J. Austral. Math. Soc. **22** (Series A) (1976), 321–331.

# REPRESENTATION OF PERMUTATIONS AS PRODUCTS OF CYCLES OF FIXED LENGTH

MARCEL HERZOG and K. B. REID

(Received 1 July 1975)

**Abstract**

We study the problem of representing a permutation $C$ as a product of a minimum number, $f_k(C)$, of cycles of length $k$. Upper and lower bounds on $f_k(C)$ are obtained and exact results are derived for $k = 2, 3, 4$.

## 1. Introduction

Ree (1971) proved a combinatorial theorem about permutation groups by using a formula for the genus of Riemann surfaces. Feit, Lyndon, and Scott (1975) gave a direct combinatorial proof of Ree's theorem and determined for a permutation $\pi$ the smallest $l(\pi) = l$ such that $\pi$ is a product of $l$ transpostions. We study the problem of representing $\pi$ as a product of a minumum number of cycles of length $k$ and use Ree's theorem to obtain exact results for $k = 2, 3, 4$.

In Section 2 we establish some notation and state our main results which are proved in Section 3. Some specialized results are discussed in Section 4.

The authors were led to this investigation by a question posed by Professor R. Burns of the University of Waterloo.

## 2. Main results

Throughout this paper $\Omega = \{1, 2, \cdots, n\}$. The symmetric and alternating groups on $\Omega$ are denoted $S_n$ and $A_n$, respectively. If $C$ is a permutation on $\Omega$, then $\operatorname{Supp} C = \{i \mid i \in \Omega, C(i) \neq i\}$. In particular, if $C = (1)$, the identity permutation, then $\operatorname{Supp} C = \varnothing$. The disjoint cycle decomposition of $C \neq (1)$ into disjoint cycles of lengths greater than 1 is denoted $dcd(C)$. If $C = (1)$, we adopt the convention that the number of cycles in any disjoint cycle decomposition of $C$ is zero. If $S$ is a finite set, then $|S|$ denotes the cardinality of $S$.

THEOREM 2.1. *Let* $C_1, C_2, \cdots, C_k, k \geqq 3$, *be permutations on* $\Omega$ *and suppose that*

$$C_k = C_1 \cdots C_{k-1}.$$

*Let* $c_i = |\operatorname{Supp} C_i|$ *and let* $r_i$ *be the number of cycles in* $dcd(C_i)$, $1 \leqq i \leqq k$. *Denote by* $a_i$, $1 \leqq i \leqq k-2$, *the number of cycles in* $dcd(C_i)$ *which do not intersect* $\operatorname{Supp} C_{k-1}$, *and denote by* $\sum I_r$, $3 \leqq r \leqq k$, *the summation of* $|\operatorname{Supp} C_{i_1} \cap \operatorname{Supp} C_{i_2} \cap \cdots \cap \operatorname{Supp} C_{i_r}|$ *over all* $r$*-tuples* $(i_1, i_2, \cdots, i_r)$ *satisfying* $1 \leqq i_1 < i_2 < \cdots < i_r \leqq k$. *Then*

$$\sum_{i=1}^{k} r_i \leqq 2r_{k-1} + 2\sum_{i=1}^{k-2} a_i + \sum I_3 - 2\sum I_4 + \cdots - (-1)^k (k-2) \sum I_k.$$

If $C \in S_n - \{(1)\}$ and $dcd(C) = C_1 \cdots C_r$, let $u_k(C) = \sum_{i=1}^{r} \{(c_i - 1)/(k-1)\}$, where $c_i = |\operatorname{Supp} C_i|$, $1 \leqq i \leqq r$, and $\{x\}$ denotes the least integer greater than or equal to $x$. If $C = (1)$, let $u_k(C) = 2$. If $C$ can be written as a product of cycles of length $k$, $1 < k \leqq n$, then $f_k(C)$ denotes the smallest $l$ such that $C$ is a product of $l$ cycles of length $k$. It is easy to see that if $k$ is even, then $f_k(C)$ is defined for all $C \in S_n$, and if $k$ is odd, then $f_k(C)$ is defined for all $C \in A_n$. We shall use the notation $D(n,k) = \{C \mid C \in S_n \text{ and } f_k(C) \text{ is defined}\}$, where $2 \leqq k \leqq n$.

THEOREM 2.2. *Let* $C \in D(n,k)$. *Then*

(i) *If* $k = 2$, *then* $f_2(C) \leqq u_2(C)$.

(ii) *If* $k$ *is odd, then* $f_k(C) \leqq u_k(C)$, *unless* $C$ *is a single cycle of odd length less than* $k$, *in which case* $f_k(C) = 2$.

(iii) *If* $k$ *is even, then* $f_k(C) \leqq u_k(C) + 1$, *unless* $C$ *is a single cycle of even length less than* $k$, *in which case* $f_k(C) = 3$.

THEOREM 2.3. *Let* $C \in D(n,k)$, *where* $2 \leqq k \leqq 4$. *Then* $f_k(C) \geqq u_k(C)$.

For $k \geqq 5$, the statement in Theorem 2.3 is false as can be seen by noting that for $k = 5$, $(12)(34)(567) = (16753)(51234)$ and then using identity (9) for $k > 5$. Note that in this paper multiplication of permutations is performed from right to left. In particular, if $a_1, \cdots, a_r, a_{r+1}, \cdots, a_s$ are distinct elements of $\Omega$, then $(a_1 \cdots a_r)(a_r a_{r+1} \cdots a_s) = (a_1 \cdots a_r \cdots a_s)$.

COROLLARY 2.4. *Let* $C \in D(n,k)$.

(i) *If* $k = 2$ or $3$, *then* $f_k(C) = u_k(C)$.

(ii) $$f_4(C) = \begin{cases} 3, & \text{if } C \text{ is a transposition} \\ u_4(C) + 1, & \text{if } u_4(C) \not\equiv u_2(C) \pmod 2 \\ u_4(C), & \text{otherwise.} \end{cases}$$

(iii) *If* $C \neq (1)$, $dcd(C) = C_1 \cdots C_r$, *and* $c_i = |\operatorname{Supp} C_i|$, $1 \leqq i \leqq r$,

*then* $f_k(C) \geqq \sum_{i=1}^{r} \left(\frac{c_i - 1}{k-1}\right)$.

https://doi.org/10.1017/S1446788700014774 Published online by Cambridge University Press

We remark that the value of $f_2(C)$ was determined using different methods by Feit, Lyndon, and Scott (1975).

## 3. Proofs

For the proof of Theorem 2.1 we require two lemmas.

LEMMA 3.1. *If* $0 < l < n$, *then*

$$\sum_{k=l+1}^{n} \binom{k-2}{l-1}\binom{n}{k}(-1)^k = (l-n)(-1)^l$$

PROOF. The proof is by induction on $l$ and $n$. If $l = 1$ and $n \geqq 2$, then $\sum_{k=2}^{n}\binom{n}{k}(-1)^k = -(1-n)$, since $(x-1)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}(-1)^k$. So suppose the Lemma holds for all $l' < l$ and $n' < n$ satisfying $0 < l' < n'$, where $1 < l < n$. If $n = l+1$, then $\binom{l-1}{l-1}\binom{l+1}{l+1}(-1)^{l+1} = (-1)(-1)^l$. So we assume that $l+1 < n$. Then

$$\begin{aligned}
&\sum_{k=l+1}^{n}\binom{k-2}{l-1}\binom{n}{k}(-1)^k \\
&= \sum_{k=l+1}^{n-1}\binom{k-2}{l-1}\binom{n-1}{k}(-1)^k + \sum_{k=l}^{n-1}\binom{k-1}{l-1}\binom{n-1}{k}(-1)^{k+1} \\
&= -\left(\sum_{k=l}^{n-1}\binom{k-2}{l-2}\binom{n-1}{k}(-1)^k - \binom{n-1}{l}(-1)^l\right) + (-1)^{l+1}\binom{n-1}{l} \\
&= -((l-n)(-1)^{l-1}) \qquad \text{(by the inductive hypothesis)} \\
&= (l-n)(-1)^l.
\end{aligned}$$

By induction the lemma follows.

The notation in the statement of Theorem 2.1 is used in the next lemma.

LEMMA 3.2. *Let $G$ be the group generated by $C_1, C_2, \cdots, C_k$, and let* Fix $G$ *be the subset of $\Omega$ fixed by $G$. Then*

$$2(n - |\operatorname{Fix} G|) = \sum_{i=1}^{k} c_i - \sum I_3 + 2\sum I_4 - \cdots + (-1)^k(k-2)\sum I_k.$$

PROOF. Let $\Delta = \Omega - \operatorname{Fix} G$. Each element of $\Delta$ occurs at least twice among the $C_i$, $1 \leqq i \leqq k$, since $C_k = C_1 \cdots C_{k-1}$. Suppose $x \in \Delta$ occurs exactly $l_x$ times. Then $x$ is counted $l_x$ times by $\sum_{i=1}^{k} c_i$, and $x$ contributes $\binom{l_x}{j}$ to $\sum I_j$, $3 \leqq j \leqq k$,

https://doi.org/10.1017/S1446788700014774 Published online by Cambridge University Press

where we understand $\binom{l}{k}=0$ for $k>l$. Thus, $x$ contributes $l_x-\binom{l_x}{3}+2\binom{l_x}{4}-\cdots+(-1)^k(k-2)\binom{l_x}{k}$ to

$$\sum_{i=1}^{k} c_i-\sum I_3+2\sum I_4-\cdots+(-1)^k(k-2)\sum I_k. \tag{1}$$

On the other hand, by Lemma 3.1, with $l=2$ and $n=l_x$, $x$ contributes 2 to (1), and the Lemma follows.

PROOF OF THEOREM 2.1. For a permutation $D\neq(1)$ on $\Omega$ define $v(D)=\Sigma_{i=1}^{m}(l_i-1)$ where $D$ is a product of disjoint cycles of lengths $l_1,\cdots,l_m$. Let $v((1))=0$. Let $T$ be the number of orbits of the group $G$ generated by $C_1, C_2,\cdots, C_k$. Then by a theorem of Ree (1971) (Feit, Lyndon, and Scott (1975) gave a combinatorial proof; a similar proof was produced by the authors)

$$2T\geqq 2n-\sum_{i=1}^{k} v(C_i). \tag{2}$$

Lemma 3.2 and (2) imply that

$$2T\geqq 2|\operatorname{Fix} G|+\sum_{i=1}^{k} r_i-\sum I_3+2\sum I_4-\cdots+(-1)^k(k-2)\sum I_k.$$

On the other hand, clearly

$$T\leqq|\operatorname{Fix} G|+r_{k-1}+\sum_{i=1}^{k-2} a_i,$$

so the Theorem follows.

The case $k=3$ of Theorem 2.1 is stated as a Corollary since it is that case which concerns us in what follows.

COROLLARY 3.3. *Let $C$, $X$, and $D$ be permutations on $\Omega$ such that $CX=D$. Let $r$, $t$, $s$ be the number of components in $dcd(C)$, $dcd(X)$, $dcd(D)$, respectively. Let*

$$k=|\operatorname{Supp} X|,\quad l=|\operatorname{Supp} X-\operatorname{Supp} D|,\quad m=|\operatorname{Supp} X-\operatorname{Supp} C|,$$

*and denote by $a$ the number of cycles in $dcd(C)$ which do not intersect* Supp $X$. *Then*

$$r+s+m+l\leqq k+t+2a.$$

PROOF. The Corollary follows immediately from Theorem 2.1 using the fact that $k-(m+l)=|C\cap X\cap D|=\Sigma I_3$.

Before we prove Theorem 2.2, we use the above notation to obtain a result on $u_k(C)$ which will be used to prove Theorem 2.3.

THEOREM 3.4. *Let C, X, and D be as in Corollary 3.3. If $t = 1$, i.e. X is a single cycle of length $k \geqq 2$, then*

(i) $|\operatorname{Supp} C| + m = |\operatorname{Supp} D| + l$,

(ii) $u_k(C) - u_k(D) \leqq ((r-a)(k-4) + (k+1) - 2m)/(k-1)$.

PROOF. Part (i) is immediate. To prove (ii), let $dcd(C) = C_1 \cdots C_r$, $dcd(D) = D_1 \cdots D_s$, and $X = (12 \cdots k)$. Let $c_i = |\operatorname{Supp} C_i|$, $1 \leqq i \leqq r_1$, and $d_i = |\operatorname{Supp} D_i|$, $1 \leqq i \leqq s$. Suppose that $a < r$. Arrange the $C_i$ so that $\operatorname{Supp} C_i \cap \{1, 2, \cdots, k\} \neq \varnothing$ if and only if $1 \leqq i \leqq r_1$, where $r_1 = r - a$. Then $C_{r_1+1}, \cdots, C_r$ are cycles in $dcd(D)$, say the last $r - r_1$ of them, so that after cancellation in $CX = D$ we obtain $C_1 \cdots C_{r_1}(12 \cdots k) = D_1 \cdots D_{s-r+r_1}$. By Corollary 3.3,

$$r_1 + (s - r + r_1) + m + l \leqq k + 1. \tag{3}$$

Now

$$u_k(C) - u_k(D) = \sum_{i=1}^{r_1} \left\{\frac{c_i - 1}{k-1}\right\} - \sum_{i=1}^{s-r+r_1} \left\{\frac{d_i - 1}{k-1}\right\}$$
$$\leqq \sum_{i=1}^{r_1} \left(\frac{c_i - 1}{k-1} + \frac{k-2}{k-1}\right) - \sum_{i=1}^{s-r+r_1} \frac{d_i - 1}{k-1}.$$

So by part (i) and (3),

$$u_k(C) - u_k(D) \leqq (1/(k-1))(|\operatorname{Supp} C| - r_1 - |\operatorname{Supp} D| + s - r + r_1)$$
$$+ r_1(k-2)/(k-1)$$
$$= (l - m - r_1 + s - r + r_1 + r_1(k-2)/(k-1)$$
$$\leqq (r_1(k-4) + (k+1) - 2m)/(k-1).$$

If $r = a$, $u_k(C) - u_k(D) = -1$. In any case (ii) follows.

COROLLARY 3.5. *Let C, X and D be as in Theorem 3.4. If $2 \leqq k \leqq 4$ or $0 \leqq r - a \leqq 1$, then $u_k(C) - u_k(D) \leqq 1$.*

PROOF. If $r = a$, then $u_k(C) - u_k(D) = -1$. So suppose that $r - a \geqq 1$. If $r - a = 1$, then by Theorem 3.3, $u_k(C) - u_k(D) \leqq [(2k-3)/(k-1)] < 2$. Also,

$$u_k(C) - u_k(D) \leqq \begin{cases} [5/3], & \text{if } k = 4 \\ [3/2], & \text{if } k = 3 \text{ (since } r - a \geqq 1) \\ [1/1], & \text{if } k = 2. \end{cases}$$

(Here $[x]$ denotes the greatest integer less than or equal to $x$.)

Before we prove a special case of Theorem 2.2 we discuss several permutation identities which will be useful. A permutation on $\Omega$ is said to be *even* (*odd*) if it can be written as a product of an even (odd) number of transpositions. So a cycle is even if and only if it is of odd length. If $i \neq j$, let $a_i$ and $a_j$ ($b_i$ and $b_j$) be distinct elements of $\Omega$. The following identities are easily verified:

$$(4) \qquad (a_1 a_2 \cdots a_{2m+1}) = (a_1 \cdots a_{m+1})(a_{m+1} \cdots a_{2m+1}) = K_1 K_2,$$

where

$$|\operatorname{Supp} K_i| = m + 1, \quad i = 1, 2.$$

If $1 < m < r$, then

$$(5) \qquad (a_1 \cdots a_m)(a_{m+1} \cdots a_{2r}) = (a_{m+1} a_1 a_{r+2} \cdots a_{2r})(a_1 \cdots a_m \cdots a_{r+1}) = K_1 K_2,$$

where

$$|\operatorname{Supp} K_i| = r + 1, \quad i = 1, 2.$$

Suppose that $2 \leqq s \leqq r \leqq n$. Let $R = (a_1 a_2 \cdots a_r)$ and $S = (b_1 b_2 \cdots b_s)$. If $b_1 \notin \operatorname{Supp} R$ and $a_r \notin \operatorname{Supp} S$, then

$$(6) \qquad RS = R(b_1 a_r)(b_1 a_r)S = (a_1 \cdots a_r b_1)(b_1 \cdots b_s a_r) = K_1 K_2,$$

where

$$|\operatorname{Supp} K_1| = r + 1 \text{ and } |\operatorname{Supp} K_2| = s + 1.$$

Next, suppose that $\operatorname{Supp} S \subseteq \operatorname{Supp} R$. Adjust notation so that $b_1 = a_r$. If $r < n$ and $x \in \Omega - \operatorname{Supp} R$, then

$$(7) \qquad RS = R(xa_r)(b_1 x)S = (a_1 \cdots a_r x)(b_1 \cdots b_s x) = K_1 K_2,$$

where

$$|\operatorname{Supp} K_1| = \; = r + 1 \text{ and } |\operatorname{Supp} K_2| = s + 1.$$

Identities (6) and (7) are special cases of a process which allows us to lengthen cycles without altering their product. By combining (4), (6) and (7) and then (5), (6) and (7), we obtain the following two general identities. Again, if $i \neq j$, then $a_i$ and $a_j$ are distinct elements of $\Omega$.

For each $l = 1, 2, \cdots, n - m$, there exist two cycles, $K_1$ and $K_2$, each of length $m + l$, so that

$$(8) \qquad (a_1 a_2 \cdots a_{2m+1}) = K_1 K_2.$$

If $m < r$, then for each $l = 1, 2, \cdots, n - r$, there exist two cycles, $K_1$ and $K_2$, each of length $r + l$, so that

$$(9) \qquad (a_1 \cdots a_m)(a_{m+1} \cdots a_{2r}) = K_1 K_2.$$

The lengthening process referred to above is described in part (ii) of our next result.

THEOREM 3.6. *Let $C$ be a permutation on $\Omega$. Suppose that $C$ can be written as the product of cycles (not necessarily disjoint) of lengths $l_1, l_2, \cdots, l_r$.*

(i) *If $\pi$ is a permutation on $\{1,2,\cdots,r\}$, then there are cycles $C_1,\cdots,C_r$ such that $C = C_1\cdots C_r$ and $|\operatorname{Supp} C_i| = l_{\pi(i)}$, $1 \leqq i \leqq r$.*

(ii) *If $l_1 \geqq l_2 \geqq \cdots \geqq l_r$ and $\{d_1, d_2, \cdots, d_r\}$ is a set of nonnegative integers such that $d_1 = d_2 + \cdots + d_r \leqq n - l_1$, then $C$ can be written as the product of $r$ cycles of lengths $l_1 + d_1, l_2 + d_2, \cdots, l_r + d_r$.*

PROOF. Part (i) follows from the fact that if $A$ and $B$ are permutations on $\Omega$, then $AB = BA^B$ and $A^B = B^{-1}AB$ has the same cycle structure as $A$.

For part (ii) we shall prove only the case $r = 3$, the proof of which clearly indicates the general procedure. So, let $C = E_1E_2E_3$, where $E_i$ is a cycle of length $l_i$, $1 \leqq i \leqq 3$, and, by (i), we may assume that $l_1 \geqq l_2 \geqq l_3$. By identites (6) and (7), there exists a product of transpositions, say $D_2$, so that $E_1D_2$ is a cycle of length $l_1 + d_2$ and $D_2^{-1}E_2$ is a cycle of length $l_2 + d_2$. Now $C = (E_1D_2)E_3(D_2^{-1}E_2)^{E_3}$. Again by (6) and (7), there exists a product of transpositions, say $D_3$, so that $E_1D_2D_3$ is a cycle of length $l_1 + d_2 + d_3$ and $D_3^{-1}E_3$ is a cycle of length $l_3 + d_3$. Since $C = (E_1D_2D_3)(D_3^{-1}E_3)(D_2^{-1}E_2)^{E_3}$, the result for $r = 3$ follows.

We now proceed to the proof of Theorem 2.2. A special case arises when all the cycles in $dcd\,(C)$ have length less than $k$.

LEMMA 3.7. *Let $C \in D(n,k)$, and if $C \neq (1)$ suppose that $dcd(C) = C_1\cdots C_r$, where $c_i = |\operatorname{Supp} C_i| < k$, $1 \leqq i \leqq r$. Then $f_k((1)) = 2$. If $C \neq (1)$, then*

(i) *If $k$ is odd, then $f_k(C) \leqq r$, unless $r = 1$ and $c_1$ is odd, in which case $f_k(C) = 2$, and*

(ii) *If $k$ is even, then $f_k(C) \leqq r + 1$, unless $r = 1$ and $c_1$ is even, in which case $f_k(C) = 3$.*

PROOF. Assume $C \neq (1)$. The proof is by induction on $r$. First, suppose $r = 1$. Then $f_k(C) \geqq 2$, as $c_1 < k$. If $c_1$ is odd, then by identity (8), $f_k(C) = 2$ as required. If $c_1$ is even, then by parity $k$ is even. Let $C = C_1 = (a_1 \cdots a_{2u})$ and let $K_1 = (a_1 \cdots a_{2u}a_{2u+1} \cdots a_k) = C_1(a_{2u} \cdots a_k)$, where $a_i$ and $a_j$ are distinct elements of $\Omega$ if $i \neq j$. As $k - 2u + 1$ is odd and less than $k$, there exist two cycles $K_2$ and $K_3$ of length $k$ such that $K_1 = C_1K_2K_3$. Thus, $f_k(C) \leqq 3$, and since $C_1$ is an odd permutation, $f_k(C) = 3$.

Next, suppose that $r = 2$. If $c_1 + c_2$ is even, then by identity (9) $C$ can be written as the product of two cycles of length $k$ and $f_k(C) \leqq 2$, as required. So assume that $c_1 + c_2$ is odd, $c_1 > c_2$, and let $d = k - c_1$. By identities (6) and (7), $C = C_1'C_2'$, where $C_1'$ ($C_2'$) is a cycle of length $k$ ($c_2 + d$, respectively). Since $C$ is an odd permutation, and $C \in D(n,k)$, $k$ must be even. So $c_2 + d$ must be odd as

$C = C_1'C_2'$. Hence, by identity (8), $C_2'$ can be written as the product of two cycles of length $k$ and $f_k(C) \leqq 3 = r + 1$, as required.

Now suppose that $r > 2$ and that the Lemma holds for all $r' < r$. Without loss of generality, assume that $c_1 \geqq c_2 \geqq \cdots \geqq c_r$ (see Theorem 3.6 (i)). Let $d = k - c_1$. If $d > \Sigma_{i=2}^{r}(k - c_i - 1) \geqq (r-1)(d-1)$, then $d = 1$ and $c_i = k - 1$, $1 \leqq i \leqq r$. By identity (6), $C = C_1'C_2'C_3 \cdots C_r$, where $C_1'$ and $C_2'$ are cycles of length $k$. If $r > 3$, then by application of the induction hypothesis to $C_3 \cdots C_r$, the result follows. So assume $r = 3$. Suppose $k$ is odd. Since $c_i = k - 1$, $1 \leqq i \leqq 3$, $C$ is an odd permutation. However, $C \in D(n, k)$, so $C$ is an even permutation, a contradiction. Consequently, $k$ is even. But then, by identity (8), $C_3$ can be written as the product of two cycles of length $k$, and $f_k(C) \leqq 4 = r + 1$, as required. Thus, it may be assumed that there exists a partition $d = d_2 + \cdots + d_r$, where $d_i \leqq k - c_i - 1$, $2 \leqq i \leqq r$. By Theorem 3.6 (ii), $C = C_1' \cdots C_r'$, where $C_i'$ is a cycle of length $c_i + d_i$, $2 \leqq i \leqq r$, and $C_1'$ is a cycle of length $k$. Note that $c_i + d_i < k$, $2 \leqq i \leqq r$, so by application of the induction hypothesis to $C_2' \cdots C_r'$, the result follows. By induction the Lemma is proved.

Proof of Theorem 2.2. Let $dcd(C) = C_1 \cdots C_r$ and $c_i = |\operatorname{Supp} C_i|$, $1 \leqq i \leqq r$. Since $(a_1 \cdots a_k \cdots a_{2k-1} \cdots) = (a_1 \cdots a_k)(a_k \cdots a_{2k-1})(a_{2k-1} \cdots) \cdots$, $C$ can be written as a product of $e = \Sigma_{i=1}^{r}[(c_i - 1)/(k-1)]$ cycles of length $k$ and at most $r$ disjoint cycles of lengths less than $k$, say these are $R_1 \cdots R_t$, $t \leqq r$.

Thus, the Theorem holds if $t = 0$; in particular (i) follows. So suppose that $k > 2$ and $t > 0$. If $t > 1$, then the Theorem follows immediately from Lemma 3.7; so assume that $t = 1$. If $r \geqq 2$, then the Theorem follows from identity (9) (if $k + |\operatorname{Supp} R_1|$ is even) and Lemma 3.7. So, assume that $r = 1$.

If $k$ is odd, then $r_1 = |\operatorname{Supp} R_1|$ is odd since $C$ is in $D(n, k)$ and hence an even permutation. If $e \neq 0$, then let

$$
\begin{aligned}
C &= (a_1 \cdots a_{e(k-1)} a_{e(k-1)+1} \cdots a_{e(k-1)+r_1}) \\
&= (a_1 \cdots a_k)(a_k \cdots a_{2k-1}) \cdots (a_{(e-1)(k-1)+1} \cdots a_{e(k-1)+1} \cdots a_{e(k-1)+r_1}) \\
&= K_1 \cdots K_{e-1} L,
\end{aligned}
$$

where $K_1 \cdots K_{e-1}$ is a product of cycles of length $k$ if $e > 1$, $K_1 \cdots K_{e-1}$ is (1) if $e = 1$, and $L$ is a cycle of odd length $k - 1 + r_1$. By identity (8), $f_k(C) \leqq u_k(C)$. If $e = 0$, then $f_k(C) = 2$ by Lemma 3.7 (i), as required.

Finally, suppose that $k$ is even. If $|\operatorname{Supp} R_1|$ is even, then either $e = 0$ and $f_k(C) = 3$ by Lemma 3.7 (ii), or $e \neq 0$ and as above $f_k(C) \leqq u_k(C)$ by identity (8). If $|\operatorname{Supp} R_1|$ is odd, then again by Lemma 3.7 (ii), $f_k(C) \leqq u_k(C) + 1$, as required.

The Theorem follows.

PROOF OF THEOREM 2.3. Fix $k$, $2 \leqq k \leqq 4$. The proof is by induction on $f_k(C)$. If $f_k(C) = 1$, then $C$ is a cycle of length $k$ and $u_k(C) = 1$. Suppose that $f_k(C) = m > 1$ and that the Theorem holds for all values of $f_k(C') < m$. If $C = K_1 K_2 \cdots K_m$, where $K_i$ is a cycle of length $k$, $1 \leqq i \leqq m$, then $f_k(CK_m^{-1}) \leqq m - 1$, so that by that induction hypotheses $f_k(CK_m^{-1}) \geqq u_k(CK_m^{-1})$. Suppose that $m \leqq u_k(C) - 1$. Then $u_k(CK_m^{-1}) \leqq f_k(CK_m^{-1}) \leqq m - 1 \leqq u_k(C) - 2$, hence $u_k(C) - u_k(CK_m^{-1}) \geqq 2$, contrary to Corollary 3.5. Thus, $f_k(C) = m \geqq u_k(C)$.

PROOF OF COROLLARY 2.4. Since $u_k((1)) = 2$ for all $2 \leqq k \leqq n$, the Corollary holds for $C = (1)$. Thus, assume that $C \neq (1)$. Part (i) follows from Theorem 2.2 (i), (ii) and Theorem 2.3. For part (ii), $0 \leqq f_4(C) - u_4(C) \leqq 1$ by Theorem 2.2 (iii) and Theorem 2.3, unless $C$ is a single transposition, in which case $f_4(C) = 3$. So assume that $C$ is not a transposition. Certainly $f_4(C) \equiv f_2(C) \pmod 2$, so by part (i) $f_4(C) \equiv u_2(C) \pmod 2$, and (ii) follows. To prove part (iii) let $C = K_1 \cdots K_m$, where $m = f_k(C)$ and $K_i$ is a cycle of length $k$, $1 \leqq i \leqq m$. Then by part (i) $\Sigma_{i=1}^{r}(c_i - 1) = f_2(C) \leqq \Sigma_{i=1}^{m} f_2(K_i) = m(k-1)$. Part (iii) follows. This completes the proof of the Corollary.

## 4. Specialized results

The argument used in the proof of Corollary 2.4 (iii) yields two results worth noting.

COROLLARY 4.1. *Let $C \in D(n, k)$, $C \neq (1)$. Suppose that $dcd(C) = C_1 \cdots C_r$ and $c_i = |\mathrm{Supp}\, C_i|$, $1 \leqq i \leqq r$.*

(i) *If $r = 1$, then $f_k(C) \geqq \{(|\mathrm{Supp}\, C| - 1)/(k-1)\}$.*

(ii) *If $C = K_1 \cdots K_m$, where $m = f_k(C)$ and $K_i$ is a cycle of length $k$, $1 \leqq i \leqq m$, such that $C_1 = K_1 \cdots K_{i_1}$, $C_2 = K_{i_1+1} \cdots K_{i_2}$, $\cdots$, $C_r = K_{i_{r-1}+1} \cdots K_m$, $1 \leqq i_1 < i_2 \cdots < i_{r-1} < m$, then $f_k(C) \geqq u_k(C)$.*

The case when $C$ is a single cycle is treated next.

THEOREM 4.2. *Let $C \in D(n, k)$ be a single cycle of length c. If k is even and $c - 1 = (k-1)q + t$, $0 \leqq t \leqq k - 2$, then*

$$f_k(C) = \begin{cases} u_k(C), & \text{if } t = 0 \text{ or } t \text{ is odd and not } c-1 \\ u_k(C) + 1, & \text{if } t \neq 0 \text{ and } t \text{ is even} \\ 3, & \text{if } t = c - 1 \text{ and } t \text{ is odd,} \end{cases}$$

*and $u_k(C) = \{(c-1)/(k-1)\}$.*

PROOF. As in the proof of Corollary 2.4 (ii), $f_k(C) \equiv c-1 \pmod 2$. But

$$c-1 \equiv t+q \equiv \begin{cases} u_k(C), & \text{if } t=0 \text{ or } t \text{ is odd and not } c-1 \\ u_k(C)+1, & \text{if } t \neq 0 \text{ and } t \text{ is even} \\ 3, & \text{if } t=c-1 \text{ and } t \text{ is odd} \end{cases} \pmod 2.$$

The Theorem then follows from Theorem 2.2 (iii) and Corollary 4.1 (i).

COROLLARY 4.3. *Let $C \in D(n,k)$, $C \neq (1)$. Let $dcd(C) = C_1 \cdots C_r$ and $c_i = |\,\mathrm{Supp}\, C_i\,|$, $1 \leqq i \leqq r$. Write $c_i - 1 = (k-1)q_i + r_i$, where $0 \leqq r_i \leqq k-2$, $1 \leqq i \leqq r$. For each $2 \leqq j \leqq k-2$, let $s_j = |\{r_i \mid 1 \leqq i \leqq t,\ r_i = j\}|$. If $k$ is even, then*

$$f_k(C) - u_k(C) \equiv \sum \{s_{2p} \mid 1 \leqq p \leqq (k-2)/2\} \pmod 2.$$

PROOF. As $k$ is even $f_k(C) \equiv \Sigma_{i=1}^{r} f_k(C_i) \pmod 2$. By Theorem 4.2, $f_k(C) \equiv u_k(C) + \Sigma\{s_{2p} \mid 1 \leqq p \leqq (k-2)/2\} \pmod 2$.

THEOREM 4.4. *With the notation of Corollary 4.3, if $k$ is even and $\Sigma\{s_{2p} \mid 1 \leqq p \leqq (k-2)/2\} \equiv 0 \pmod 2$, then $f_k(C) \leqq u_k(C)$ unless $C$ is a single cycle of even length less than $k$, in which case $f_k(C) = 3$.*

PROOF. Apply Theorem 2.2 (iii) and Corollary 4.3.

The previous results allow us to restate the conclusion of Corollary 2.4 (ii) when $C \neq (1)$ as

$$f_4(C) = \begin{cases} 3, & \text{if } C \text{ is a transposition} \\ u_4(C)+1, & \text{if } s_2 \equiv 1 \pmod 2 \\ u_4(C), & \text{if } s_2 \equiv 0 \pmod 2 \end{cases}$$

where $s_2$ is the number of cycles in $dcd(C)$ whose lengths are divisible by 3.

A slight improvement of the inequality used in the proof of Corollary 2.4 (iii) can be obtained if consideration is given to the way that the cycles $K_i$ combine to yield the disjoint cycles $C_j$. The *intersection graph* of a set $\{S_1, \cdots, S_m\}$ of distinct subsets of some set $S$ has vertex set $\{S_1, \cdots, S_m\}$ and $S_i$ and $S_j$ are adjacent if $i \neq j$ and $S_i \cap S_j \neq \varnothing$.

THEOREM 4.5. *Let $C \in S_n - \{(1)\}$, $dcd(C) = C_1 \cdots C_r$ and $c_i = |\,\mathrm{Supp}\, C_i\,|$, $1 \leqq i \leqq r$. If $C = K_1 \cdots K_m$, where $K_i$ is a cycle of length $k_i$, $1 \leqq i \leqq m$, then $\Sigma_{i=1}^{m}(k_i - 1) \geqq (\Sigma_{i=1}^{r} c_i) - p$, where $p$ is the number of connected components in the intersection graph of $\{\mathrm{Supp}\, K_1, \cdots, \mathrm{Supp}\, K_m\}$.*

The proof is left to the reader.

## References

W. Feit, R. Lyndon, and L. Scott (1975), 'A remark about permutations', *J. Combinatorial Theory* **18,** 234–235.

R. Ree (1971), 'A theorem on permutations', *J. Combinatorial Theory* **10,** 174–175.

Department of Mathematics,
Institute of Advanced Studies,
The Australian National University,
Canberra, ACT 2600.

Department of Mathematics,
Institute of Advanced Studies,
The Australian National University,
Canberra, ACT 2600.

Department of Mathematics,
Tel-Aviv University,
Tel-Aviv, Israel.

Department of Mathematics,
Louisiana State University,
Baton Rouge, Louisiana 70803, U.S.A.

https://doi.org/10.1017/S1446788700014774 Published online by Cambridge University Press