PACIFIC JOURNAL OF MATHEMATICS
Vol. 18, No. 1, 1966

A COMBINATORIAL PROBLEM IN THE SYMMETRIC GROUP

OSCAR ROTHAUS AND JOHN G. THOMPSON

If G is a group and T is a nonempty subset of G, we say that T divides G if and only if G contains a subset S such that every element of G has a unique representation as ts with t in T, s in S, in which case we write $T \cdot S = G$. We study the case where G is Σ_n, the symmetric group on n symbols and T is the set consisting of the identity and all transpositions in Σ_n.

The problem may be given a combinatorial setting as follows: For x, y in Σ_n, let $d(x, y)$ be the minimum number of transpositions needed to write xy^{-1}. One verifies that d converts Σ_n into a metric space, and that T divides Σ_n if and only if Σ_n can be covered by disjoint closed spheres of radius one.

We use the irreducible characters of Σ_n, together with judiciously selected permutation representations of Σ_n, to prove the following result.

THEOREM. **If $1 + (n(n-1))/2$ is divisible by a prime exceeding $\sqrt{n} + 2$, then T does not divide Σ_n.**

The proof depends on properties of Σ_n (see [1] and [2], pp. 190–193).

If $\lambda_1, \lambda_2, \cdots, \lambda_s$ are the parts of the partition σ in decreasing order and $\mu_1, \cdots, \mu_t$ are the parts of the partition τ in decreasing order, we write $\sigma > \tau$ provided the first nonvanishing difference $\lambda_i - \mu_i$ is positive. We say that σ dominates τ provided $\lambda_i - \mu_i \geqq 0$ for $i = 1, 2, \cdots, s$. Let σ' be the conjugate partition to σ with parts $\lambda'_1 \geqq \lambda'_2 \geqq \cdots \geqq \lambda'_{s'}$, and set

$$\pi(\sigma) = \sum_{i=1}^{s} \frac{\lambda_i(\lambda_i - 1)}{2} - \sum_{i=1}^{s'} \frac{\lambda'_i(\lambda'_i - 1)}{2} .$$

The function π has a simple interpretation. Namely, in the dot diagram of σ, the number of unordered pairs of dots in a common row minus the number of unordered pairs of dots in a common column equals $\pi(\sigma)$. However, it will become apparent that $\pi(\sigma)$ has a group theoretic interpretation too.

LEMMA 1. *If σ dominates τ, and $\sigma \neq \tau$ then $\pi(\sigma) > \pi(\tau)$.*

Proof. Let the parts of σ be $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_s$ and those of τ be $\mu_1 \geqq \mu_2 \geqq \cdots \geqq \mu_t$. By the hypotheses, we may suppose that $\lambda_1 = \mu_1$, $\lambda_2 = \mu_2, \cdots, \lambda_{r-1} = \mu_{r-1}, \lambda_r > \mu_r$ and $\lambda_{r+1} \geqq \mu_{r+1}, \cdots, \lambda_s \geqq \mu_s$, for some integer r less than s. A straightforward computation shows that $\pi(\tau)$ increases if μ_r is increased by 1 and μ_t is decreased by 1. With this observation made, the result is clear.

For any subset A of Σ_n, $\dot{A}$ denotes the sum of the elements of A in the group algebra of Σ_n (over the rationals), while

$$\ddot{A} = \sum_{a \in A} sg(a) \cdot a .$$

LEMMA 2. *If $R = R_\sigma$ is the irreducible representation of Σ_n associated to the partition σ, then $R(\dot{T})$ is singular if and only if $\pi(\sigma) = 1$.*

Proof. Since $\dot{T}$ is in the center of the group algebra, $R(\dot{T})$ is a scalar matrix, say $(1 + c)I = R(\dot{T})$. Thus, $R(\dot{T})$ is singular if and only if $c = -1$. Let Y be a Young tableau associated to σ, that is, the dot diagram of σ with a label on each dot, the labels coming from and exhausting the set $\{1, 2, \cdots, n\}$. Let A be the subgroup of Σ_n permuting the columns of Y and B the subgroup of Σ_n permuting the rows of Y, and let

$$E = \frac{\dot{A}}{|A|} \cdot \frac{\ddot{B}}{|B|} .$$

Then E is a primitive idempotent and has the property that $R_\tau(E) = 0$ for $\tau \neq \sigma$. We have $R_\sigma(E)R_\sigma(\dot{T}) = (1 + c)R_\sigma(E)$. As E vanishes in each R_τ with $\tau \neq \sigma$, we have trivially, $R_\tau(E) \cdot R_\tau(\dot{T}) = (1 + c)R_\tau(E)$ for all $\tau \neq \sigma$. Hence

$$E \cdot \dot{T} = (1 + c)E . \tag{4}$$

Let T_0 be the set of transpositions in Σ_n. Then (4) implies

$$E \cdot \dot{T}_0 = cE . \tag{5}$$

Since $A \cap B = 1$, to determine c, it suffices to determine the multiplicity (i.e., coefficient) of 1 in $E \cdot \dot{T}_0$. It follows readily that $c = \Sigma sg(b)$, the summation ranging over all triples (a, b, t) with a in A, b in B, t in T_0, such that $abt = 1$. Since $abt = 1$ if and only if $ab = t$, it is easy to see that whenever $abt = 1$, then either $t \in A$ or $t \in B$. Hence, $c = -\pi(\sigma)$, as required.

In the following discussion, σ, Y, A, B, E have the same meaning as above.

We next consider a family of permutation representations of Σ_n. Let X be a Young tableau for the partition τ and let C be the subgroup permuting the columns of X. Then P_τ denotes the permutation representation of Σ_n on the cosets of C. Thus, for x in Σ_n,

$P_\tau(x)\colon Cg \to Cgx$. It is clear that P_τ depends only on τ and not on X. As is customary, we view P_τ as a representation of the group algebra.

LEMMA 3. *If $\sigma > \tau$, then R_σ is not a constituent of P_τ.*

Proof. Since E is a primitive idempotent, $tr(P_\tau(E))$ is the multiplicity of R_σ in P_τ. Consider a coset Cg. A contribution to $tr(P_\tau(E))$ occurs each time $Cgab = Cg$ with a in A, b in B, the contribution being

$$\frac{sg(b)}{|A|\cdot|B|}.$$

Thus, from the coset Cg, we get

$$\frac{\Sigma sg(b)}{|A|\cdot|B|},$$

the summation being over those pairs (a, b) with a in A, b in B and ab in $g^{-1}Cg$. As $\sigma > \tau$, it is easy to verify that there is a row of Y which has at least two symbols in common with some column of Xg, that is, $B \cap g^{-1}Cg$ contains a transposition $t = t(g)$. This implies that whenever a pair (a, b) occurs in the above summation, so does the pair (a, bt), so $tr(P_\tau(E)) = 0$, as required.

Now let p be a prime divisor of $1 + (n(n-1))/2$ with $p \geqq \sqrt{n} + 2$. Let $n = (p-1)q + r$ with $0 \leqq r < p - 1$. Hence $q < p - 2$. Let τ be the partition of n with r parts equal to $q + 1$ and $p - 1 - r$ parts equal to q. We see that τ' has q parts equal to $p - 1$ and one part equal to r. Hence

$$\begin{aligned}\pi(\tau) &= \frac{(q+1)q}{2}r + \frac{q(q-1)}{2}(p-1-r) \\ &\qquad - \left\{\frac{(p-1)(p-2)}{2}q + \frac{r(r-1)}{2}\right\} \\ &= \frac{q(p-1)}{2}\{q + 1 - (p-2)\} - \frac{r(r-1)}{2} - q(p-1-r)\,.\end{aligned}$$

Since $q + 1 \leqq p - 2$, it follows that $\pi(\tau) < -1$.

By Lemma 3, if R_σ is a constituent of P_τ, then $\sigma \leqq \tau$. The structure of τ now yields that whenever $\sigma \leqq \tau$, then τ dominates σ.

By Lemma 1, $\pi(\sigma) \leqq \pi(\tau) < -1$, and hence by Lemma 2, $R_\sigma(\dot{T})$ is nonsingular. Thus $P_\tau(\dot{T})$ is nonsingular.

Let $d = d_\tau$ be the degree of P_τ. Since $d = |\Sigma_n : C|$, we see that d is divisible by the same power of p as $|\Sigma_n|$, since $|C| = (p-1)!^q r!$ is prime to p. Now suppose $T \cdot U = \Sigma_n$. Then $P_\tau(\dot{T})P_\tau(U) = P_\tau(\dot{\Sigma}_n)$.

It is clear that $P_\tau(\dot{\Sigma}_n)$ is the matrix with $|C|$ in every entry, so is of rank 1. Since $P_\tau(\dot{T})^{-1}$ is a polynomial in $P_\tau(\dot{T})$, and since $P_\tau(\dot{\Sigma}_n) = P_\tau(\dot{x})P_\tau(\dot{\Sigma}_n)$ for all x in Σ_n, it follows that $P_\tau(\dot{U}) = aP_\tau(\dot{\Sigma}_n)$ for some rational number a. This implies that $a(1 + (n(n-1))/2) = 1$, so that

$$P_\tau(\dot{U}) = \frac{1}{1 + \dfrac{n(n-1)}{2}} P_\tau(\dot{\Sigma}_n)$$

does not have integral entries, which is a contradiction, since $P_\tau(\dot{U})$ is a sum of $|U|$ permutation matrices.

REMARK 1. The integers 1, 2, 3, 6, 91, 137, 733 and 907 are the only integers less than 1,000 which fail to satisfy the theorem.

REMARK 2. As the referee has noted, essentially the same proof yields: If $(n(n-1))/2$ is divisible by a prime exceeding $\sqrt{n} + 2$, then T_0 does not divide Σ_n.

REFERENCES

1. D. E. Littlewood, *The theory of group characters*, Oxford at the Clarendon Press.
2. B. L. van der Waerden, *Modern algebra*, Vol. II.

Received December 22, 1964.

INSTITUTE FOR DEFENSE ANALYSES
PRINCETON, NEW JERSEY
UNIVERSITY OF CHICAGO