addition some new

0019-9958/79/100001-19$02.00/0

results of the authors are proved and some interesting open problems of both a mathematical and engineering nature are discussed.

II. Bounds for the Permutation Arrays $A(r, \leqslant \lambda; v)$

Denote by $R(r, \leqslant \lambda)$ the maximum value of v such that an $A(r, \leqslant \lambda; v)$ exists. By arranging those rows with a given element in a given position it is seen that

$$R(r, \leqslant \lambda) \leqslant rR(r-1, \leqslant (\lambda-1))$$

and, iterating the argument,

$$R(r, \leqslant \lambda) \leqslant \frac{r!}{(r-\lambda)!} R(r-\lambda, \leqslant 0).$$

Since $R(r-\lambda, \leqslant 0) = r-\lambda$, as the existence of an $A(r, \leqslant 0; r)$ is equivalent to the existence of a Latin square of order r which exist for all positive integers r, it follows that

$$R(r, \leqslant \lambda) \leqslant \frac{r!}{(r-\lambda-1)!}.$$

More sophisticated bounds can be obtained (Deza and Vanstone, 1977; Deza and Frankl, 1977). Let D_i be the number of disorders on i elements (i.e., the number of permutations leaving no element fixed):

$$D_i = i!\left(\sum_{j=0}^{i} \frac{(-1)^j}{j!}\right).$$

Let S_k be the number of permutations at a (Hamming) distance k or less from a given permutation:

$$S_k = \sum_{j=0}^{k} D_j \binom{r}{j} = 1 + \sum_{j=2}^{k} D_j \binom{r}{j}.$$

The quantity S_k is the volume of a sphere of radius k in a permutation space. Define further the function

$$T_1(r, \lambda) = \sum_{i=0}^{(r-\lambda)/2} \binom{r}{i} D_i \qquad r-\lambda \text{ even}$$

$$= \sum_{i=0}^{(r-\lambda-1)/2} \binom{r}{i} D_i + \binom{r-1}{(r-\lambda-1)/2} D_{(r-\lambda-1)/2} \qquad r-\lambda \text{ odd}$$

and note that $T_1(r, \lambda) = S_{(r-\lambda)/2}$ in the case of $r-\lambda$ even.

The following bound can be shown (Deza and Frankl, 1977, Theorem 4):

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

The lower bound is a direct analog of the Gilbert bound in coding theory. When $T_1(r, \lambda+1) > (r-\lambda-1)!$ and $(r-\lambda-1)$ is even, the upper bound becomes $r!/S_{(r-\lambda-1)/2}$, which is a direct analog of the Hamming–Rao bound of coding. Because of this analogy we have the following:

DEFINITION. The PA $A(r, \leqslant\lambda; v)$ is called *perfect* if $v = r!/T_1(r, \lambda+1)$. The following definition is motivated by the notion of sharply transitive groups, considered in Section IV.

DEFINITION. The PA $A(r, \leqslant\lambda; v)$ is called *sharp* if $v = R(r, \leqslant\lambda) = r!/(r-\lambda-1)!$.

Perfect and sharp PAs are discussed in the following two sections.

III. Perfect Permutation Arrays

In order for a perfect PA to exist it is necessary that $T_1(r, \lambda+1) > (r-\lambda-1)!$. It is easy to show that

(i) $T_1(r, \lambda) > (r-\lambda)!$ for $r \geqslant r_0(r-\lambda)$,

(ii) $T_1(r, \lambda) < (r-\lambda)!$ for $r \geqslant r_1(\lambda)$

for some functions r_0 and r_1, and that for $r-\lambda = 4$, $r_0 = 8$ and for $r-\lambda = 6$, $r_0 = 14$. Very little else is known about the behavior of these functions. However, for the case of $r-\lambda = 5$, corresponding to a two-error correcting code, if a perfect array exists then

(i) $S_2 = T_1(r, \lambda+1) > 4!$,

(ii) $r!/S_2$ is an integer.

It can be shown that the only possible values for r, $r \leqslant 20$, satisfying these two conditions are 11 and 18. Interestingly, for $r = 11$ and $\lambda = 6$, $11!/S_2 = |M_{11}| \cdot 90$, where M_{11} is the Mathieu group of degree 11. The existence of this perfect PA, or any nontrivial perfect PA, remains an interesting open problem.

IV. Sharp Permutation Arrays

A λ-transitive permutation group on a set of elements Ω, $|\Omega| = r$, is one for which there exists at least one permutation taking any ordered λ-set of distinct

elements of Ω into any other ordered λ-set of distinct elements. If, for any two λ-sets there exists exactly one such permutation, then the group is called sharply λ-transitive and its order must necessarily be $r!/(r-\lambda)!$. In a sharply λ-transitive group, every nonidentity element moves at least $(r-\lambda+1)$ elements and hence the group is an $A(r, \leqslant\lambda-1; r!/(r-\lambda)!)$. We will call any PA $A(r, \leqslant\lambda-1; v)$ for which $v = r!/(r-\lambda)!$, a sharp PA, regardless of whether or not it was generated by a group. If it is generated by a group it will be denoted by $A^*(r, \leqslant\lambda; v)$. For the remainder of the section we will consider what is known about sharp PAs, group or otherwise.

If a sharp PA $A(r, \leqslant\lambda; v)$ exists then $T_1(r, \lambda) < (r-\lambda)!$ and a sharp PA $A(r-1, \leqslant\lambda-1; v')$ exists. All sharply λ-transitive permutation groups are known for $\lambda \geqslant 2$ and, we enumerate the possibilities (Nagao, 1967; Gorenstein and Hughes, 1961):

$\lambda = 2$ The group of linear transformations $x \to ax + b$ on a finite near field

$\lambda = 3$ The group of transformations $x \to (a \cdot x + b)/(c \cdot x + d)$ where $+$ and $\div$ are those of a finite field and $\cdot$ is either the field multiplication or proper near-field multiplication

$\lambda = 4$ The Mathieu group M_{11}

$\lambda = 5$ The Mathieu group M_{12}

The only other sharply transitive groups are S_r, which is sharply r and $(r-1)$-transitive, and A_r which is sharply $(r-1)$-transitive.

Not all known sharp PAs arise from groups. Pedrini (1966) has constructed a sharply 3-transitive array, which is not a group. On infinite $(r = \infty)$ sets there exist λ-transitive sets for any λ(Heise–Sorensen) but on such sets there exist sharply λ-transitive groups only for $\lambda = 2$ or 3.

For the remainder of the section some properties and characterizations of sharply λ-transitive sets are examined. In analogy with sharply λ-transitive groups we have the following:

DEFINITION. Let A be a set of permutations on the set Ω. Then A is called sharply λ-transitive iff for every ordered pair of λ-subsets of Ω, $(a_1, a_2, \ldots, a_\lambda)$ and $(b_1, b_2, \ldots, b_\lambda)$, there is a unique element of A such that $a_i g = b_i$, $i = 1, 2, \ldots, \lambda$.

The following proposition shows the equivalence of the notions of sharpness and sharp λ-transitivity.

PROPOSITION 1. *The* PA $A(r, \leqslant\lambda-1; v)$ *A is sharp iff it is sharply λ-transitive.*

Proof. First suppose that A is sharp and let $(a_1, a_2, \ldots, a_\lambda)$ and $(b_1, b_2, \ldots, b_\lambda)$ be two λ-subsets of Ω. If $G = S_n$, the symmetric group on n letters, let $G_0 =$

$\{g \in G \mid a_i g = a_i,\ i = 1,\ldots,\lambda\}$, the stabilizer of the first λ-subset. Since A is a sharp PA $A(r; \lambda - 1; v)$ it follows that distinct elements of A must lie in distinct cosets of G_0. Since A is sharp it must form a complete set of coset representatives of G_0 in G. Thus there is a unique $g \in A$ such that $a_i g = b_i$, $i = 1, 2,\ldots, \lambda$. The converse is trivial.

PROPOSITION 2. *$A^* = A^*(r, \leqslant 1; v)$ is a sharply 2-transitive group of degree r iff $v > (r-1)^2$.*

Proof. For an element $a \in \Omega$ define $A_a^* = \{g \in A^* \mid ag = a\}$. Then A_a^* is a subgroup of A^* and A^* is transitive iff $|A^* : A_a^*| = r$. Now if $s = |A^* : A_a^*|$ then s is the size of the orbit of a under the action of A^* and it follows that $s \leqslant r$. Also, since A^* is an $A(r, \leqslant 1; v)$, $A_{ab}^* = \{g \in A^* \mid ag = a, bg = b\} = 1$, for all $b \neq a$. Using the same argument again gives $|A_a^* : A_{ab}^*| \leqslant r - 1$ and so $|A_a^*| \leqslant r - 1$. Thus $(r-1)^2 < |A^*| = |A^* : A_a^*|\,|A_a^*| \leqslant s(r-1)$ and so $s > (r-1)$ implying that $s = r$, and hence that A^* is transitive. From Passman (1967, Sect. 8) it follows that A^* is a Frobenius group and so $|A^*| = |A_a^*| \cdot r$ and $|A_a^*| \mid (r-1)$. Thus

$$|A_a^*| = |A^*|/r > \frac{(r-1)^2}{r} \geqslant \frac{r-1}{2} \qquad \text{for } r \geqslant 2,$$

implying that $|A^*| = |A_a^*|\, r = (r-1)r$, which completes the argument. Again the converse is trivial.

Minkowski-m-structures were defined in Heise (1972). Implicit among the results of that paper is the following:

PROPOSITION 3. *A Minkowski-m-structure of order $(r - m)$ exists iff a sharply $(m+2)$-transitive set of Ω exists.*

A Minkowski-0-structure is just an affine plane and a Minkowski-1-structure is called a Minkowski plane. Since finite projective and affine planes coexist proposition 3 immediately yields the following proposition for which an alternate, more direct, proof is provided.

PROPOSITION 4. *A projective plane $PG(2, r)$ exists iff there exists a sharply 2-transitive set on Ω.*

Proof. Consider the $r(r-1)\,xr$ set with the permutations as rows, assumed sharply 2-transitive. Each of the r elements of Ω must appear $(r-1)$ times in each column or the set would not be sharply 2-transitive. Divide the array into r blocks of $(r-1)$ rows each such that the first column of the ith block contains all i's. All ordered $r(r-1)$ pairs of the form (a, b), $a, b \in \Omega$, $a \neq b$ appear exactly once in any ordered pair of columns. For each i, augment the ith block of the array by adding a row of all i's to form an $r^2 \times r$ array. Each of the r^2

ordered pairs of Ω now appears once in any choice of two columns. Discard the first column and form $(r-1)$ $r \times r$ subarrays by using the jth column of the ith block as the ith column in the jth subarray, $j = 1, 2, \ldots, r$. By construction these subarrays form a complete set of orthogonal Latin squares of order r. From Hall (1967, Chap. 12) this is equivalent to a projective plane of order r which completes the theorem.

The equivalence between a Minkowski-m-structure of finite order n and a sharply λ-transitive set with $\lambda = m + 2$ and $r = m + n$ follows from this proposition.

It has been observed that sharp PAs $A(r, \leqslant 0; v)$ are not always groups. The Klein 4-group gives an example of a noncyclic sharp $A^*(4, \leqslant 0; 4)$. Similarly sharp $A(r, \leqslant 1; v)$ are not necessarily groups as there exist projectives planes which are not over a near field. However, the existence of nongroup sharp $A(r, \leqslant 2; v)$ is known to be impossible for r odd and it is an open question for r even. For $\lambda \geqslant 3$ all the sharp $A^*(r, \leqslant \lambda; v)$ have been enumerated in Section IV.

DEFINITION. A set of permutations on Ω, Ω not necessarily finite, is *symmetric* if for any $a, b \in A$ the existence of $x \in \Omega$ such that $a(x) \neq b(x)$ and $a^{-1}b(x) = b^{-1}a(x)$ implies $a^{-1}b = b^{-1}a$.

It is known that any $A(r, \leqslant 2; v)$, r finite and odd, is symmetric. The following proposition indicates the strength of the symmetric assumption.

PROPOSITION 5 (Karzel, 1978). *Any sharp 3-transitive symmetric* PA, $A(r, \geqslant 2; v)$ *containing the identity*, $3 \leqslant r \leqslant \infty$, *is a group.*

Other aspects of this problem are considered in Heise (1976) and Quattrocchi (1975).

To conclude the section, the known results on the existence of sharp PAs for $r \leqslant 12$, $\lambda \leqslant 4$, are summarized:

(i) No such array exists for $(r, \lambda) = (6, 1), (7, 2), (7, 3), (8, 3), (9, 3), (10, 3), (8, 4), (9, 4), (10, 4)$;

(ii) the question is open for $(v, \lambda) = (10, 1), (12, 1), (11, 2), (12, 3), (11, 4)$;

(iii) as established otherwise for groups.

For $\lambda = 1$ it is known from Deza and Vanstone (1977) that $R(6, \leqslant 1) = 18$, $R(10, \leqslant 1) \geqslant 32$, and $R(12, \leqslant 1) \geqslant 24$.

V. PERMUTATION GROUPS

Many of the problems considered by group theorists working on permutation groups are of interest from a permutation array perspective. Some of the most

relevant work will be reviewed in Sections VI and VII, while the present section gives the background and notation required.

The *degree* of the permutation group G acting on the set Ω is the number of points of Ω actually moved by G. The degree of an element $g \in G$ is the number of points actually moved by g. The smallest of these degrees over the non-identity elements of the group is called the *minimal degree* of the group, which will be denoted by d. A permutation group G of degree n and minimal degree d is an $A(n, \leqslant(n-d); \mid G \mid)$.

The notions of t-transitive and sharply t-transitive permutation groups were defined in the previous section, and, in the following two sections, groups which are t-transitive but not sharply t-transitive are considered.

Denote by G_a the subgroup $\{g \mid a \cdot g = a, g \in G\}$, the stabilizer subgroup of the point a. Similarly for $\Delta \subset \Omega$ the subgroup $G_\Delta = \{g \mid g \cdot \beta = \beta, \forall \beta \in \Delta, g \in G\}$ is called the stabilizer of Δ. The group G is called semiregular if $G_\alpha = 1$ $\forall \alpha \in \Omega$. It is called *regular* if it is semiregular and transitive.

A *Frobenius* group of degree n is a transitive group which has minimal degree $(n-1)$. Clearly, in such a group, the stabilizer of any two points is the identity. A permutation group is called a *Zassenhaus* group if it is doubly transitive, the stabilizer of any three points is the identity and if it has no regular normal subgroup. The classification of all such groups is known (Nagao, 1967). Note that the stabilizer of a single point, in a Zassenhaus group, is a *Frobenius* group.

VI. The Minimal Degree of a Permutation Group

Determining the minimal degree of a permutation group was a problem of interest to group theorists of the earlier part of this century. The problem continues to be worked on and in this section some known results on it are surveyed. Its direct interpretation as the minimum distance of the permutation code makes it important for our purposes. Perhaps the most fundamental result is the theorem (Wielandt, 1964) attributed to Manning.

Theorem. *Let G be a t-transitive group, neither alternating nor symmetric. Let n be its degree and d its minimal degree. Then, n, d, and t satisfy the following relationships:*

$t \geqslant$	2	3	4	5	6	8	25
$d \geqslant$	$\dfrac{(n-2(n^{1/2}))}{3}$	$\dfrac{n}{3}-1$	$\dfrac{n-1}{2}$	$\dfrac{n}{2}$	$\dfrac{3n}{5}$	$\dfrac{2n}{3}$	$\dfrac{25n}{31}$

Another result, due to Jordan and quoted in Wielandt (1964), states that if G is a primitive group with minimal degree $d > 3$, then

$$n < \frac{d^2}{4}\log\left(\frac{d}{2}\right) + d\left(\log\left(\frac{d}{2}\right) + \frac{3}{2}\right).$$

Table I summarizes what is known on the problem for $d \leqslant 15$, deduced from the works of Jordan and Manning.

Carmichael (1956) states that $d \geqslant 2t - 2$ if $3 \leqslant t \leqslant n - 3$ for any t-transitive group. It has already been observed that $d \leqslant n - t + 1$ with equality iff G is sharply t-transitive and that $|G| \cdot (d - 1)! \leqslant n!$ with equality iff G is sharply $(n - d + 1)$-transitive.

TABLE I

Jordan's Results on Primitive Groups with $d \leqslant 15$ and Mathieu Groups M_{22}, M_{23}, M_{24}

d	n	t	$\lvert G \rvert$	Number of different groups	
1				0	
2				∞	
3				∞	
4				6	
5				1	
6				14	
7				3	
8				18	(including M_{11} and M_{12})
9				0	(Herzog and Prager, 1976, p. 43)
10				7	
11				25	
12	$\leqslant 18$				
	25			1	
	27			2	
	28	2		1	
	35			1	
13				1	
14	9	1		1	
	49	1	$2(7!)^2$	1	
	22	3	$22 \cdot 21 \cdot 20 \cdot 96$	1	
	21	2	$21 \cdot 20 \cdot 96$	1	
	21	2	$21 \cdot 20 \cdot 288$	1	
15	16	1	80	1	
	16	2	240	1	
	17	3	4080	1	
	21	1	2520	1	
	21	2	$21 \cdot 20 \cdot 144$	1	
	25	1	7200	1	
	25	1	14400	2	
16	22	3	$22 \cdot 21 \cdot 20 \cdot 48$	1	M_{22}
	23	4	$23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$	1	M_{23}
	24	5	$24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$	1	M_{24}

Enough is now known about the problem that we can make the following two attempts at classification. In the first we characterize t-transitive groups for which $d = n - t$, $t = 1, 2, 3, 4$.

(i) $t = 1$, $d = n - 1$. G is a Frobenius group.

(ii) $t = 2$, $d = n - 2$. G is a Zassenhaus group.

(iii) $t = 3$, $d = n - 3$. G is either (Gorenstein and Hughes, 1961):

(a) S_4, S_5, A_6 or M_{11} (i.e., sharply 4-transitive).

(b) The linear fractional group over $GF(q)$ or the group of fractional transformations

$$x \mapsto \frac{(ax^{\sigma(\Delta)} + b)}{(cx^{\sigma(\Delta)} + d)}$$

over $GF(q^2)$, q odd, where $\sigma(\Delta)$: $x \mapsto x^q$ if Δ is a nonsquare in $GF(q^2)$ and the identity map otherwise. (These groups are sharply 3-transitive.)

(c) The full semilinear fractional group:

$$x \mapsto \frac{(ax^\alpha + b)}{(cx^\alpha + d)}, \qquad ab - bc \neq 0,$$

over $GF(q^2)$, q a prime and α an automorphism of $GF(q^2)$.

(iv) $t = 4$, $d = n - 4$. G is sharply 5-transitive (A_7, S_6 or M_{12}).

(v) $t \geqslant 5$, $d = n - t$. G is A_{t+2} or S_{t+1}.

A slightly different approach to characterization classiffication, due to several different authors is contained in the following statement:

Let G be a permutation group which forms an $A^*(r, \leqslant \lambda - 1; |G|)$ and is $(\lambda - 1)$-transitive but not sharply λ or $(\lambda - 1)$-transitive. Then $\lambda \leqslant 5$,

$$\frac{r!}{(r - \lambda + 1)!} < |G| < \frac{r!}{(r - \lambda)!}$$

and one of the following three cases hold:

(i) $\lambda = 4$. In this case $G = PTL(2, 2^p)$, p prime, $r = 2^p + 1$ and $|G| = r(r - 1)(r - 2)\log_2(r - 1)$.

(ii) $\lambda = 3$. There are three possibilities:

(a) G contains a normal subgroup of order r, in which case $r = 2^a$, $G \cong TA(2^a)$ and $|G| = r(r - 1)\log_2(r)$.

(b) $r = p^a + 1$, in which case $G = PSL(2, p)$ G is simple and $|G| = \frac{1}{2}r(r - 1)(r - 2)$.

(c) $r = q^2 + 1$, $q = 2^a$, a odd, in which case $G \cong Sz(q)$, G is simple and $|G| = r(r - 1)((r - 1)^{1/2} - 1)$ (Tsuzuki, 1967).

(iii) $\lambda = 2$, in which case G is a Frobenius group. The classification of these is equivalent to the classification of all near fields.

A result related to the above, shown in Yoshizawa (1977), states that if G is a 4-transitive group with the property that the stabilizer of any four points is a Frobenius group then G is either S_7, S_8, or M_{23}. Herzog and Praeger (1976) have also investigated the problem of the minimal degree of a group and have obtained interesting results which we will not discuss here.

To conclude the section we state several results relating to the average number of points left fixed by a permutation. First, suppose G is a transitive permutation group and let $\theta(g)$, $g \in G$ be the number of points left fixed by g. It is then a simple matter to show that

$$\sum_{g \in G} \theta(g) = |G|.$$

Each permutation in such a group leaves, on the average, one point fixed. If the group has k orbits then (Wielandt, 1964) each element leaves, on the average, k points fixed. Merris and Pierce show that

$$\sum_{g \in G} (\theta(g))^r \geqslant X_r |G|,$$

where X_r is the rth Bell number which satisfies the recurrence relation

$$X_{r+1} = \sum_{k=0}^{r} \binom{r}{k} X_{r-k}.$$

Equality takes place iff G is r-transitive.

VII. Groups with a Specified Distance Enumerator

Recently several papers have appeared where, in our terminology, groups with a given distance enumerator are classified. This is considerably more information than the minimal degree of the group considered in the previous section, and the characterizations tend to be involved.

Let $f(g)$ be the number of points fixed by $g \in G$, a subgroup of S_r, and suppose that $\{f(g), g \in G, g \neq 1\} \subseteq L$, where L is a subset of $\{0, 1, \ldots, r\}$. We call the group G of type L and denote it by $A^*(L, r, m)$, $m = |A^*|$. Bannai *et al.* (1978) have conjectured

$$|A^*(L, r)| \leqslant \prod_{l_i \in L} (r - l_i)$$

and if equality is achieved the array is called sharp. It has recently been shown by Kiyota (1978) that

$$|A^*(L, r)| \Big| \sum_{l_i \in L} (r - l_i).$$

The method of proof used the generalized character

$$\hat{\theta} = \prod_{l_i \in L} (\theta - l_i \cdot 1_G),$$

where 1_G is the identity character on G and $\theta(g) = \gamma(g)$, the permutation character on G. It can be shown that θ is actually a Z-linear sum of irreducible characters of G and that the usual inner product of $\hat{\theta}$ with 1_G over G is

$$(\hat{\theta}, 1_G)_G = \Big(\sum_{g \in G} \hat{\theta}(g)\Big)\Big/|G| = \hat{\theta}(1)/|G| = \prod_{l_i \in L} (r - l_i)/|G|.$$

Denote by $R^*(L, r)$ the maximum size of the group $A^*(L, r)$. When a sharp array $A^*(L, r)$ exists, $R^*(L, r) = \prod_{l_i \in L} (r - l_i)$.

In particular, sharp arrays $A^*(L, r)$ are classified by Ito and Kiyota (1979) when L is of the form

(i) $L = \{l_1, l_1 + 1, l_1 + 2, \ldots, l_1 + l_2 - 1\}$, $l_1 \geqslant 0$, $1 \leqslant l_2 \leqslant r - l_1$, and

(ii) $L = \{l_1, l_1 + l_2\}$, $l_1 \geqslant 0$, $1 \leqslant l_2 \leqslant 3$,

and we consider some special subcases:

1. $R^*(\{l, l + 2\}, r) = (r - l)(r - l - 2)$ iff $r - l = 4, 6, 8$ or 14. The case $l = 0$ was considered by Tsuzuki (1967), who also showed that $A^*(\{0, 1, 3\}, r, m)$ exists iff $r = 7, 9$ or 15.

2. $R^*(\{l_1, l_1 + 1, l_1 + 2, \ldots, l_1 + l_2 - 1\}, r) = \prod_{i=l_1}^{l_1+l_2-1} (r - i)$ iff one of the following cases holds:

(a) $l_2 = r - l_1, r - l_1 - 1, r - l_1 - 2$ or 1.

(b) $l_2 = 2, r = p^a$ or $l_2 = 3, r = p^a + 1$.

(c) $l_2 = 4, r = 11$ or $l_2 = 5, r = 12$.

2′. The case $l_1 = 0$ is exactly the case of a sharply l_2-transitive group.

2″. The case $l_2 = r - l_1$ gives

$$R^*(\{l, l + 1, l + 2, \ldots, r - 1\}, r) = (r - l)!$$

for any r and l. This interesting result is an analog of the theorem of Erdos, Ko, and Rado which states that for any family $\{A_i\}$ of r-subsets of a given v-set, with $|A_i \cap A_j| \geqslant l$ and $v > v_0(r)$ holds, where $v_0(r)$ is some function of r only,

then $|\{A_i\}| = \binom{v-l}{r-l}$. In Deza and Frankl (1977) the exact value of $R(\{l, l+1,\ldots, r-1\}, r)$ (i.e., the nongroup case) was found for $r > r_0(r-l)$, where $r_0(r-l)$ is some fixed function of $r-l$. It was also conjectured that

$$R(\{l, l+1,\ldots, r-1\}, r) = (r-l)! = R^*(\{l, l+1,\ldots, r-1\}, r)$$

for $r > r_0(l)$. It is known, for example, that $R(\{2, 3, 4, 5\}, 6) = (6-2)! = 24$. It is also known that $A^*(\{1, 2,\ldots, r-1\}, r; (r-1)!)$ is the unique sharp group array for $L = \{1, 2,\ldots, r-1\} - \{l\}$.

$2'''$. The case $l_2 = 1$ gives $R^*(\{l\}, r) = r - l$ for any r, l. Note in particular that $R^*(\{0\}, r) = r = R(\{0\}, r)$ (the Latin square case) and $R(\{1\}, r) \geqslant 2r - 4 > r - 1 = R^*(\{1\}, r)$ for $r > 5$ (a result of Heinrich and van Rees). Vanstone showed that

$$R(r, \lambda) \leqslant 2 + \left\lfloor \frac{\lambda}{\lceil (r-\lambda)/3 \rceil} \right\rfloor$$

and equality is achieved when $\lambda > (r-\lambda)^3/3$. It is possible to show from Iwahori (1964) that any sharp $A^*(\{l\}, r, m)$ with $l < 3$ has l fixed points with the exception of the case $l = 2$ and r even.

A few other results are known on this problem. For example, Frobenius groups are of type (0, 1) and Zassenhaus groups are of type (0, 1, 2). Iwahori (1964) classified all type 2 groups and Iwahori and Kondo (1965) extended this work to type 3 groups. The more general notion of type L groups appears to have been first considered in Pretzel and Schleiermacher (1975b). Type (0, 3) groups were studied in Pretzel and Schleiermacher (1975a), where a restricted characterization of them is given. Other papers, with limited results, deal with characterizing type (0, 2) and type $(0, p)$ groups, where p is a prime.

VIII. Distance Enumeration of Permutation Codes

The previous two sections indicate that the problem of distance enumeration of permutation codes is interesting, much as the case for algebraic codes over finite fields. The problem appears very difficult and, apart from the few results already mentioned, there has been little done on the problem. Section VI considered the determination of the minimum distance of a group or code, or groups for which the minimal distance could be determined. In the previous section, groups which had a specified distance enumerator were examined. In this section a set of equations, given in Carmichael (1956), are derived which in certain cases give the distance distribution of the group.

Let G be a t-transitive group of degree n. The order of G is of the form $(n!/(n-t)!)m$, where m is the order of a stabilizer of a t-set. It is also the number of permutations taking a given t-set to another ordered t-set. Let x_i be the

number of permutations of the group fixing precisely i points. Determining the x_i is equivalent to determining the distance enumerator of the code. Clearly, we have

$$x_0 + x_1 + \cdots + x_n = |G|.$$

If the group is transitive then $|G| = n|G_1|$. Now enumerate in two ways the permutations. Each point is left fixed by $|G_1|$ permutations. A permutation leaving i points fixed contributes i to the count giving

$$1 \cdot x_1 + 2 \cdot x_2 + \cdots + n \cdot x_n = n \cdot |G_1| = |G|.$$

Extending the argument, suppose G is a 2-transitive group and enumerate on the number of ordered 2-sets left fixed. There are $n(n-1)$ ordered 2-sets and each of these is left fixed by m permutations where $|G| = n(n-1)m$. A permutation fixing i points contributes $i(i-1)$ to the count and so

$$\sum_{i=2}^{n} i(i-1)x_i = n(n-1)m = |G|.$$

Since a 2-transitive set is also transitive, the previous two equations hold for such a group. By extending the argument, for a t-transitive group

$$\sum_{i=j}^{n} i(i-1)\cdots(i-j+1)x_i = |G|, \qquad j = 1, 2, \ldots, t,$$

$$\sum_{i=0}^{n} x_i = |G|,$$

and this is a set of $(t+1)$ equations in the n unknowns $x_0, x_1, \ldots, x_{n-1}, (x_n = 1)$. For sharply t-transitive groups $x_i = 0$ for $i \geqslant (t+1)$ and, in this case, there is a unique solution for x_i, $0 \leqslant i \leqslant t$.

These equations are very reminiscent of the equations for the intersection numbers of t-designs. They also bear a resemblance to the MacWilliams identities in the case that d' (the dual distance) is at least as great as the number of nonzero weights s of the code. It is clear, however, that more tools are needed for the determination of distance enumerators of many permutation groups of interest.

IX. Decoding Permutation Codes

Several authors have considered the problem of decoding PAs, viewed as codes with the Hamming metric. As the distance between any two codewords of the PA $A(r, \leqslant\lambda; v)$ is at least $r - \lambda$, as a code it is capable of correcting $[(r - \lambda - 1)/2]$ errors. Decoding algorithms for sharply 2- and 3-transitive

groups were given in Blake (1974) and Cohen and Deza (1977), respectively. The latter reference also considered decoding M_{11} and M_{12}, and the method of decoding M_{12} will be described at the end of this section.

To begin with we describe a "basic" decoding algorithm for any PA, analogous in many ways to the standard array decoding technique of algebraic coding, due to Schellenberg and Vanstone (1976). A generalized Room square $S(r, \leqslant\lambda; v)$ is an $r \times r$ array of cells with the properties:

(a) Every cell contains a (possibly empty) subset of permutations of $A(r, \leqslant\lambda; v)$.

(b) Every permutation is contained in exactly one cell of each row and each column of the array.

(c) Every unordered pair of permutations of A is contained in at most λ cells.

The existence of $S(r, \leqslant\lambda; v)$ is equivalent to the existence of $A(r, \leqslant\lambda; v)$, as is easily demonstrated by the set of maps:

$$\begin{aligned} \sigma\colon V &\to V, \qquad \sigma \in A(r, \leqslant\lambda; v), \\ j &\to i, \qquad \text{iff } \sigma \text{ is in cell}(i, j) \text{ of } S(r, \leqslant\lambda; v), \end{aligned}$$

where $V = \{1, 2,..., v\}$, the set on which A is defined, and given either A or S, the other is easily constructed using these maps.

To use the generalized Room square for decoding, suppose that the received word is $(a_1, a_2,..., a_r)$, $a_i \in V$. If no errors were made in transmission and the received word corresponds to $\sigma \in A(r, \leqslant\lambda; v)$ then cells $(a_1, 1), (a_2, 2),...,$ (a_r, r) of S all contain σ, since $\sigma(j) = a_j$, $j = 1, 2,..., r$.

If $e \leqslant \lfloor (r - \lambda - 1)/2 \rfloor$ errors have been made in transmission then at least $(r - e)$ of the correspondences $\sigma_k(j) = a_j$, $j = 1, 2,..., r$, will be correct and so at least $(r - e)$ of the cells (a_j, j) of S will contain σ. Furthermore if $\eta \in A$ was contained in more than $r - \lfloor (r - \lambda - 1)/2 \rfloor$ of these cells then σ and η under the stated conditions would be closer than $r - \lambda$, which gives a contradiction. Consequently the decoding algorithm for the received word $(a_1, a_2,..., a_r)$ is to search the cells $(a_1, 1), (a_2, 2),..., (a_r, r)$ for the unique permutation contained in at least $r - \lfloor (r - \lambda - 1)/2 \rfloor$ cells. The permutation σ is the transmitted codeword.

The decoding algorithm is simple and general but the number of computations becomes prohibitive as $|G|$ becomes large. The generalized Room square contains $r|G|$ permutations and each cell, on the average, contains $|G|/r$ permutations. Decoding thus requires a search among r sets of $|G|/r$ permutations, on the average, to find the most frequently occurring permutations.

Another interesting decoding method proposed in Vanstone (1978) first converts the q-ary code (not even necessarily a permutation array) to a binary code which is majority logic decodable. Let the words of the (n, k, d) q-ary code C

($|C| = k$), be written as a $k \times n$ array A. A $k \times nq$ array B is constructed as follows: let $i = rq + s$, $0 \leqslant r \leqslant n-1$, $0 \leqslant s < q-1$. Then the ith column of the array B has a "1" in all positions where the column $(r+1)$ of A has the symbol $s-1$. It is straightforward to verify that the array B is an $(nq, k, 2d)$ binary code which is majority logic decodable. The following example illustrates the procedure.

EXAMPLE. Consider the 4-ary (4, 3, 3) code

$$A = \begin{pmatrix} 0 & 2 & 2 & 3 \\ 1 & 2 & 3 & 1 \\ 2 & 0 & 2 & 1 \end{pmatrix}$$

and, using the above procedure, construct the array

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

which is a (16, 3, 6) binary code. Suppose that (2 0 3 1) is received. Then from B take the columns $0 \cdot q + (2+1)$, $1 \cdot q + (0+1)$, $2 \cdot q + (3+1)$ and $3 \cdot q + (1+1)$ where $q = 4$, to form the binary array S,

$$S = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

(In the general case if $(x_1, x_2, \ldots, x_n)$ is received, take the columns $(i-1) \cdot q + (x_i + 1)$, $1 \leqslant i \leqslant n$.) The only row of S containing more 1's than 0's is the third, implying that the third row of A (2 0 2 1) is the correct codeword.

To conclude the section a brief description of the method proposed in Cohen and Deza (1977) to decode the Mathieu group M_{12}, which is a (12, 95040, 8) code is given. Let E be the set of 132 codewords of weight 6 in the $(12, 3^6, 6)$ ternary Golay code. It is known that the action of M_{12} on the coordinate positions of these codewords is to permute them among themselves and M_{12} is the largest group which fixes E. Now suppose that $\sigma \in M_{12}$ and r is received, $d(r, \sigma) \leqslant 3$. There are two possibilities:

(i) $r \in S_{12}$. Comparing the sets E and $r(E) = \{r(x), x \in E\}$ gives the number and positions of the errors. Let $\{d_i\}$ be the set of permutations that do not fix any of the erroneous positions. For precisely one of these we will have $r \circ d_i(E) = E$ and the decoded word is $r \circ d_i$.

(ii) $r \notin S_{12}$. Letters appearing more than once in the received word are changed into the missing ones in all possible ways and the algorithm of section (i) is applied.

If (i) has no solution or (ii) has more than one solution then four errors are detected.

X. On the Asymptotic Behavior of t-Transitive Sets

In analogy with algebraic coding arguments, it is possible to derive interesting bounds relating, asymptotically, the parameters d, n, and $|G|$. Following the argument used in deriving the Varshamov–Gilbert bound it is easy to show that if

$$\sum_{i=0}^{d-1} D_i \binom{n}{i} \geqslant \frac{n!}{|G|}$$

then a PA $A(n, n-d, |G|)$ exists. It follows from this inequality that

$$2D_{d-1}\binom{n}{d-1} \sim 2e^{-1}(d-1)!\binom{n}{d-1} \geqslant \frac{n!}{|G|}$$

since $D_i \sim i!e^{-1}$. Consequently,

$$\frac{n!}{(n-d+1)!} \geqslant \frac{n!}{|G|}$$

and

$$n^d > \frac{n!}{(n-d+1)!} \geqslant \frac{n!}{|G|}.$$

Defining the rate of the code to be $R = \log |G| / \log n!$ and taking logs of both sides of this equation gives

$$d \log n > \log n! - \log |G|$$

or, dividing by $\log n!$,

$$\frac{d \log n}{\log n!} > 1 - R.$$

Using the Stirling approximation it is possible to show that

$$\frac{d \log n}{\log n!} \sim \frac{d}{n} > 1 - R$$

and codes satisfying this inequality exist and are called "asymptotically good." As with algebraic codes the problem remains in trying to find such codes.

If G is sharply t-transitive it is possible to show that, asymptotically,

$$\frac{d}{n} \sim 1 - R \qquad \text{for} \quad \frac{t}{n} - \epsilon < r < \frac{t}{n} + \epsilon$$

and hence sharply t-transitive groups are asymptotically good. The problem remains that, asymptotically, the only achievable rates are 0 or 1.

For codes which are t-transitive, but not sharply t-transitive, it can be shown that for $t \geqslant 2$

$$\frac{d}{n} \leqslant 1 - R$$

and so for such groups, asymptotically good codes do not exist. For $t = 1$ the existence of such codes remains an open question.

XI. Comments and Open Problems

Many aspects of permutation arrays remain to be investigated more thoroughly. This paper has attempted to lay a basis for such further work by considering briefly the known results of these arrays.

Of the many interesting problems suggested by this material it appears that the distance enumeration of permutation groups is one of the most important. The work reported in Section VII was concerned with bounding the size of arrays of type L and characterizing groups which satisfy these bounds. It is apparent that many more results of a similar nature will be forthcoming. Many other problems on the distance enumeration problem suggest themselves. In comparing the situation to that existing with algebraic codes over finite fields, the lack of tools to deal with the problem is noted. For example, suppose G is a subgroup of S_n and $G = H \times K$. For such a group, how are the distance enumerators of G, H and K related, considering their isomorphic copies in S_n? Further equations which the distances in a group must satisfy, similar to those of Section VIII, would be useful.

Further effort at finding perfect and sharp arrays should prove fruitful. Again the situation is reminiscent of that with algebraic codes, and the existence of perfect and sharp arrays invariably have interesting structure. In addition they define in some manner the "boundaries" of achievable performance and hence are important.

As a sidelight, the relationship between permutation groups and t-designs have been studied by many investigators. Recently they have been used to construct new t-designs, and it is likely that the relationship between t-designs and extremal permutation arrays is worthy of further study.

Many open problems will occur to the reader, and the results contained in this paper will, it is hoped, provide a useful starting point for their investigation.

ACKNOWLEDGMENT

The authors would like to thank the reviewer for his careful reading of the manuscript and for suggesting the proofs of propositions 1 and 2 used here, which are simpler than the original ones and, in the case of proposition 2, gave a slightly tighter bound than the original.

RECEIVED: April 28, 1978; REVISED November 17, 1978

REFERENCES

BLAKE, I. F. (1974), Permutation codes for discrete channels, *IEEE Trans. Information Theory* **20**, 138–140.

CARMICHAEL, R. D. (1956), "Introduction to the Theory of Groups of Finite Order," Dover, New York.

COHEN, G., AND DEZA, M. (1977), Decoding of permutation codes, *in* "International CNRS Colloquium," July, France.

DEZA, M., AND FRANKL, P. (1977), On maximal numbers of permutations with given maximal or minimal distance, *J. Combinatorial Theory A* **22**.

DEZA, M., AND VANSTONE, S. A. (1977), "Bounds for Permutation Arrays," Research Report CORR 77/28, University of Waterloo.

GORENSTEIN, D., AND HUGHES, D. R. (1961), Triply transitive groups in which only the identity fixes four letters, *Illinois J. Math.* **5**, 486–491.

HALL, M. (1967), "Combinatorial Theory," Ginn–Blaisdell, Boston.

HEISE, W. (1976), On sharply transitive sets of permutations, *J. Geometry* **7**, 9.

HEISE, W., AND KARZEL, H. (1972), Laguerre and Minkowski-m-Strukturen, *Rend. Inst. Mat. Univ. Trieste IV*, 1–9.

HERZOG, M., AND PRAGER, C. E. (1976), "Minimal Degree of Primitive Permutation Groups," Lecture Notes in Mathematics, No. 560, pp. 116–122, Springer–Verlag, Berlin/New York.

ITO, T., AND KIYOTA, M. (1979), Sharp permuation groups, in preparation.

IWAHORI, N. (1964), On a property of a finite group, *J. Fac. Sci. Univ. Tokyo* **10**, Part 1, 47–64.

IWAHORI, N., AND KONDO, T. (1965), On finite groups admitting a permutation representation P such that $TrP(\sigma) = 3$ for all $\sigma \neq 1$, *J. Fac. Sci. Univ. Tokyo* **10**, Part 2, 113–144.

KARZEL, M. (1978), Symmetrische Permutationsmengen, in *Aequationes Math.* **17**, 83–90.

KIYOTA, M. (1978), An inequality for finite permutation groups, to appear.

NAGAO, H. (1967), "Multiply Transitive Groups," Mathematics Department, California Institute of Technology, Pasadena, Calif.

PASSMAN, D. S. (1967), "Permutation Groups," Benjamin, New York.

PEDRINI, C. (1966), 3 Reti (Non Immergibili) Aventi dei Piani Duali di Qulli di Maulton Quali Sattopiani, *Rend. Accad. Naz. Lincei* **40** (VIII), 385–392.

PRETZEL, O., AND SCHLEIERMACHER, A. (1975a), On permutation groups whose nontrivial elements have at most three fixed points, *Proc. London Math. Soc.* **31** (3), 1–20.

PRETZEL, O., AND SCHLEIERMACHER, A. (1975b), On permutation groups in which nontrivial elements have p fixed points or none, *Proc. London Math. Soc.* **30** (3), 471–495.

QUATTROCCHI, P. (1975), Sugli insiemi di Sostituzioni Strettamente 3-Transitivi Finiti, *Atti. Sem. Mat. Fis. Univ. Modena* **24**.

SCHELLENBERG, P. J., AND VANSTONE, S. A. (1976), Some results on equidistant permutations, *in* "Proceedings, 6th Manitoba Conference on Numerical Mathematics," pp. 389–410.

TSUZUKI, T. (1967), Transitive extensions of certain permutation groups of rank 3, *Nagoya Math. J.* **31**, 31–36.

VANSTONE, S. (1978), personal communication.

WIELANDT, H. (1964), "Finite Permutation Groups," Academic Press, New York.

YOSHIZAWA, M. (1977), Quadruply transitive permutation groups whose four-point stabilizer is a Frobenius group, *Proc. Japan Acad.* **53**, 20–22.