AN APPLICATION OF LINEAR PROGRAMMING TO PERMUTATION GROUPS

W. H. MILLS

Let S_N denote the symmetric group acting on a finite set X of N elements, $N \geqq 3$. Let σ and τ be elements of S_N. In a previous paper [1] the following question was raised: If σ and τ commute on most of the points of X, does it necessarily follow that τ can be approximated by an element in the centralizer $C(\sigma)$ of σ?

We define a distance $D(\sigma, \tau)$ between two elements σ and τ in S_N to be the number of points g in X such that $g\sigma \neq g\tau$. (This differs from the distance $d(\sigma, \tau)$ defined in [1] by a factor of N.) Then $D(\sigma\tau, \tau\sigma)$ is the number of points in X on which σ and τ do not commute. Let $D_\sigma(\tau)$ denote the distance from τ to the centralizer $C(\sigma)$ of σ in S_N. Thus

$$D_\sigma(\tau) = \min_{\lambda \in C(\sigma)} D(\tau, \lambda) .$$

It will be shown that the determination of $D_\sigma(\tau)$ is equivalent to the optimal assignment problem in linear programming.

The question raised in [1] can be phrased thus: If $D(\sigma\tau, \tau\sigma)$ is small, is $D_\sigma(\tau)$ necessarily small? If σ is not the identity we set

$$D_\sigma = \max_{\tau \notin C(\sigma)} D_\sigma(\tau)/D(\sigma\tau, \tau\sigma) .$$

Now D_σ is large unless σ is the product of many disjoint cycles, most of which have the same length. Some examples of this are worked out in detail in [1]. This leads us to study the case where σ is the product of m disjoint cycles of length n, where $N = nm$ and m is large. In [1] it was shown that if $m \geqq 2$, then

(a) if n is even, then $D_\sigma = n/4$, and

(b) if n is odd, $n \geqq 3$, then
$(n-1)/4 \leqq D_\sigma \leqq n/4$.

In the present paper it is shown that if n is odd, $n \geqq 3$, and $m \geqq n-2$, then

$$D_\sigma = (n-1)^2/(4n-6) .$$

1. Relation to linear programming. Let σ be an arbitrary element of the symmetric group S_N. We write σ as the product of disjoint cycles:

$$\sigma = C_1 C_2 \cdots C_m ,$$

Received October 22, 1962.

where C_i is a cycle of length n_i, and every point left fixed by σ is counted as a cycle of length 1. Then

$$n_1 + n_2 + \cdots + n_m = N .$$

Let g_i be a fixed element of the cycle C_i, $1 \leqq i \leqq m$. Then every element of the underlying set X is of the form $g_i\sigma^a$, where $1 \leqq i \leqq m$ and $0 \leqq a < n_i$.

Let λ be an element of $C(\sigma)$, the centralizer of σ in S_N. Then since

$$(g_i\sigma^a)\lambda = (g_i\lambda)\sigma^a ,$$

it follows that λ is determined by its effect on the g_i, and that λ permutes the cycles C_i. Let $\bar{\lambda}$ be the permutation of $1, 2, \cdots, m$ such that $i\bar{\lambda} = j$ if λ maps C_i onto C_j. We will call a permutation α in S_m admissible if $\alpha = \bar{\lambda}$ for some $\lambda \in C(\sigma)$. It is easy to see that α is admissible if and only if $n_i = n_{i\alpha}$, $1 \leqq i \leqq m$. Let A denote the group of all admissible permutations.

Let τ be a second element of S_N. We wish to determine

$$D_\sigma(\tau) = \min_{\lambda \in C(\sigma)} D(\tau, \lambda) ,$$

where $D(\tau, \lambda)$ is the number of points g in X such that $g\tau \neq g\lambda$. Let $E(\tau, \lambda)$ denote the number of points h in X such that $h\tau = h\lambda$, and set

$$E_\sigma(\tau) = \max_{\lambda \in C(\sigma)} E(\tau, \lambda) .$$

Then

$$D_\sigma(\tau) = N - \max_{\lambda \in C(\sigma)} E(\tau, \lambda) = N - E_\sigma(\tau) .$$

We shall show that the determination of $E_\sigma(\tau)$ is equivalent to the optimal assignment problem in linear programming.

The elements λ in $C(\sigma)$ are the permutations of the form

$$(g_i\sigma^a)\lambda = g_{i\alpha}\sigma^{a+r_i}, 1 \leqq i \leqq m, 0 \leqq a < n_i ,$$

where α is admissible and $r_1, r_2, \cdots, r_m$, are integers. Moreover

$$E(\tau, \lambda) = \sum_{i=1}^{m} F_i(r_i, i\alpha) ,$$

where $F_i(r, j)$ is the number of solutions of

$$(1) \qquad (g_i\sigma^x)\tau = g_j\sigma^{x+r}, 0 \leqq x < n_i .$$

Set

$$b_{ij} = \begin{cases} 0 & \text{if } n_i \neq n_j \\ \max_r F_i(r, j) & \text{if } n_i = n_j \,. \end{cases}$$

Thus b_{ij} is the maximum number of points of C_i on which an element λ in $C(\sigma)$, that maps C_i onto C_j, can agree with τ. We have

$$E_\sigma(\tau) = \max_{\lambda \in C(\sigma)} E(\tau, \lambda) = \max_{\alpha \in A} \max_{r_1 \cdots, r_m} \sum_{i=1}^m F_i(r_i, i\alpha) \,,$$

or

$$(2) \qquad E_\sigma(\tau) = \max_{\alpha \in A} \sum_{i=1}^m b_{i,i\alpha} \,.$$

Now let β be an arbitrary permutation of $1, 2, \cdots, m$. There is an $\alpha \in A$ such that $i\alpha = i\beta$ for all i such that $n_i = n_{i\beta}$. Therefore, since $b_{ij} = 0$ if $n_i \neq n_j$, it follows that we can take the maximum in (2) over the entire symmetric group S_m instead of over the subgroup A. Thus

$$(3) \qquad E_\sigma(\tau) = \max_{\beta \in S_m} \sum_{i=1}^m b_{i,i\beta} \,.$$

The determination of a maximum of the form (3) is the optimal assignment problem in linear programming—ordinarily expressed in terms of m individuals to be assigned to m jobs, where b_{ij} is a measure of how well the ith individual can do the jth job. (See [2]; or [3], pp. 131-136.) Von Neumann [2] has shown that this problem is equivalent to a certain zero-sum two-person game.

The equality (3) can be rewritten in the form

$$(4) \qquad E_\sigma(\tau) = \max_P \sum_{i,j} e_{ij} b_{ij} \,,$$

where P is the set of all $m \times m$ permutation matrices (e_{ij}). The set P is clearly a subset of the set R of all real $m \times m$ matrices (y_{ij}) such that

$$(5) \qquad y_{ij} \geqq 0, 1 \leqq i, j \leqq m \,,$$

$$(6) \qquad \sum_{i=1}^m y_{ij} = 1 \,, \qquad 1 \leqq j \leqq m \,,$$

and

$$(7) \qquad \sum_{j=1}^m y_{ij} = 1 \,, \qquad 1 \leqq i \leqq m \,.$$

The matrices of the set R form a convex bounded subset of real m^2-dimensional Euclidean space, whose vertices are the permutation matrices. (This result is due to Garrett Birkhoff. See [2], pp. 8–10.) It follows that

$$E_\sigma(\tau) = \max_P \sum_{i,j} e_{ij}b_{ij} = \max_R \sum_{i,j} y_{ij}b_{ij} \; .$$

It is now clear that the determination of $E_\sigma(\tau)$ is actually a problem in linear programming. It is easy to see that the equalities (6) and (7) can be replaced by inequalities (see [2], Lemma 1). Thus if Y is the set of all real $m \times m$ matrices (y_{ij}) satisfying (5),

$$\sum_{i=1}^{m} y_{ij} \leqq 1 \; , \qquad 1 \leqq j \leqq m \; , \tag{8}$$

and

$$\sum_{j=1}^{m} y_{ij} \leqq 1 \; , \qquad 1 \leqq i \leqq m \; , \tag{9}$$

then

$$E_\sigma(\tau) = \max_Y \sum_{i,j} y_{ij}b_{ij} \; .$$

For our purposes this is the most useful formulation of the problem.

2. **Blocks.** By a block of length s, $s \geqq 1$, we mean a set of the form $g\sigma, g\sigma^2, \cdots, g\sigma^s$, such that σ and τ commute on $g\sigma, g\sigma^2, \cdots, g\sigma^{s-1}$, but do not commute on g and $g\sigma^s$. The length of a block B will be denoted by $|B|$. If σ and τ commute on every point of the cycle C_i, then we say that σ and τ commute on C_i. In this case the cycle C_i contains no blocks. On the other hand if C_i contains exactly q points on which σ and τ do not commute, $q \geqq 1$, then C_i consists of exactly q blocks, and each point of C_i belongs to one and only one block. Now $D(\sigma\tau, \tau\sigma)$ is the number of points in X on which σ and τ do not commute. It follows that $D(\sigma\tau, \tau\sigma)$ is equal to the total number of blocks in all cycles.

If σ and τ commute on the points $g, g\sigma, g\sigma^2, \cdots, g\sigma^a$, then it follows, by induction on a, that

$$(g\sigma^\nu)\tau = (g\tau)\sigma^\nu \; , \qquad 0 \leqq \nu \leqq a + 1 \; .$$

In particular if σ and τ commute on the cycle C_i, and if $g_i\tau = g_j\sigma^r$, then

$$g_i\sigma^x\tau = g_j\sigma^{r+x}$$

for all x. Therefore, in this case, the number of solutions $F_i(r, j)$ of (1) is n_i, so that $b_{ij} = n_i = n_j$.

Now let C_i be a cycle on which σ and τ do not commute. Then

C_i is composed of one or more blocks. Let B be one of the blocks of C_i, and let B consist of the points

$$g_i\sigma^b,\ g_i\sigma^{b+1},\ \cdots,\ g_i\sigma^{b+s-1}\ .$$

Then $|B| = s$. Let $g_i\sigma^b\tau = g_j\sigma^{b+r}$. Since σ and τ commute on $g_i\sigma^{b+\mu}$, $0 \leqq \mu \leqq s-2$, we have

$$g_i\sigma^{b+\nu}\tau = g_j\sigma^{b+r+\nu}\ , \qquad 0 \leqq v \leqq s-1\ .$$

In particular $n_j \geqq s$. Moreover if $n_i = n_j$, then the number of solutions $F_i(r, j)$ of (1) is at least s, and hence $b_{ij} \geqq s$. It follows that *if $n_i = n_j$, then b_{ij} is at least the length of the longest block of C_i that τ maps into C_j.*

Moreover since σ and τ do not commute on $g_i\sigma^{b+s-1}$, we have

$$g_i\sigma^{b+s}\tau \neq g_i\sigma^{b+s-1}\tau\sigma = g_j\sigma^{b+r+s}\ .$$

In particular if C_i consists of the single block B, then $s = n_i$, and

$$g_j\sigma^{b+r} = g_i\sigma^b\tau = g_i\sigma^{b+s}\tau \neq g_j\sigma^{b+r+s}\ .$$

It follows that $s \neq n_j$. Therefore we must have $n_j > s = n_i$. Thus if C_i consists of a single block B, then τ maps B into a cycle C_j such that $n_j > n_i$. This is a generalization of a result noted in [1]: *If the cycles C_i all have the same length, then no cycle can consist of a single block.*

3. The case n odd. We now restrict ourselves to the case where σ is the product of m cycles of the same length n, $n > 1$, $N = mn$, $N \geqq 3$. Thus we have $n_1 = n_2 = \cdots = n_m = n$, and every permutation in S_m is admissible, so that $A = S_m$. Set

$$D_\sigma = \max_{\tau \notin C(\sigma)} \{D_\sigma(\tau)/D(\sigma\tau, \tau\sigma)\}\ .$$

It was shown in [1] that if n is even and $m \geqq 2$, then $D_\sigma = n/4$. We now show that if n is odd and $m \geqq n-2$, then $D_\sigma = (n-1)^2/(4n-6)$. Without loss of generality we can take X to be the set of the first N positive integers, and

$$\sigma = (1, 2, \cdots, n)(n+1, \cdots, 2n) \cdots (N-n+1, \cdots, N)\ .$$

Thus for g in X we have

$$g\sigma = \begin{cases} g+1 & \text{if } n \nmid g\ , \\ g+1-n & \text{if } n \mid g\ . \end{cases}$$

We let C_i denote the ith cycle:

$$C_i = (in - n + 1, in - n + 2, \cdots, in) .$$

We must show that

$$\max_{\tau \notin C(\sigma)} \{D_\sigma(\tau)/D(\sigma\tau, \tau\sigma)\} = (n-1)^2/(4n-6) .$$

We break up the proof into two lemmas.

LEMMA 1. *If n is odd and $m \geqq n-2$, then there exists a $\tau \in S_N$, $\tau \notin C(\sigma)$, such that*

$$D_\sigma(\tau)/D(\sigma\tau, \tau\sigma) = (n-1)^2/(4n-6) .$$

Proof. Suppose first that $n = 3$. Then

$$\sigma = (123)(456) \cdots (N-2, N-1, N) .$$

Here we take $\tau = (12)$. Then $\sigma\tau\sigma^{-1}\tau^{-1} = (132)$, so that σ and τ commute on all but three points, and $D(\sigma\tau, \tau\sigma) = 3$. Moreover

$$b_{ij} = \begin{cases} 0 & \text{if } i \neq j , \\ 1 & \text{if } i = j = 1 , \\ 3 & \text{if } i = j > 1 . \end{cases}$$

Hence

$$E_\sigma(\tau) = \max_P \sum_{i,j} e_{ij} b_{ij} = \sum_{i=1}^{m} b_{ii} = 3m - 2 = N - 2 .$$

Therefore $D_\sigma(\tau) = N - E_\sigma(\tau) = 2$, and

$$D_\sigma(\tau)/D(\sigma\tau, \tau\sigma) = 2/3 = (n-1)^2/(4n-6) .$$

We can now suppose that $n \geqq 5$. Set $n = 2K + 1$. Then $K \geqq 2$, and $m \geqq 2K - 1$. Set $\tau = \tau_1\tau_2 \cdots \tau_K$, where

$$\begin{aligned} \tau_r = (r, n + r, 2n + r, \cdots, Kn - n + r, K + r ,\\ Kn + r, Kn + n + r, \cdots, 2Kn - 2n + r) . \end{aligned}$$

Thus for g in X we have

$$g\tau = \begin{cases} g + n \text{ if } g = pn + r, 0 \leqq p \leqq K - 2, 1 \leqq r \leqq K , \\ K + r \text{ if } g = Kn - n + r, 1 \leqq r \leqq K , \\ Kn + r \text{ if } g = K + r, 1 \leqq r \leqq K , \\ g + n \text{ if } g = pn + r, K \leqq p \leqq 2K - 3, 1 \leqq r \leqq K , \\ r \text{ if } g = 2Kn - 2n + r, 1 \leqq r \leqq K , \\ g \text{ otherwise} . \end{cases}$$

The blocks of τ are shown schematically in Figure 1.

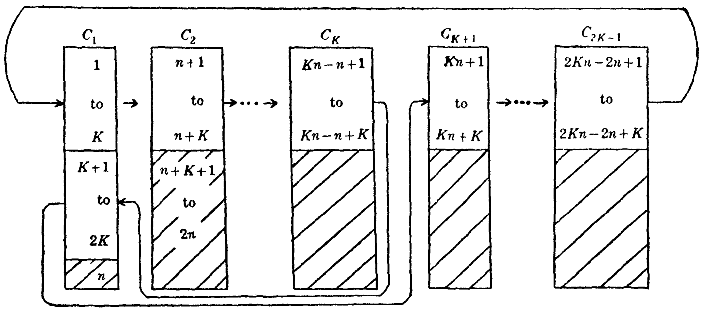

Figure 1

The permutation τ maps the shaded blocks of Figure 1 onto themselves, and it maps the other blocks as indicated by the arrows. The permutations σ and τ commute on the cycles C_i with $i \geqq 2K$. Hence these cycles contain no blocks and are not shown in the figure. Let c denote the number of cycles on which σ and τ commute. Thus $c = m - (2K - 1)$. The number of points on which the identity I agrees with τ is

$$E(\tau, I) = cn + 1 + (2K - 2)(K + 1) .$$

Clearly I belongs to $C(\sigma)$. On the other hand suppose that λ is an arbitrary element of $C(\sigma)$. If there exists a cycle C_i such that τ and λ do not agree on any points of C_i, then

$$E(\tau, \lambda) \leqq cn + (2K - 2)(K + 1) .$$

If τ and λ agree on the point n, then

$$E(\tau, \lambda) \leqq cn + 1 + (2K - 2)(K + 1) .$$

If τ and λ do not agree on n, and if τ and λ agree on at least one point of every cycle C_i, then there are at least $K - 1$ blocks of length $K + 1$ on which τ and λ do not agree. Hence in this case

$$\begin{aligned} E(\tau, \lambda) &\leqq cn + (K - 1)(K + 1) + K^2 \\ &= cn + 1 + (2K - 2)(K + 1) . \end{aligned}$$

Therefore

$$\begin{aligned} E_\sigma(\tau) &= \max_{\lambda \in C(\sigma)} E(\tau, \lambda) = E(\tau, I) = cn + 1 + (2K - 2)(K + 1) \\ &= (m - 2K + 1)n + 2K^2 - 1 = N - 2K^2. \end{aligned}$$

Hence

$$D_\sigma(\tau) = N - E_\sigma(\tau) = 2K^2 = \tfrac{1}{2}(n - 1)^2 .$$

We see from Figure 1 that the total number of blocks is

$$2(2K-2)+3=2n-3\ .$$

Since this is equal to $D(\sigma\tau, \tau\sigma)$, we have

$$D_\sigma(\tau)/D(\sigma\tau, \tau\sigma)=(n-1)^2/(4n-6)\ .$$

This proves the lemma.

Lemma 1 establishes that $D_\sigma \geqq (n-1)^2/(4n-6)$ if n is odd and $m \geqq n-2$. Our other lemma, which establishes the opposite inequality, does not depend on the size of m.

LEMMA 2. *If n is odd and $\tau \in S_N$, $\tau \notin C(\sigma)$, then*

$$D_\sigma(\tau)/D(\sigma\tau, \tau\sigma) \leqq (n-1)^2/(4n-6)\ .$$

Proof. As before we set $n=2K+1$. Let c denote the number of cycles C_i on which σ and τ commute, and let Q_s denote the total number of blocks of length s. Since the cycles C_i all have the same length n, it follows from the last paragraph of § 2 that there are no blocks of length n. Hence

$$D(\sigma\tau, \tau\sigma)=\sum_{s=1}^{n-1} Q_s\ ,$$

since this sum is equal to the total number of blocks. Set

$$G(\tau)=N-\frac{(n-1)^2}{4n-6}\sum_{s=1}^{n-1} Q_s\ .$$

The desired result holds if and only if

$$E_\sigma(\tau) \geqq G(\tau)\ .$$

By § 1 it is sufficient to show that there exists a real $m \times m$ matrix (y_{ij}) satisfying (5), (8), (9) and

$$\sum_{i,j} y_{ij} b_{ij} \geqq G(\tau)\ . \tag{10}$$

Case 1.

$$cn+\sum_{s=1}^{n-1} s^2 Q_s/n \geqq G(\tau)\ .$$

In this case we set $y_{ij}=n_{ij}/n$, where n_{ij} is the number of points of C_i which are mapped into C_j by τ. Now (5), (6) and (7) hold for this choice of (y_{ij}). Hence (8) and (9) also hold.

Suppose C_i is a cycle on which σ and τ commute. Suppose τ maps C_i onto the cycle C_z. Then

$$y_{ij} = \begin{cases} 1 & \text{if } j = z , \\ 0 & \text{if } j \neq z . \end{cases}$$

Moreover $b_{iz} = n$ by § 2. Hence

$$\sum_{j=1}^{m} y_{ij} b_{ij} = n ,$$

and therefore

$$\sum_{1} \sum_{j=1}^{m} y_{ij} b_{ij} = cn ,$$

where Σ_1 runs over those c values of i such that σ and τ commute on C_i.

Next suppose that C_i is a cycle on which σ and τ do not commute. Let C_z be a cycle such that one or more blocks of C_i are mapped into C_z by τ. Let us denote these blocks by $B_1, B_2, \cdots, B_u$. We may suppose that these blocks are numbered in such a way that B_1 is the longest of them. Then $b_{iz} \geqq |B_1|$ by § 2. Moreover

$$n_{iz} = |B_1| + |B_2| + \cdots + |B_u| ,$$

and

$$y_{iz} b_{iz} \geqq n_{iz} |B_1| / n \geqq \sum_{\mu=1}^{u} |B_\mu|^2 / n .$$

Hence

$$\sum_{2} \sum_{j=1}^{m} y_{ij} b_{ij} \geqq \sum_{s=1}^{n-1} s^2 Q_s / n ,$$

where the summation Σ_2 is taken over those values of i such that σ and τ do not commute on C_i. Combining these results we obtain

$$\sum_{i,j} y_{ij} b_{ij} \geqq cn + \sum_{s=1}^{n-1} s^2 Q_s / n \geqq G(\tau) ,$$

which disposes of Case 1.

Case 2.

$$cn + \sum_{s=1}^{n-1} s^2 Q_s / n < G(\tau) .$$

Since the total number of points of X that do not belong to any block is cn, we have

$$N = cn + \sum_{s=1}^{n-1} s Q_s .$$

Therefore

$$G(\tau) = cn + \sum_{s=1}^{n-1} sQ_s - \frac{(n-1)^2}{4n-6} \sum_{s=1}^{n-1} Q_s \,, \tag{11}$$

and we have

$$\sum_{s=1}^{n-1} s(n-s)Q_s > \frac{n(n-1)^2}{4n-6} \sum_{s=1}^{n-1} Q_s \,. \tag{12}$$

The inequality (12) cannot hold for $n = 3$. Hence $n \geqq 5$, $K \geqq 2$.

Let $q(i)$ denote the number of blocks in the cycle C_i. We denote the blocks of C_i by $B_{1i}, B_{2i}, \cdots, B_{q(i),i}$, where we suppose the blocks are ordered in such a way that

$$|B_{1i}| \geqq |B_{2i}| \geqq \cdots \geqq |B_{q(i),i}| \,.$$

We note that if σ and τ do not commute on the cycle C_i, then $q(i) \geqq 2$,

$$\sum_{w=1}^{q(i)} |B_{wi}| = n = 2K+1 \,,$$

and $|B_{\mu i}| \leqq K$ for $\mu \geqq 2$. If σ and τ commute on the cycle C_i, then $q(i) = 0$.

We call C_i a special cycle if σ and τ do not commute on C_i and $|B_{1i}| \leqq K$. Let d denote the number of special cycles. Since every cycle that is composed of blocks and is not a special cycle contains exactly one block of length at least $K+1$, we have

$$c + d + \sum_{s=K+1}^{n-1} Q_s = m = N/n = c + \sum_{s=1}^{n-1} sQ_s/n \,,$$

or

$$nd - \sum_{s=1}^{K} sQ_s + \sum_{s=K+1}^{n-1} (n-s)Q_s = 0 \,. \tag{13}$$

We call the block B_{wi} a special block if C_i is a special cycle and either

(a) $q(i) = 3$, or

(b) $q(i) = 4$ and $w \leqq 2$.

The image $B\tau$ of a block B is a block of τ^{-1}. We call $B\tau$ a block image. Let $v(i)$ denote the number of block images in the cycle C_i, and let $B'_{1i}, B'_{2i}, \cdots, B'_{v(i),i}$ denote these block images. We can suppose that

$$|B'_{1i}| \geqq |B'_{2i}| \geqq \cdots \geqq |B'_{v(i),i}| \,.$$

We call the block image B'_{wi} a special image if it is a special block of τ^{-1}. More precisely B'_{wi} is a special image if $|B'_{1i}| \leqq K$ and either

(a) $v(i) = 3$, or
(b) $v(i) = 4$ and $w \leqq 2$.
If σ and τ commute on the cycle C_i set

$$y_{ij} = \begin{cases} 1 & \text{if } \tau \text{ maps } C_i \text{ onto } C_j \text{ ,} \\ 0 & \text{otherwise .} \end{cases}$$

If C_i consists of blocks and is not a special cycle, then we set

$$y_{ij} = \begin{cases} 1 & \text{if } \tau \text{ maps } B_{1i} \text{ into } C_j \text{ ,} \\ 0 & \text{otherwise .} \end{cases}$$

If C_i is a special cycle we set

$$y_{ij} = \Sigma''(K - |B|)/(K-1) \text{ ,}$$

where the summation Σ'' runs over all special blocks B of C_i that τ maps onto special images contained in C_j. Notice that replacing τ by τ^{-1} has the effect of replacing the matrix (y_{ij}) by its transpose. Clearly $y_{ij} \geqq 0$ for all i, j. Moreover if the cycle C_i is not special, then

$$\sum_{j=1}^{m} y_{ij} = 1 \text{ .}$$

Now suppose that C_i is a special cycle. Then

$$\sum_{j=1}^{m} y_{ij} \leqq \Sigma'(K - |B|)/(K-1) \text{ ,}$$

where Σ' runs over all special blocks B of C_i. Since C_i is special we must have $q(i) \geqq 3$. If $q(i) = 3$, then every block of C_i is special, $\Sigma' |B| = 2K + 1$, and

$$\Sigma'(K - |B|)/(K-1) = (3K - \Sigma' |B|)/(K-1) = 1 \text{ .}$$

If $q(i) = 4$, then

$$|B_{1i}| + |B_{2i}| + |B_{3i}| + |B_{4i}| = 2K + 1 \text{ ,}$$

so that

$$\Sigma' |B| = |B_{1i}| + |B_{2i}| \geqq K + 1 \text{ ,}$$

and

$$\Sigma'(K - |B|)/(K-1) = (2K - \Sigma' |B|)/(K-1) \leqq 1 \text{ .}$$

Finally if $q(i) \geqq 5$, then C_i contains no special blocks, so that

$$\Sigma'(K - |B|)/(K-1) = 0 \text{ .}$$

Thus we have

$$\sum_{j=1}^{m} y_{ij} \leqq 1, 1 \leqq i \leqq m .$$

By interchanging τ and τ^{-1} we obtain

$$\sum_{i=1}^{m} y_{ij} \leqq 1, 1 \leqq j \leqq m .$$

Thus conditions (5), (8), and (9) are satisfied. We must show that (10) is satisfied also.

Let T_s denote the total number of special blocks of length s. Similarly let U_s denote the total number of special images of length s. Since there are exactly $Q_s - U_s$ block images of length s that are not special images, it follows that there are at least

$$T_s - (Q_s - U_s) = T_s + U_s - Q_s$$

special blocks of length s that are mapped onto special images by τ.

If σ and τ commute on the cycle C_i, then

$$\sum_{j=1}^{m} y_{ij} b_{ij} = n .$$

If C_i consists of blocks and is not a special cycle, then $|B_{1i}| \geqq K + 1$, and

$$\sum_{j=1}^{m} y_{ij} b_{ij} \geqq |B_{1i}| .$$

If C_i is a special cycle, then

$$\begin{aligned}\sum_{j=1}^{m} y_{ij} b_{ij} &= \sum_{j=1}^{m} \Sigma''(K - |B|) b_{ij}/(K-1) \\ &\geqq \Sigma^{\#} |B| (K - |B|)/(K-1) ,\end{aligned}$$

where Σ'' runs over those special blocks B of C_i that are mapped onto special images contained in C_j by τ, and $\Sigma^{\#}$ runs over all special blocks B of C_i that are mapped onto special images by τ. It follows that

$$\begin{aligned}\sum y_{ij} b_{ij} \geqq cn &+ \sum_{s=K+1}^{n-1} sQ_s \\ &+ \sum_{s=1}^{K} s(T_s + U_s - Q_s)(K - s)/(K-1) .\end{aligned} \tag{14}$$

To complete the proof of the lemma it is sufficient to show that (10) holds. Suppose that (10) does not hold. Then

$$G(\tau) > \sum_{i,j} y_{ij} b_{ij} .$$

Using (11) and (14) this gives us

$$cn + \sum_{s=1}^{n-1} sQ_s - \frac{(n-1)^2}{4n-6} \sum_{s=1}^{n-1} Q_s$$
$$> cn + \sum_{s=K+1}^{n-1} sQ_s + \sum_{s=1}^{K} s(T_s + U_s - Q_s)(K-s)/(K-1) ,$$

or

$$\sum_{s=1}^{K} s\{Q_s - (T_s + U_s - Q_s)(K-s)/(K-1)\}$$
$$(15) \qquad > \frac{(n-1)^2}{4n-6} \sum_{s=1}^{n-1} Q_s .$$

We multiply (15) by $n-3$ and add (12). Since $n-3 = 2(K-1)$ this gives as

$$\sum_{s=1}^{K} s\{(2n-s-3)Q_s - 2(T_s + U_s - Q_s)(K-s)\}$$
$$(16) \qquad + \sum_{s=K+1}^{n-1} s(n-s)Q_s$$
$$> \tfrac{1}{2}(n-1)^2 \sum_{s=1}^{n-1} Q_s = 2K^2 \sum_{s=1}^{n-1} Q_s .$$

Now we multiply (13) by $K-1$ and add (16). This yields

$$(17) \qquad (K-1)nd - V_1 - V_2 + W_1 + W_2 > 0 ,$$

where

$$V_1 = 2\sum_{s=1}^{K} sT_s(K-s) ,$$
$$V_2 = 2\sum_{s=1}^{K} sU_s(K-s) ,$$
$$W_1 = \sum_{s=1}^{K} \{s(2n-s-K-2) + 2s(K-s) - 2K^2\}Q_s$$
$$= \sum_{s=1}^{K} \{s(3K-s) + 2s(K-s) - 2K^2\}Q_s$$
$$= \sum_{s=1}^{K} (K-s)(3s-2K)Q_s ,$$

and

$$W_2 = \sum_{s=K+1}^{n-1} \{(K-1)(n-s) + s(n-s) - 2K^2\}Q_s$$
$$= \sum_{s=K+1}^{n-1} (s-1)(K-s+1)Q_s .$$

The effect on (17) of replacing τ by τ^{-1} is to interchange V_1 and V_2.

Now $D(\sigma\tau, \tau\sigma) = D(\sigma\tau^{-1}, \tau^{-1}\sigma)$ and $D_\sigma(\tau) = D_\sigma(\tau^{-1})$. Thus it is sufficient to prove the desired result with τ replaced by τ^{-1}. It follows that we can assume, without loss of generality, that $V_1 \leqq V_2$. Then we obtain

$$\begin{aligned}(K-1)nd + W_1 + W_2 > V_1 + V_2 &\geqq 2V_1 \\ &= 4\sum_{s=1}^{K} sT_s(K-s)\ ,\end{aligned}$$

or

$$\begin{aligned}(K-1)nd > &\sum_{s=1}^{K}\{(K-s)(2K-3s)Q_s + 4s(K-s)T_s\} \\ &+ \sum_{s=K+1}^{n-1}(s-1)(s-K-1)Q_s\ .\end{aligned} \tag{18}$$

Let $Q_s^{(i)}$ denote the number of blocks of length s in the cycle C_i, and let $T_s^{(i)}$ denote the number of special blocks of length s in C_i. Then (18) can be written in the form

$$(K-1)nd > \sum_{i=1}^{m} Z_i\ , \tag{19}$$

where

$$\begin{aligned}Z_i = &\sum_{s=1}^{K}\{(K-s)(2K-3s)Q_s^{(i)} + 4s(K-s)T_s^{(i)}\} \\ &+ \sum_{s=K+1}^{n-1}(s-1)(s-K-1)Q_s^{(i)}\ .\end{aligned}$$

If σ and τ commute on the cycle C_i we have $Q_s^{(i)} = T_s^{(i)} = 0$ for all s, so that $Z_i = 0$.

If the cycle C_i contains exactly two blocks, B_{1i} and B_{2i}, then we set $s' = |B_{2i}|$, and we have $s' \leqq K, |B_{1i}| = 2K + 1 - s' \geqq K + 1$, $T_s^{(i)} = 0$ for all s, and

$$\begin{aligned}Z_i &= (K-s')(2K-3s') + (2K-s')(K-s') \\ &= 4(K-s')^2 \geqq 0\ .\end{aligned}$$

Now suppose that C_i is a cycle that is not special, but that contains three or more blocks. Thus $q(i) \geqq 3$, and $|B_{1i}| > K$. Set $f(x) = (K-x)(2K-3x)$. The second derivative of the function f is positive, so that f is a convex function. Now $|B_{2i}| + |B_{3i}| \leqq n - |B_{1i}| \leqq K$. Therefore $f(|B_{2i}|/2 + |B_{3i}|/2) > 0$. Now for $w \geqq 4$, we have $|B_{wi}| \leqq K/3$ and $f(|B_{wi}|) > 0$. Whence

$$\begin{aligned}Z_i \geqq \sum_{w=2}^{q(i)} f(|B_{wi}|) &\geqq f(|B_{2i}|) \\ &+ f(|B_{3i}|) \geqq 2f(|B_{2i}|/2 + |B_{3i}|/2) > 0\ .\end{aligned}$$

We have shown that $Z_i \geqq 0$ for every i such that C_i is not a special cycle. Hence these terms can be dropped from the right side of (19). Now there are exactly d special cycles. Therefore, by (19), there is a special cycle C_t such that

$$Z_t < (K-1)n = 2K^2 - K - 1 .$$

Since C_t is special we have $Q_s^{(t)} = 0$ for $s > K$, and so

$$2K^2 - K - 1 > Z_t = \sum_{s=1}^{K} \{(K \quad s)(2K - 3s)Q_s^{(t)} + 4s(K-s)T_s^{(t)}\} . \tag{20}$$

Now set $q = q(t)$; and $s_w = |B_{wt}|$, $1 \leqq w \leqq q$. Then (20) can be written in the form

$$2K^2 - K - 1 > \sum_{w=1}^{q} (K - s_w)H(w) , \tag{21}$$

where

$$H(w) = \begin{cases} 2K + s_w & \text{if } B_{wt} \text{ is a special block ,} \\ 2K - 3s_w & \text{if } B_{wt} \text{ is not a special block .} \end{cases}$$

Since C_t is a special cycle we have $q = q(t) \geqq 3$.

(A) Suppose $q \geqq 5$. Then C_t has no special blocks, and (21) becomes

$$2K^2 - K - 1 > \sum_{w=1}^{q} f(s_w) ,$$

where $f(x) = (K - x)(2K - 3x)$ as before. Since f is a convex function we have

$$\sum_{w=1}^{q} f(s_w) \geqq qf(\Sigma s_w/q) = qf(n/q) .$$

Now $f(x)$ is a decreasing function of x for $x \leqq 5K/6$, and

$$n/q \leqq n/5 = (2K+1)/5 < 5K/6 .$$

Hence $f(n/q) \geqq f(n/5)$. Moreover

$$25f(n/5) = (5K - n)(10K - 3n) = (3K - 1)(4K - 3) ,$$

which is positive. Therefore

$$5(2K^2 - K - 1) > 5qf(n/q) \geqq 25f(n/5) = (3K-1)(4K-3) ,$$

or

$$0 > 2K^2 - 8K + 8 = 2(K-2)^2 ,$$

which is impossible. This disposes of the case $q \geqq 5$. Hence $q = 3$

or $q = 4$.

(B) Next suppose that $q = 3$. Here all blocks of C_t are special blocks so that (21) gives us

$$\begin{aligned} 2K^2 - K - 1 &> \sum_{w=1}^{3} (K - s_w)(2K + s_w) \\ &= 2K \sum_{w=1}^{3} (K - s_w) + \sum_{w=1}^{3} s_w(K - s_w) \, . \end{aligned} \tag{22}$$

Now

$$\sum_{w=1}^{3} (K - s_w) = 3K - \sum_{w=1}^{3} s_w = 3K - n = K - 1 \, .$$

We have $K \geqq s_1 \geqq s_2 \geqq s_3 \geqq 1$, $s_1 + s_2 + s_3 = 2K + 1$, and $K \geqq 2$. Hence $s_3 < K$. Therefore $1 \leqq s_3 \leqq K - 1$, and we have

$$\sum_{w=1}^{3} s_w(K - s_w) \geqq s_3(K - s_3) \geqq K - 1 \, .$$

Substitution in (22) now gives us

$$2K^2 - K - 1 > 2K(K - 1) + K - 1 \, ,$$

a contradiction. Thus we have eliminated the case $q = 3$. There remains only $q = 4$.

(C) Suppose finally that $q = 4$. Here B_{1t} and B_{2t} are special blocks, B_{3t} and B_{4t} are not. Thus (21) gives us

$$2K^2 - K - 1 > L_1 + L_2 + M_3 + M_4 \, , \tag{23}$$

where $L_w = (K - s_w)(2K + s_w)$ and

$$M_w = f(s_w) = (K - s_w)(2K - 3s_w) \, .$$

If $n = 5$, then $K = 2$, $s_1 = 2$, $s_2 = s_3 = s_4 = 1$, $L_1 = 0$, $L_2 = 5$, $M_3 = M_4 = 1$, which contradicts (23). Hence $n \geqq 7$ and $K \geqq 3$.

Now set $J = s_3 + s_4 = 2K + 1 - s_1 - s_2$. Then since

$$s_1 \geqq s_2 \geqq s_3 \geqq s_4 \, ,$$

we have $J \leqq K$. Since $f(x)$ is convex we have

$$M_3 + M_4 = f(s_3) + f(s_4) \geqq 2f(J/2) = (2K - J)(4K - 3J)/2 \, .$$

combining this with (23) we get

$$2K^2 > L_1 + L_2 + M_3 + M_4 \geqq L_1 + L_2 + 4K^2 - 5KJ + 3J^2/2 \, ,$$

or

$$0 > 2L_1 + 2L_2 + 4K^2 - 10KJ + 3J^2 \, .$$

Since $K \geqq 3$, we have $2K + 1 \leqq 7K/3$, and

$$J \leqq 7K/3 - s_1 - s_2 \, .$$

Since $s_1 + s_2 > K$, we have $7K/3 - s_1 - s_2 \leqq 4K/3$. Now $3x^2 - 10Kx$ is a decreasing function of x for $x \leqq 5K/3$. Hence

$$\begin{aligned} 3J^2 - 10KJ &\geqq 3(7K/3 - s_1 - s_2)^2 - 10K(7K/3 - s_1 - s_2) \\ &= -7K^2 - 4K(s_1 + s_2) + 3(s_1 + s_2)^2 \, . \end{aligned}$$

Combining inequalities we get finally

$$\begin{aligned} 0 &> 2L_1 + 2L_2 + 4K^2 + 3J^2 - 10KJ \\ &\geqq 2(K - s_1)(2K + s_1) + 2(K - s_2)(2K + s_2) \\ &\quad - 3K^2 - 4K(s_1 + s_2) + 3(s_1 + s_2)^2 \\ &= 5K^2 - 6K(s_1 + s_2) + s_1^2 + 6s_1s_2 + s_2^2 \\ &= 4(K - s_1)(K - s_2) + (s_1 + s_2 - K)^2 \, . \end{aligned}$$

This is impossible since $K \geqq s_1 \geqq s_2$. This contradiction completes the proof of the lemma.

Lemma 2 shows that $D_\sigma \leqq (n-1)^2/(4n-6)$ if n is odd, regardless of the size of m. Combining this with Lemma 1 we obtain our main result:

THEOREM. *If σ is the product of m cycles of length n, where n is odd, $n \geqq 3$, $N = nm$, and $m \geqq n - 2$, then*

$$D_\sigma = (n-1)^2/(4n-6) \, . \tag{24}$$

In the notation of [1], (24) *becomes*

$$d_\sigma = \frac{(n-1)^2}{2n(2n-3)} \, .$$

REFERENCES

1. Daniel Gorenstein, Reuben Sandler and W. H. Mills, *On Almost-commuting permutations*, Pacific J. Math. **12** (1962), 913-923.

2. John von Neumann, *A Certain Zero-Sum Two-Person Game Equivalent to the Optimal Assignment Problem, Contributions to the Theory of Games*, Vol. 2 (Edited by H. W. Kuhn and A. W. Tucker), pp. 5-12.

3. Samuel Karlin, *Mathematical Methods and Theory in Games, Programming and Economics*, Vol. 1, (1959).

YALE UNIVERSITY,
INSTITUTE FOR DEFENSE ANALYSES