A COMBINATORIAL PROBLEM IN THE SYMMETRIC GROUP

Oscar S. Rothaus and John Griggs Thompson
A COMBINATORIAL PROBLEM IN THE
SYMMETRIC GROUP

OSCAR ROTAUS 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 \( \Sigma_n \), the symmetric group on \( n \) symbols and \( T \) is the set consisting of the identity and all transpositions in \( \Sigma_n \).

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

We use the irreducible characters of \( \Sigma_n \), together with judiciously selected permutation representations of \( \Sigma_n \), 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 \( \Sigma_n \).

The proof depends on properties of \( \Sigma_n \) (see [1] and [2], pp. 190–193). If \( \lambda_1, \lambda_2, \cdots, \lambda_s \) are the parts of the partition \( \sigma \) in decreasing order and \( \mu_1, \cdots, \mu_t \) are the parts of the partition \( \tau \) in decreasing order, we write \( \sigma > \tau \) provided the first nonvanishing difference \( \lambda_i - \mu_i \) is positive. We say that \( \sigma \) dominates \( \tau \) provided \( \lambda_i - \mu_i \geq 0 \) for \( i = 1, 2, \cdots, s \). Let \( \sigma' \) be the conjugate partition to \( \sigma \) with parts \( \lambda'_1 \geq \lambda'_2 \geq \cdots \geq \lambda'_s \), and set

\[
\pi(\sigma) = \sum_{i=1}^{s} \frac{\lambda_i(\lambda_i - 1)}{2} - \sum_{i=1}^{t} \frac{\lambda'_i(\lambda'_i - 1)}{2}.
\]

The function \( \pi \) has a simple interpretation. Namely, in the dot diagram of \( \sigma \), 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 \( \sigma \) dominates \( \tau \), and \( \sigma \neq \tau \) then \( \pi(\sigma) > \pi(\tau) \).

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

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

\[
\hat{A} = \sum_{a \in A} sg(a) \cdot a.
\]

**Lemma 2.** If \( R = R_\sigma \) is the irreducible representation of \( \Sigma_n \) associated to the partition \( \sigma \), then \( R(\hat{T}) \) is singular if and only if \( \pi(\sigma) = 1 \).

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

\[
E = \frac{\hat{A}}{|A|} \cdot \frac{\hat{B}}{|B|}.
\]

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

\[
E \cdot \hat{T} = (1 + c)E.
\]

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

\[
E \cdot T_0 = cE.
\]

Since \( A \cap B = 1 \), to determine \( c \), it suffices to determine the multiplicity (i.e., coefficient) of 1 in \( E \cdot T_0 \). 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, \( \sigma, Y, A, B, E \) have the same meaning as above.

We next consider a family of permutation representations of \( \Sigma_n \). Let \( X \) be a Young tableau for the partition \( \tau \) and let \( C \) be the subgroup permuting the columns of \( X \). Then \( P_\tau \) denotes the permutation representation of \( \Sigma_n \) on the cosets of \( C \). Thus, for \( x \) in \( \Sigma_n \),
$P_\tau(x) : Cg \rightarrow Cgx$. It is clear that $P_\tau$ depends only on $\tau$ and not on $X$. As is customary, we view $P_\tau$ as a representation of the group algebra.

**Lemma 3.** If $\sigma > \tau$, then $R_\sigma$ is not a constituent of $P_\tau$.

**Proof.** Since $E$ is a primitive idempotent, $tr(P_\tau(E))$ is the multiplicity of $R_\sigma$ in $P_\tau$. 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

$$sg(b) \frac{1}{|A| \cdot |B|}.$$

Thus, from the coset $Cg$, we get

$$\sum sg(b) \frac{1}{|A| \cdot |B|},$$

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 $p \geq \sqrt{n} + 2$. Let $n = (p - 1)q + r$ with $0 \leq r < p - 1$. Hence $q < p - 2$. Let $\tau$ be the partition of $n$ with $r$ parts equal to $q + 1$ and $p - 1 - r$ parts equal to $q$. We see that $\tau'$ has $q$ parts equal to $p - 1$ and one part equal to $r$. Hence

$$\pi(\tau) = \frac{(q + 1)q}{2} r + \frac{q(q - 1)}{2} (p - 1 - r)$$

$$- \left\{ \frac{(p - 1)(p - 2)}{2} q + \frac{r(r - 1)}{2} \right\}$$

$$= \frac{q(p - 1)}{2} \left\{ q + 1 - (p - 2) \right\} - \frac{r(r - 1)}{2} - q(p - 1 - r).$$

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

By Lemma 3, if $R_\sigma$ is a constituent of $P_\tau$, then $\sigma \leq \tau$. The structure of $\tau$ now yields that whenever $\sigma \leq \tau$, then $\tau$ dominates $\sigma$.

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

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

A COMBINATORIAL PROBLEM IN THE SYMMETRIC GROUP 177
It is clear that $P_\tau(\hat{\Sigma}_n)$ is the matrix with $|C|$ in every entry, so is of rank 1. Since $P_\tau(\hat{T})^{-1}$ is a polynomial in $P_\tau(\hat{T})$, and since $P_\tau(\hat{\Sigma}_n) = P_\tau(\hat{x})P_\tau(\hat{\Sigma}_n)$ for all $x$ in $\Sigma_n$, it follows that $P_\tau(\hat{U}) = aP_\tau(\hat{\Sigma}_n)$ for some rational number $a$. This implies that $a(1 + (n(n - 1))/2) = 1$, so that

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

does not have integral entries, which is a contradiction, since $P_\tau(\hat{U})$ 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 $\Sigma_n$.

**References**

Edward Joseph Barbeau, *Semi-algebras that are lower semi-lattices* .... 1
Steven Fredrick Bauman, *The Klein group as an automorphism group without fixed point* ........................................ 9
Homer Franklin Bechtell, Jr., *Frattini subgroups and \(\Phi\)-central groups* .... 15
Edward Kenneth Blum, *A convergent gradient procedure in prehilbert spaces* ........................................ 25
Edward Martin Bolger, *The sum of two independent exponential-type random variables* ........................................ 31
David Wilson Bressler and A. P. Morse, *Images of measurable sets* .... 37
Dennison Robert Brown and J. G. LaTorre, *A characterization of uniquely divisible commutative semigroups* ........................................ 57
Selwyn Ross Caradus, *Operators of Riesz type* ........................................ 61
Jeffrey Davis and Isidore Isaac Hirschman, Jr., *Toeplitz forms and ultraspherical polynomials* ........................................ 73
Lorraine L. Foster, *On the characteristic roots of the product of certain rational integral matrices of order two* ........................................ 97
Alfred Gray and S. M. Shah, *Asymptotic values of a holomorphic function with respect to its maximum term* ........................................ 111
Sidney (Denny) L. Gulick, *Commutativity and ideals in the biduals of topological algebras* ........................................ 121
G. J. Kurowski, *Further results in the theory of monodiffric functions* .... 139
Lawrence S. Levy, *Commutative rings whose homomorphic images are self-injective* ........................................ 149
Calvin T. Long, *On real numbers having normality of order \(k\)* .......... 155
Bertram Mond, *An inequality for operators in a Hilbert space* .......... 161
John William Neuberger, *The lack of self-adjointness in three-point boundary value problems* ........................................ 165
C. A. Persinger, *Subsets of \(n\)-books in \(E^3\)* ........................................ 169
Oscar S. Rothaus and John Griggs Thompson, *A combinatorial problem in the symmetric group* ........................................ 175
Rodolfo DeSapio, *Unknotting spheres via Smale* ........................................ 179
James E. Shockley, *On the functional equation* 
\[ F(mn)F((m, n)) = F(m)F(n)f((m, n)) \] ........................................ 185
Kenneth Edward Whipple, *Cauchy sequences in Moore spaces* ........................................ 191