



Title	Multiply transitivity of perfect 1-codes in symmetric groups
Author(s)	Nomura, Kazumasa
Citation	Osaka Journal of Mathematics. 1985, 22(4), p. 767-771
Version Type	VoR
URL	https://doi.org/10.18910/10522
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

Nomura, K.
Osaka J. Math.
22 (1985), 767-771

MULTIPLY TRANSITIVITY OF PERFECT 1-CODES IN SYMMETRIC GROUPS

Dedicated to Professor Hirosi Nagao on his 60th birthday

KAZUMASA NOMURA

(Received September 27, 1984)

1. Introduction

Let n be a positive integer, S_n be the symmetric group on $X=\{1, \dots, n\}$, T be the set of all transpositions in S_n and $U=T \cup \{1\}$. A subset Z of S_n is a *1-code* in S_n if $Ug \cap Uh = \emptyset$ holds for any distinct two elements g and h in Z . A 1-code Z in S_n is *perfect* if $S_n = \bigcup_{g \in Z} Ug$ (see [1]). Let $X^{(k)}$ be the set of all ordered k -tuples of distinct elements of X . We consider the natural action of S_n on $X^{(k)}$. A subset Z of S_n is k -transitive if the following condition holds.

For any x and y in $X^{(k)}$, there exists some z in Z that moves x to y , and the number of such elements in Z is a constant that is independent of the choice of x and y .

In this paper we shall prove the following result.

Theorem. *Perfect 1-codes in symmetric group of degree n are k -transitive for $0 \leq k < (n/2)$.*

From the above theorem we easily get the following corollary by counting the number of elements of Z that move x to y for fixed $x, y \in X^{(k)}$.

Corollary. *If S_n has a perfect 1-code then $\binom{n}{2} + 1$ divides $[(n/2) + 1]!$.*

In [4] Rothaus and Thompson proved that if S_n has a perfect 1-code then $\binom{n}{2} + 1$ is not divisible by any prime exceeding $\sqrt{n} + 1$. Their proof is based on the theory of group characters. In this paper we will give a combinatorial proof without using group characters.

Throughout this paper we assume that n is a fixed positive integer and S_n has a perfect 1-code Z . We shall use the following notations.

NOTATIONS

$X = \{1, \dots, n\}$.

$G=S_n$ the symmetric group on X .

T : the set of all transpositions in G .

$U=T \cup \{1\}$, where 1 denotes the identity in G .

S_Y : the symmetric group on a subset Y of X . We regard S_Y as a subgroup of G .

$T_Y=T \cap S_Y$.

Z : a perfect 1-code in G .

$p_K=|K \cap Z|$ for a subset K of G .

X^k : the set of all ordered k -tuples of elements of X .

$X^{(k)}=\{(a_1, \dots, a_k) \in X^k \mid a_i \neq a_j \text{ if } i \neq j\}$.

For $a=(a_1, \dots, a_k)$, $b=(b_1, \dots, b_k)$ in $X^{(k)}$ and g in G :

$ag=(a_1g, \dots, a_kg)$.

$a(i)=(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_k)$ for $1 \leq i \leq k$.

$a=\{a_1, \dots, a_k\}$ a subset of X .

$[a; b]=\{g \in G \mid ag=b\}$.

Proof of the theorem is based on the following equation.

Proposition. Let $0 < k < n$ and $a, b \in X^{(k)}$. Then

$$\left\{ \binom{n-k}{2} + 1 - k \right\} p_{[a; b]} + \sum_{u \in T_{\bar{b}}} p_{[a; bu]} + \sum_{i=1}^k p_{[a(i); b(i)]} = (n-k)!.$$

2. Proof of the proposition

Throughout this section we assume $0 < k < n$ and $a=(a_1, \dots, a_k)$, $b=(b_1, \dots, b_k) \in X^{(k)}$. We divide the proof into several steps.

Step 1. $|[a; b]| = (n-k)!$.

Proof. If $g \in [a; b]$ then $a_i g = b_i$ for $1 \leq i \leq k$ and $(X-a)g = X-\bar{b}$. Since $|X-a| = |X-\bar{b}| = n-k$, the number of such permutations is $(n-k)!$.

Step 2. $[a; b] = \bigcup_{g \in Z \cap U[a; b]} ([a; b] \cap Ug)$.

Proof. We have $G = \bigcup_{g \in Z} Ug$ since Z is a perfect 1-code. Then $K = \bigcup_{g \in Z} (K \cap Ug)$ for any subset K of G . If $h \in K \cap Ug$, then $h = ug$ for some $u \in U$, and $g = uh \in UK$. This implies $K \cap Ug = \emptyset$ when $g \notin UK$. Therefore we have $K = \bigcup_{g \in Z \cap UK} (K \cap Ug)$.

Step 3. $U[a; b] = \bigcup_{u \in U} [a; bu]$.

Proof. Note that $U[a; b] = [a; b]U$ since U is invariant under conjugation. Since $[a; b]g = [a; bg]$ holds for $g \in G$, we easily get step 3.

Let $Y = \bar{b} = \{b_1, \dots, b_k\}$. We divide U into three subsets.

$$\begin{aligned} T_1 &= \{(i, j) \in T \mid i, j \in X - Y\} \cup \{(1)\}, \\ T_2 &= \{(i, j) \in T \mid i, j \in Y\}, \\ T_3 &= \{(i, j) \in T \mid i \in Y \text{ and } j \in X - Y\}. \end{aligned}$$

Then $U = T_1 \cup T_2 \cup T_3$ (disjoint). Also we set

$$V_i = \bigcup_{u \in T_i} [a; bu] \quad (1 \leq i \leq 3).$$

Step 4. $V_1 = [a; b]$.

Proof. If $u \in T_1$ then $bu = b$ since u fixes all points in Y .

Step 5. $V_3 = \bigcup_{i=1}^k ([a(i); b(i)] - [a; b])$.

Proof. Take $g \in V_3$. Then $g \in [a; bu]$ for some $u \in T_3$. By definition of T_3 we have $b_i, u \in X - Y$ for some i . Then $a_i g = b_i u \neq b_i$ and $g \notin [a; b]$. Hence we have $g \in [a(i); b(i)]$. To show the converse take any $g \in [a(i); b(i)] - [a; b]$. Let $u = (b_i, a_i g) \in T$. Then $a_i g \neq b_i$ and $a_i g \in X - Y$. This implies $u \in T_3$. Moreover $a_i g = b_i u$ implies $g \in [a; bu]$. Hence $g \in V_3$.

Step 6. If $g \in V_1$ then $|[a; b] \cap Ug| = \binom{n-k}{2} + 1$.

Proof. We have $|[a; b] \cap Ug| = |[a; b] g^{-1} \cap U|$ since right translation by g^{-1} is a bijection on G . Since $g \in [a; b]$ from step 4, $[a; b] g^{-1} = [a; bg^{-1}] = [a; a]$. Hence $|[a; b] \cap Ug| = |[a; a] \cap U| = \binom{n-k}{2} + 1$ since $[a; a] \cap U$ contains 1 and all transpositions on $X - a$.

Step 7. If $g \in V_2$ or $g \in V_3$ then $|[a; b] \cap Ug| = 1$.

Proof. In either case we have $g \notin [a; b]$. As in the proof of step 6 we have $|[a; b] \cap Ug| = |[a; bg^{-1}] \cap U|$. Let $c = bg^{-1} = (c_1, \dots, c_k)$. Then $c \neq a$ since $g \notin [a; b]$. Hence $a_i \neq c_i$ for some i . If $u \in [a; c] \cap U$ then $a_i u = c_i$ and $u = (a_i, c_i)$. Since u is uniquely determined, we have $|[a; c] \cap U| \leq 1$. We also have $[a; c] \cap U \neq \emptyset$ since $g \in V_2 \cup V_3$.

Step 8. $\left\{ \binom{n-k}{2} + 1 \right\} p_{V_1} + p_{V_2} + p_{V_3} = (n-k)!$.

Proof. From step 1 and step 2 we have

$$\sum_{g \in G \cap U(a; b)} |[a; b] \cap Ug| = (n-k)!.$$

From step 3 and definition of V_i we have

$$U[a; b] = V_1 \cup V_2 \cup V_3.$$

This implies

$$Z \cap U[a; b] = (Z \cap V_1) \cup (Z \cap V_2) \cup (Z \cap V_3).$$

Then from step 6 and step 7 we get step 8.

Now the proposition follows from step 4, step 5 and step 8.

3. Proof of the theorem

We shall prove that $p_{[a; b]} = p_{[c; d]}$ holds for a, b, c, d in $X^{(k)}$ by induction on k . We assume $0 < k < (n/2)$ and the above equality holds for $k-1$.

Let $a, b \in X^{(k)}$ and $Y = \bar{b} = \{b_1, \dots, b_k\}$. Then from the proposition we have

$$r p_{[a; b]} + \sum_{u \in T_Y} p_{[a; bu]} = s,$$

where $r = \binom{n-k}{2} + 1 - k$, $s = (n-k)! - kq$ and $q = p_{[a(i); b(i)]}$. Note that q is independent of a, b and i by induction.

Then for $g \in S_Y$ we have

$$r p_{[a; bg]} + \sum_{u \in T_Y} p_{[a; bgu]} = s.$$

For simplification we write $p_g = p_{[a; bg]}$, then the above is

$$(1) \quad r p_g + \sum_{u \in T_Y} p_{gu} = s \quad (g \in S_Y).$$

We regard (1) as a system of linear equations with unknowns p_g ($g \in S_Y$). Then (1) has a solution

$$p_g = s / \left\{ r + \binom{k}{2} \right\} \quad (g \in S_Y).$$

Since r and s are constants which depend only on n and k , we must only show that (1) has a unique solution.

Let $S_Y = \{g_1, \dots, g_m\}$, $m = k!$, and let $D = (d_{ij})$ be the coefficient matrix of (1). Then

$$d_{ij} = \begin{cases} r & \text{if } i = j \\ 1 & \text{if } g_i u = g_j \text{ for some } u \in T_Y \\ 0 & \text{otherwise} \end{cases}$$

Now we consider the graph structure on S_Y defined by

“ g_i is adjacent to g_j if $g_i u = g_j$ for some $u \in T_Y$ ”. Let A be the adjacency matrix of the graph S_Y . Then $D = A + rE$, where E denotes the unit matrix of degree m . We must show that $\det(A + rE) \neq 0$. By way of contradiction, we assume that $\det(A + rE) = 0$. Then $(-r)$ is an eigenvalue of A . But the

absolute value of any eigenvalue of regular graph cannot exceeds its valency (see [3]). Therefore we have $r \leq \binom{k}{2}$. This implies $n^2 - (2k+1)n + 2 \leq 0$ and $2k \geq n$. This is a contradiction.

References

- [1] J.H. van Lint: *Introduction to coding theory*, Springer, New York, 1982.
- [2] E. Bannai and T. Ito: *Algebraic combinatorics*, Benjamin, 1984.
- [3] N. Biggs: *Finite groups of automorphisms*, Cambridge, 1971.
- [4] O. Rothaus and J.G. Thompson: *A combinatorial problem in the symmetric group*, *Pacific J. Math.* **18** (1966) 175–178.
- [5] M. Hall: *The theory of groups*, Macmillan, New York, 1959.

Faculty of General Education
Tokyo Medical and Dental University
Ichikawa, Chiba 272, Japan

